

Legislația ta completă pentru **E-Commerce**

Furnizată de lege [5]



Cuprins

Ordonanța de urgență nr. 34/2014 privind drepturile consumatorilor în cadrul contractelor încheiate cu profesioniștii

Ordonanța nr. 85/2004 privind protecția consumatorilor la încheierea și executarea contractelor la distanță privind serviciile financiare

Ordinul nr. 553/2019 privind reglementarea procedurii de avizare a instrumentelor de plată electronică cu acces la distanță

Regulamentul nr. 3/2018 privind monitorizarea infrastructurilor pieței financiare și a instrumentelor de plată

Legea nr. 296/2004 privind Codul consumului

Legea nr. 365/2002 privind comerțul electronic

Legea nr. 193/2000 privind clauzele abuzive din contractele încheiate între profesioniști și consumatori

Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR

Regulamentul nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor - GDPR)

Ordonanța de urgență nr. 34/2014 privind drepturile consumatorilor în cadrul contractelor încheiate cu profesioniștii, precum și pentru modificarea și completarea unor acte normative

În vigoare de la 13 iunie 2014

Consolidarea din data de **05 noiembrie 2019** are la bază [publicarea din Monitorul Oficial, Partea I](#) nr. 427 din 11 iunie 2014

Include modificările aduse prin următoarele acte: L [157/2015](#); OG [2/2018](#); L [109/2019](#).
Ultimul amendament în 31 mai 2019.

Având în vedere că transpunerea în legislația națională a Directivei [2011/83/UE](#) a Parlamentului European și a Consiliului din 25 octombrie 2011 privind drepturile consumatorilor, de modificare a Directivei [93/13/CEE](#) a Consiliului și a Directivei [1999/44/CE](#) a Parlamentului European și a Consiliului și de abrogare a Directivei [85/577/CEE](#) a Consiliului și a Directivei [97/7/CE](#) a Parlamentului European și a Consiliului trebuia realizată până la data de 13 decembrie 2013,

adoptarea prezentei ordonanțe de urgență se impune pentru a crea un cadru unitar, bazat pe concepte juridice clar definite, care să reglementeze anumite aspecte ale raporturilor dintre comercianți și consumatori în cadrul Uniunii.

Ținând cont de faptul că, în lipsa unei reglementări imediate privind drepturile consumatorilor la încheierea contractelor, aceștia nu ar putea beneficia de drepturile prevăzute de actul normativ european, fiind prejudiciați de informațiile ce trebuie oferite consumatorilor în stadiul precontractual, precum și de informațiile contractuale pe care comercianții trebuie să le furnizeze consumatorilor, de condițiile de formă pe care trebuie să le îndeplinească aceste contracte, precum și ținând cont de necesitatea inițierii de către operatorii economici a unor demersuri în vederea respectării prevederilor directivei,

pentru a se evita posibilitatea declanșării procedurii de infringement de către Comisia Europeană împotriva României pentru neimplementarea în dreptul intern a prevederilor directivei comunitare și de a asigura implementarea acesteia,

Directiva [2011/83/UE](#) a fost publicată în Jurnalul Oficial, seria L, nr. 304 din 22 noiembrie 2011 și a intrat în vigoare în a 20-a zi de la data publicării sale în Jurnalul Oficial. Statele membre au avut un termen de 2 ani pentru transpunerea directivei. Respectivul termen a expirat la 13 decembrie 2013. Întrucât nu i-au fost comunicate din partea autorităților române măsurile naționale pentru transpunerea directivei, la data de 27 ianuarie 2014, Comisia Europeană (Comisia) a declanșat o acțiune în constatarea neîndeplinirii obligațiilor împotriva României, în temeiul [art. 258](#) TFUE, transmițând o scrisoare de punere în întârziere. Termenul de răspuns la respectiva scrisoare s-a împlinit la 27 martie 2014.

Faza contencioasă debutează cu sesizarea Curții de Justiție a Uniunii Europene - CJUE de către Comisie. Curtea poate condamna statul vizat, dacă constată neîndeplinirea obligațiilor. În acest caz, potrivit art. 260 [paragraful 3](#) din [Tratatul](#) privind funcționarea Uniunii Europene - TFUE, CJUE poate

aplica statului vizat sancțiuni pecuniare (sumă forfetară și/sau penalități pe zile de întârziere), în limita valorii indicate de Comisie. Obligația de plată intră în vigoare la data stabilită de Curte prin hotărârea sa. Potrivit Comunicării Comisiei C(2013) 8101 final privind actualizarea datelor utilizate pentru calcularea sumei forfetare și a penalităților cu titlu cominatoriu pe care Comisia urmează să le propună Curții de Justiție în cadrul procedurii de constatare a neîndeplinirii obligațiilor "Comunicarea din 2013", care modifică și actualizează Comunicarea Comisiei SEC(2005) 1658¹ privind punerea în aplicare a [articolului 228](#) din Tratatul de instituire a Comunității Europene, Comunicarea Comisiei C(2012) 6106 final privind actualizarea datelor folosite pentru calcularea sumelor forfetare sau a penalităților cu titlu cominatoriu care vor fi propuse de Comisie Curții de Justiție în procedurile în constatarea neîndeplinirii obligațiilor, Comunicarea Comisiei SEC(2011) 1024 final pentru actualizarea datelor folosite pentru calcularea sumei forfetare sau a penalităților cu titlu cominatoriu care vor fi propuse de Comisie Curții de Justiție în procedurile în constatarea neîndeplinirii obligațiilor, Comunicarea Comisiei SEC(2010) 1371 privind punerea în aplicare a articolului 260 [alineatul \(3\)](#) din TFUE, suma forfetară minimă fixă care ar putea fi propusă de Comisie pentru România este în valoare de 1.787.000 euro.

Penalitățile pe zile de întârziere (penalitățile cu titlu cominatoriu) constau în obligarea la plata unei sume de bani pentru fiecare zi/lună/an de întârziere în adoptarea măsurilor de conformare, cu începere de la data hotărârii Curții pronunțate în temeiul art. 260 [paragraful 3](#) TFUE până la executarea integrală a obligațiilor. Acestea sunt de natură să determine un stat membru să pună capăt cât mai repede încălcării constatate și care persistă.

Potrivit Comisiei, penalitățile cu titlu cominatoriu se calculează pornind de la o sumă de bază, care în prezent este stabilită la 650 de euro pe zi de întârziere. Această sumă de bază este înmulțită cu un coeficient de gravitate, cu un coeficient de durată și cu factorul "n", stabilit pentru România.

Potrivit Comunicării din 2013, factorul "n" pentru România este de 3,32.

Penalitățile pe zile de întârziere se aplică din ziua în care hotărârea prin care CJUE constată existența unei încălcări ar fi comunicată României până în ziua în care s-ar pune capăt încălcării.

În acest context, MAE-SCUE a subliniat și că aceste acțiuni, în cazul în care ajung în fază contencioasă, sunt soluționate de Curte cu celeritate - a se vedea, de exemplu, Cauza C-202/09, Comisia/Irlanda, în care Comisia a sesizat CJUE la data de 5 iunie 2009, iar Curtea a pronunțat hotărârea sa la data de 26 noiembrie 2009, deci în mai puțin de 6 luni.

Ținând cont de faptul că aceste aspecte vizează interesul public și constituie situații de urgență și extraordinare a căror reglementare nu poate fi amânată,

în temeiul art. 115 [alin. \(4\)](#) din Constituția României, republicată,

Guvernul României adoptă prezenta ordonanță de urgență.

CAPITOLUL I

Obiect, definiții și domeniu de aplicare

ARTICOLUL 1 Obiect Prezenta ordonanță de urgență reglementează drepturile consumatorilor în cadrul contractelor încheiate cu profesioniștii, pentru asigurarea unui nivel înalt de protecție a consumatorilor și o bună funcționare a pieței.

ARTICOLUL 2 Definiții În sensul prezentei ordonanțe de urgență, următoarele expresii și termeni se definesc după cum urmează:

1. consumator - orice persoană fizică sau grup de persoane fizice constituite în asociații, așa cum sunt definite la art. 2 [pct. 2](#) din Ordonanța Guvernului nr. 21/1992 privind protecția consumatorilor, republicată, cu modificările și completările ulterioare;

2. profesionist - orice persoană fizică sau juridică, publică sau privată, care acționează în cadrul activității sale comerciale, industriale sau de producție, artizanale ori liberale în legătură cu contractele care intră sub incidența prezentei ordonanțe de urgență, precum și orice persoană care acționează în același scop, în numele sau pe seama acesteia;

3. produs - orice bun corporal mobil, cu excepția bunurilor vândute prin executare silită sau valorificate ca urmare a aplicării prevederilor legale; apa, gazele naturale, energia electrică și energia termică sunt considerate "produse" atunci când acestea sunt puse în vânzare în volum limitat sau în cantitate fixă;

4. produse realizate conform specificațiilor clientului - orice produse care nu sunt prefabricate, realizate pe baza opțiunilor individuale sau a deciziei clientului;

5. contract de vânzare - orice contract în temeiul căruia profesionistul transferă sau se angajează să transfere proprietatea asupra unor produse către consumator, iar consumatorul plătește sau se angajează să plătească prețul acestora, inclusiv orice contract care are drept obiect atât produse, cât și servicii;

6. contract de prestări de servicii - orice contract, altul decât un contract de vânzare, în temeiul căruia profesionistul prestează sau se angajează să presteze un serviciu consumatorului, iar acesta plătește sau se angajează să plătească prețul acestuia;

7. contract la distanță - orice contract încheiat între profesionist și consumator în cadrul unui sistem de vânzări sau de prestare de servicii la distanță organizat, fără prezența fizică simultană a profesionistului și a consumatorului, cu utilizarea exclusivă a unuia sau a mai multor mijloace de comunicare la distanță, până la și inclusiv în momentul în care este încheiat contractul;

8. contract în afara spațiilor comerciale - orice contract dintre un profesionist și un consumator, într-una din următoarele situații:

a) încheiat în prezența fizică simultană a profesionistului și a consumatorului, într-un loc care nu este spațiul comercial al profesionistului;

b) încheiat ca urmare a unei oferte din partea consumatorului în aceleași circumstanțe ca cele menționate la lit. a);

c) încheiat în spațiile comerciale ale profesionistului sau prin orice mijloace de comunicare la distanță, imediat după ce consumatorul a fost abordat în mod personal și individual, într-un loc care nu este spațiul comercial al profesionistului, în prezența fizică simultană a acestuia și a consumatorului;

d) încheiat în cursul unei deplasări organizate de profesionist cu scopul sau efectul de a promova și a vinde consumatorului produse sau servicii;

9. spațiu comercial - orice unitate care îndeplinește una dintre următoarele condiții:

a) unitate imobilă de vânzare cu amănuntul, în care profesionistul își desfășoară activitatea în permanență;

b) unitate mobilă de vânzare cu amănuntul, în care profesionistul își desfășoară activitatea în mod obișnuit;

10. suport durabil - orice instrument care permite consumatorului sau profesionistului să stocheze informații care îi sunt adresate personal, într-un mod accesibil pentru referințe ulterioare pentru o perioadă de timp adecvată, în vederea informării, și care permite reproducerea neschimbată a informațiilor stocate;

11. conținut digital - acele date care sunt produse și livrate în formă digitală;

12. serviciu financiar - orice serviciu cu caracter bancar, de creditare, asigurări, pensii private, de investiții sau plăți;

13. licitație - metoda de vânzare prin care profesionistul oferă produse sau servicii consumatorilor, care participă sau au posibilitatea de a participa în persoană la licitație, prin intermediul unei proceduri de licitare transparentă, concurențială, condusă de un judecător și în care ofertantul câștigător este obligat să achiziționeze produsele sau serviciile;

14. garanție comercială - orice angajament din partea profesionistului sau a unui producător (denumit în continuare garantul) față de consumator, în plus față de obligațiile legale prevăzute la [art. 5-14](#) din Legea [nr. 449/2003](#) privind vânzarea produselor și garanțiile asociate acestora, republicată, cu modificările și completările ulterioare, referitoare la garanția legală de conformitate, de a rambursa prețul plătit sau de a înlocui, a repara sau a întreține produsele în orice mod, în cazul în care acestea nu corespund specificațiilor sau oricărei altei cerințe din declarația privind garanția sau din publicitatea relevantă disponibilă în momentul sau înaintea încheierii contractului, cerință care nu este legată de conformitate;

15. contract auxiliar - un contract prin care consumatorul obține produsele sau serviciile care fac obiectul unui contract la distanță sau al unui contract în afara spațiilor comerciale, iar aceste produse sau servicii sunt livrate, respectiv prestate de profesionist sau de o parte terță, pe baza unui acord între partea terță respectivă și profesionist.

ARTICOLUL 3 Domeniul de aplicare (1) Prezenta ordonanță de urgență se aplică oricărui contract încheiat între un profesionist și un consumator, inclusiv contractelor de furnizare a unor servicii de comunicații electronice destinate publicului sau a unor servicii de acces și conectare la rețele publice de comunicații electronice, precum și de livrare a unor echipamente terminale care au legătură cu furnizarea serviciului. Ea se aplică și contractelor de furnizare a apei, gazelor naturale, energiei electrice sau energiei termice, inclusiv de către furnizorii publici, în măsura în care aceste utilități sunt furnizate pe bază contractuală.

(2) În cazul în care vreo dispoziție a prezentei ordonanțe de urgență intră în contradicție cu o dispoziție a unui alt act din legislația națională ce transpune un act al Uniunii Europene care reglementează sectoare specifice, dispozițiile acestuia din urmă prevalează și se aplică sectoarelor specifice în cauză.

(3) Prezenta ordonanță de urgență nu se aplică următoarelor contracte:

a) de prestare a unor servicii sociale, printre care cele de cazare socială, de îngrijire a copiilor și de susținere a familiilor și a persoanelor aflate permanent sau temporar în nevoie, inclusiv cele de îngrijire pe termen lung;

- b) având ca obiect serviciile de sănătate furnizate pacienților de către cadrele medicale pentru evaluarea, menținerea sau refacerea stării lor de sănătate, inclusiv prescrierea, eliberarea și furnizarea de medicamente și dispozitive medicale, indiferent dacă acestea sunt sau nu furnizate în cadrul unor unități medicale;
 - c) având ca obiect jocurile de noroc care implică mizarea pe un pot cu valoare pecuniară în jocuri de noroc, inclusiv loterii, jocuri de cazinou și tranzacții de tipul pariurilor;
 - d) referitoare la servicii financiare;
 - e) pentru crearea, dobândirea sau transferul unui bun imobil sau al unor drepturi asupra unui bun imobil;
 - f) având ca obiect construirea unor clădiri noi, transformarea substanțială a unor clădiri existente și închirierea de locuințe în scopuri rezidențiale;
 - g) având ca obiect pachetele, astfel cum sunt definite la art. 3 [pct. 12](#) din Ordonanța Guvernului nr. 2/2018 privind pachetele de servicii de călătorie și serviciile de călătorie asociate, precum și pentru modificarea unor acte normative, cu excepția art. 6 [alin. \(7\)](#), art. 8 [alin. \(2\)](#) și [\(6\)](#), [art. 21](#) și [art. 22](#) care se aplică în cazul călătorilor astfel cum sunt definiți la art. 3 [pct. 2](#) din Ordonanța Guvernului nr. 2/2018;
 - h) care intră sub incidența Ordonanței de urgență a Guvernului [nr. 14/2011](#) pentru protecția consumatorilor la încheierea și executarea contractelor privind dobândirea dreptului de folosință pe o perioadă determinată a unuiu sau a mai multor spații de cazare, a contractelor pe termen lung privind dobândirea unor beneficii pentru produsele de vacanță, a contractelor de revânzare, precum și a contractelor de schimb;
 - i) având ca obiect furnizarea alimentelor, băuturilor sau a altor bunuri destinate consumului casnic, livrate fizic de un profesionist care se deplasează frecvent și periodic la locuința, reședința sau locul de muncă al consumatorului;
 - j) de prestare a unor servicii de transport de pasageri, cu excepția art. 8 [alin. \(2\)](#) și a [art. 22](#);
 - k) încheiate prin intermediul automatelor sau incintelor comerciale automatizate;
 - l) încheiate cu furnizorii de servicii de comunicații electronice prin telefoane publice cu plată, pentru utilizarea acestora, sau încheiate pentru utilizarea unei conexiuni unice, care presupune executarea unei singure prestații, realizată simultan încheierii contractului și nemijlocit prin intermediul telefonului, internetului sau faxului, ca urmare a solicitării consumatorului.
- (4) Prezenta ordonanță de urgență nu se aplică în cazul contractelor în afara spațiilor comerciale în care plata ce trebuie efectuată de către consumator este mai mică decât echivalentul în lei a 10 euro la cursul de zi al Băncii Naționale a României, cu excepția [art. 9-16](#) și a [art. 18-24](#) care se aplică și acestor contracte. În cazul contractelor de prestări servicii valoarea contractului este stabilită prin înmulțirea valorii lunare a serviciului cu durata contractului.
- (5) Prezenta ordonanță de urgență nu împiedică oferirea de către profesionist a unor condiții contractuale mai avantajoase pentru consumator.

CAPITOLUL II

Informații destinate consumatorilor pentru alte contracte decât contractele la distanță sau contractele în afara spațiilor comerciale

ARTICOLUL 4 Cerințe în materie de informare pentru alte contracte decât contractele în afara spațiilor comerciale și contractele la distanță (1) Înainte ca un contract, altul decât un contract la distanță sau un contract în afara spațiilor comerciale, sau orice ofertă similară să producă efecte obligatorii asupra consumatorului, profesionistul trebuie să îi furnizeze consumatorului următoarele informații în mod vizibil, lizibil și ușor de înțeles, în cazul în care respectivele informații nu reies în mod evident din context:

- a) principalele caracteristici ale produselor sau serviciilor, având în vedere mediul de comunicare, precum și produsele sau serviciile în cauză;
- b) identitatea profesionistului, incluzând denumirea sa, adresa poștală la care profesionistul este stabilit, precum și, în cazul în care există, numărul de telefon, numărul de fax și adresa de poștă electronică ale acestuia la care poate fi efectiv contactat, pentru a-i permite consumatorului să ia rapid legătura cu profesionistul și să comunice cu acesta în mod eficient și, dacă este cazul, adresa poștală și identitatea profesionistului în numele căruia acționează;
- c) prețul total al produselor sau serviciilor cu toate taxele incluse sau, în cazul în care prețul nu poate fi calculat în avans în mod rezonabil dată fiind natura produselor sau a serviciilor, modalitatea de calcul al prețului și, după caz, toate costurile suplimentare de transport, de livrare sau taxele poștale sau, în cazul în care acestea nu pot fi calculate în avans în mod rezonabil, menționarea faptului că aceste costuri suplimentare ar putea fi suportate de consumator;
- d) după caz, modalitățile de plată, livrare și executare, data până la care profesionistul se angajează să livreze produsele sau să presteze serviciile și politica profesionistului de soluționare a reclamațiilor;
- e) în plus față de o mențiune a existenței unei garanții legale de conformitate pentru produse, existența și condițiile privind serviciile postvânzare și garanțiile comerciale, după caz;
- f) durata de valabilitate a contractului, după caz, sau, pentru un contract pe durată nedeterminată ori un contract care urmează să fie prelungit în mod automat, condițiile de încetare a contractului și penalitățile aplicabile, dacă este cazul;
- g) acolo unde este cazul, funcționalitatea, inclusiv aplicarea unor măsuri tehnice de protecție pentru conținuturile digitale;
- h) acolo unde este cazul, orice interoperabilitate relevantă a conținuturilor digitale cu componentele hardware și software de care profesionistul are cunoștință sau se așteaptă în mod rezonabil să aibă cunoștință;
- i) despăgubirile aplicabile și procedura de acordare a acestora în cazul nerespectării nivelurilor de calitate convenite și a celorlalte clauze contractuale;
- j) opțiunea consumatorului de a se include sau de a nu se include datele sale cu caracter personal în baze de date în vederea furnizării de servicii de informații privind abonații sau de registre ale abonaților, precum și, în cazul în care acesta optează pentru includerea în registrul abonaților, indicarea datelor în cauză, în conformitate cu prevederile Legii [nr. 506/2004](#) privind prelucrarea datelor cu

caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare.

(2) Prevederile [alin. \(1\)](#) se aplică și contractelor de furnizare a apei, gazelor naturale sau energiei electrice, atunci când acestea nu sunt puse în vânzare într-un volum limitat sau cantitate fixă, a energiei termice sau a conținuturilor digitale care nu sunt livrate pe un suport material.

(3) Prevederile [alin. \(1\)](#) nu se aplică contractelor care implică tranzacții care se efectuează cu regularitate zilnic și care sunt puse în execuție imediat, în momentul în care sunt încheiate.

(4) Informațiile prevăzute la [alin. \(1\)](#) fac parte integrantă din contract.

ARTICOLUL 5 Sarcina probei Sarcina probei în ceea ce privește îndeplinirea cerințelor în materie de informare stabilite în prezentul capitol revine profesionistului.

CAPITOLUL III

Informații destinate consumatorilor și dreptul de retragere din contractele la distanță și cele în afara spațiilor comerciale

ARTICOLUL 6 Cerințe de informare pentru contractele la distanță și cele în afara spațiilor comerciale

(1) Înainte ca un contract la distanță sau în afara spațiilor comerciale sau orice ofertă similară să producă efecte obligatorii asupra consumatorului, profesionistul trebuie să îi furnizeze consumatorului următoarele informații în mod clar și inteligibil:

a) principalele caracteristici ale produselor sau serviciilor, având în vedere mediul de comunicare și produsele sau serviciile în cauză;

b) identitatea profesionistului, cum ar fi denumirea sa comercială;

c) adresa poștală la care profesionistul este stabilit, precum și, în cazul în care există, numărul de telefon, numărul de fax și adresa de poștă electronică ale acestuia la care poate fi efectiv contactat, pentru a-i permite consumatorului să ia rapid legătura cu profesionistul și să comunice cu acesta în mod eficient și, dacă este cazul, adresa poștală și identitatea profesionistului în numele căruia acționează;

d) în cazul în care este diferită de adresa furnizată în conformitate cu lit. c), adresa poștală a locului în care profesionistul își desfășoară activitatea și, după caz, adresa poștală a profesionistului în numele căruia acționează, la care consumatorul poate trimite eventualele reclamații;

e) prețul total al produselor și serviciilor cu toate taxele incluse sau, în cazul în care prețul nu poate fi calculat dinainte în mod rezonabil dată fiind natura produselor sau a serviciilor, modalitatea de calcul al prețului și, după caz, toate costurile suplimentare de transport, de livrare, taxele poștale sau de orice altă natură sau, în cazul în care acestea nu pot fi calculate dinainte în mod rezonabil, menționarea faptului că aceste costuri suplimentare ar putea fi suportate de consumator, inclusiv perioada de valabilitate a ofertei sau a prețurilor. În cazul serviciilor de acces și conectare la rețele publice de comunicații electronice ori de servicii de comunicații electronice destinate publicului se vor menționa contravaloarea planului tarifar, cu precizarea numărului de minute, a creditului sau a traficului de date inclus, precum și a condițiilor de utilizare a acestora, dacă este cazul, extraopțiunile disponibile și contravaloarea acestora, tarifele pentru apeluri și pentru minutele ori traficul de date suplimentar, după

caz, tariful de conectare sau instalare, cu toate taxele incluse. În cazul unui contract pe durată nedeterminată sau al unui contract care include un abonament, prețul total va include costurile totale pe perioada de facturare. În cazul în care aceste contracte sunt taxate la un tarif fix, prețul total va cuprinde și costurile lunare totale. În cazul în care costul total nu poate fi calculat dinainte trebuie indicat modul în care se calculează prețul;

f) costul de utilizare a mijloacelor de comunicare la distanță în vederea încheierii contractului, atunci când este calculat pe baza unui alt tarif decât tariful de bază;

g) modalitățile de plată, livrare, executare, data până la care profesionistul se angajează să livreze produsele sau să presteze serviciile și, după caz, procedura profesionistului de soluționare a reclamațiilor;

h) în cazul în care există un drept de retragere, condițiile, termenele și procedurile de exercitare a dreptului respectiv, în conformitate cu art. 11 [alin. \(1\)](#), precum și formularul tipizat de retragere, prezentat în partea B din anexă;

i) acolo unde este cazul, informația potrivit căreia consumatorul va trebui să suporte costul aferent returnării produselor în caz de retragere și, pentru contractele la distanță, dacă produsele, prin însăși natura lor, nu pot fi, în mod normal, returnate prin poștă, costul aferent returnării produselor;

j) în cazul în care consumatorul își exercită dreptul de retragere după formularea unei cereri în conformitate cu art. 7 [alin. \(3\)](#) sau cu art. 8 [alin. \(8\)](#), informația potrivit căreia consumatorul este obligat să achite profesionistului costuri rezonabile, în conformitate cu art. 14 [alin. \(3\)](#);

k) în cazul în care dreptul de retragere nu este prevăzut în conformitate cu [art. 16](#), informația conform căreia consumatorul nu va beneficia de un drept de retragere sau, după caz, circumstanțele în care consumatorul își pierde dreptul de retragere;

l) o mențiune referitoare la existența unei garanții legale privind conformitatea produselor;

m) acolo unde este cazul, existența și condițiile de asistență după vânzare acordată consumatorului, serviciile prestate după vânzare și garanțiile comerciale;

n) existența codurilor de conduită relevante, astfel cum sunt definite în art. 2 [lit. f\)](#) din Legea nr. 363/2007 privind combaterea practicilor incorecte ale comercianților în relația cu consumatorii și armonizarea reglementărilor cu legislația europeană privind protecția consumatorilor, cu modificările ulterioare, și modalitatea în care pot fi obținute copii ale acestora, după caz;

o) durata contractului, după caz, sau, dacă contractul este încheiat pe durată nedeterminată sau urmează să fie prelungit în mod automat, condițiile de încetare a contractului, inclusiv penalitățile aplicabile, dacă este cazul;

p) acolo unde este cazul, durata minimă de valabilitate a obligațiilor care îi revin consumatorului conform contractului;

q) acolo unde este cazul, existența și condițiile aferente avansurilor sau altor garanții financiare care trebuie plătite sau oferite de consumator la cererea profesionistului;

r) acolo unde este cazul, funcționalitatea, inclusiv aplicarea unor măsuri tehnice de protecție pentru conținutul digital;

s) acolo unde este cazul, orice interoperabilitate relevantă a conținutului digital cu componentele hardware și software de care profesionistul are cunoștință sau se așteaptă în mod rezonabil să aibă cunoștință;

t) acolo unde este cazul, posibilitatea și modalitatea de a recurge la un mecanism extrajudiciar de depunere și soluționare a reclamațiilor cărui i se supune profesionistul.

(2) Alin. (1) se aplică și contractelor de furnizare a apei, gazelor naturale sau energiei electrice atunci când acestea nu sunt puse în vânzare într-un volum limitat sau cantitate fixă, a energiei termice și a conținuturilor digitale care nu sunt livrate pe un suport material.

(3) În cazul unei licitații, informațiile menționate la alin. (1) [lit. b\)](#), [c\)](#) și [d\)](#) pot fi înlocuite cu datele echivalente privind adjudecătorul.

(4) Informațiile menționate la alin. (1) [lit. h\)](#), [i\)](#) și [j\)](#) pot fi furnizate utilizând formularul tipizat de informare cu privire la retragere prevăzut la partea A din anexa care face parte integrantă din prezenta ordonanță de urgență. Profesionistul respectă cerințele în materie de informare stabilite la alin. (1) [lit. h\)](#), [i\)](#) și [j\)](#) dacă a furnizat consumatorului aceste instrucțiuni corect completate.

(5) Informațiile menționate la [alin. \(1\)](#) fac parte integrantă din contractul la distanță sau din contractul în afara spațiilor comerciale și nu pot fi modificate decât în cazul în care părțile contractante decid altfel în mod explicit.

(6) În cazul în care profesionistul nu îndeplinește cerințele în materie de informare cu privire la costuri suplimentare, conform celor menționate la alin. (1) [lit. e\)](#), sau la costurile aferente returnării produselor, conform celor menționate la alin. (1) [lit. i\)](#), consumatorul nu suportă respectivele costuri.

(7) Informațiile contractuale se prezintă în limba română într-o formă accesibilă, astfel încât acestea să fie înțelese cu ușurință de consumator, fără a exclude prezentarea acestora și în alte limbi.

(8) Cerințele în materie de informare prevăzute în prezenta ordonanță de urgență completează cerințele de informare cuprinse în Ordonanța de urgență a Guvernului [nr. 49/2009](#) privind libertatea de stabilire a prestatorilor de servicii și libertatea de a furniza servicii în România, aprobată cu modificări și completări prin Legea [nr. 68/2010](#), și în Legea [nr. 365/2002](#) privind comerțul electronic, republicată, cu modificările ulterioare.

(9) Fără a aduce atingere alin. (8), dacă o dispoziție cu privire la conținutul și modul în care trebuie furnizate informațiile din cadrul Ordonanței de urgență a Guvernului [nr. 49/2009](#), aprobată cu modificări prin Legea [nr. 68/2010](#), respectiv din cadrul Legii [nr. 365/2002](#), republicată, cu modificările ulterioare, contravine unei dispoziții din prezenta ordonanță de urgență, prevalează dispozițiile prezentei ordonanțe de urgență.

(10) Sarcina probei în ceea ce privește îndeplinirea cerințelor în materie de informare stabilite în prezentul capitol revine profesionistului.

ARTICOLUL 7 Condiții de formă pentru contractele în afara spațiilor comerciale (1) În cazul contractelor în afara spațiilor comerciale, profesionistul transmite informațiile prevăzute la art. 6 [alin. \(1\)](#) consumatorului pe suport hârtie sau, în cazul în care consumatorul este de acord, pe un alt suport durabil. Aceste informații sunt lizibile și redactate într-un limbaj simplu și inteligibil.

(2) Profesionistul furnizează consumatorului un exemplar original al contractului semnat sau confirmarea contractului pe suport hârtie sau, dacă consumatorul este de acord, pe un alt suport

durabil, inclusiv, dacă este cazul, confirmarea acordului prealabil expres al consumatorului în conformitate cu art. 16 [lit. m](#)).

(3) În cazul în care consumatorul dorește ca prestarea unor servicii sau furnizarea de apă, gaze naturale, energie electrică, atunci când acestea nu sunt puse în vânzare într-un volum limitat sau cantitate fixă, sau de energie termică să înceapă în timpul perioadei de retragere de 14 zile, profesionistul solicită consumatorului să formuleze o astfel de cerere expresă pe un suport durabil.

(4) În cazul contractelor în afara spațiilor comerciale, unde consumatorul a solicitat expres serviciile profesionistului pentru a efectua lucrări de reparație sau de întreținere, iar profesionistul și consumatorul își îndeplinesc imediat obligațiile contractuale care le revin, iar suma care trebuie plătită de consumator nu depășește echivalentul a 200 euro la cursul Băncii Naționale a României din ziua respectivă:

a) profesionistul furnizează consumatorului informațiile menționate la art. 6 alin. (1) [lit. b](#) și [c](#) și informații referitoare la preț sau la maniera de calculare a prețului, împreună cu o estimare a costului total, pe suport hârtie sau, dacă consumatorul este de acord, pe un alt suport durabil; profesionistul furnizează informațiile menționate la art. 6 alin. (1) [lit. a](#), [h](#) și [k](#), dar poate opta să nu le furnizeze pe suport hârtie sau pe un alt suport durabil dacă consumatorul își dă acordul expres;

b) confirmarea contractului furnizată în conformitate cu [alin. \(2\)](#) din prezentul articol conține informațiile menționate la art. 6 [alin. \(1\)](#).

ARTICOLUL 8 Condiții de formă pentru contractele la distanță (1) În cazul contractelor la distanță, profesionistul transmite informațiile prevăzute la art. 6 [alin. \(1\)](#) sau pune la dispoziția consumatorului respectivele informații într-un mod adecvat mijlocului de comunicare la distanță utilizat, folosind un limbaj simplu și inteligibil. În măsura în care respectiva informație este prezentată pe un suport durabil, aceasta trebuie să fie lizibilă.

(2) Dacă un contract la distanță care urmează să fie încheiat prin mijloace electronice obligă consumatorul să plătească, profesionistul aduce la cunoștința consumatorului de o manieră clară și foarte vizibilă, în mod direct, înainte ca acesta să facă comanda, informațiile prevăzute la art. 6 alin. (1) [lit. a](#), [e](#), [o](#) și [p](#)). Profesionistul se asigură că, atunci când consumatorul face comanda, acesta din urmă recunoaște în mod explicit că această comandă implică o obligație de a plăti. Dacă pentru a face comanda este necesar să se activeze un buton sau o funcție similară, butonul sau funcția similară este etichetat/tă de o manieră lizibilă doar cu mențiunea "comandă ce implică o obligație de plată" sau o formulare neambiguă corespunzătoare, care să indice că a face comanda implică obligația de a plăti profesionistului. Dacă profesionistul încalcă prevederile prezentului alineat, consumatorul nu are nicio obligație în temeiul contractului sau al comenzii.

(3) Site-urile comerciale indică clar și lizibil, cel mai târziu la începutul procesului de formulare a comenzii, dacă se aplică vreo restricție în ceea ce privește livrarea și care sunt mijloacele de plată acceptate.

(4) În cazul în care contractul este încheiat printr-un mijloc de comunicare la distanță ce permite un spațiu sau un timp limitat pentru afișarea informației, profesionistul furnizează prin mijlocul de comunicare respectiv, înaintea încheierii contractului, cel puțin informațiile precontractuale referitoare la principalele caracteristici ale produsului sau serviciului, identitatea profesionistului, prețul total,

dreptul la retragere, durata contractului și, în cazul contractelor pe durată nedeterminată, modalitățile de încetare a contractului, prevăzute la art. 6 alin. (1) [lit. a\)](#), [b\)](#), [e\)](#), [h\)](#) și [o\)](#). Celelalte informații menționate la art. 6 [alin. \(1\)](#) sunt furnizate consumatorului de profesionist într-un mod adecvat, în conformitate cu alin. (1) din prezentul articol.

(5) Fără a aduce atingere alin. (4), în cazul în care profesionistul apelează telefonic consumatorul în vederea încheierii unui contract la distanță, profesionistul își declină identitatea la începutul conversației cu consumatorul și, dacă este cazul, declină identitatea persoanei în numele căreia a efectuat apelul telefonic și specifică scopul comercial al apelului.

(6) În cazul în care urmează să se încheie un contract la distanță prin intermediul telefonului, profesionistul trebuie să confirme oferta consumatorului, al cărui angajament începe doar după ce acesta a semnat oferta sau după ce și-a trimis consimțământul scris. Aceste confirmări trebuie făcute pe un suport durabil.

(7) Profesionistul transmite consumatorului confirmarea încheierii contractului, pe un suport durabil, într-un termen rezonabil din momentul încheierii contractului la distanță și cel târziu la momentul livrării produselor sau înainte de începerea prestării serviciului solicitat. Respectiva confirmare include:

a) toate informațiile menționate la art. 6 [alin. \(1\)](#), cu excepția cazului în care profesionistul a transmis deja informațiile respective consumatorului, pe un suport durabil, înaintea încheierii contractului la distanță;

b) acolo unde este cazul, confirmarea acordului prealabil expres al consumatorului și acordul în conformitate cu art. 16 [lit. m\)](#).

(8) În cazul în care consumatorul dorește ca prestarea unor servicii sau furnizarea de apă, gaze naturale, energie electrică, atunci când acestea nu sunt puse în vânzare într-un volum limitat ori cantitate fixă, sau de energie termică să înceapă în timpul perioadei de retragere de 14 zile, profesionistul solicită consumatorului să facă o cerere expresă în acest sens.

(9) Momentul încheierii contractului la distanță îl constituie momentul confirmării, pe un suport durabil, de către profesionist a acceptării comenzii transmise de consumator.

(10) Prezentul articol nu aduce atingere dispozițiilor privind încheierea prin mijloace electronice a contractelor și comenzile prin internet, astfel cum sunt stabilite la [art. 7](#) și [9](#) din [Legea nr. 365/2002](#), republicată, cu modificările ulterioare.

ARTICOLUL 9 Dreptul de retragere (1) Cu excepția cazurilor prevăzute la [art. 16](#), consumatorul beneficiază de o perioadă de 14 zile pentru a se retrage dintr-un contract la distanță sau dintr-un contract în afara spațiilor comerciale, fără a fi nevoit să justifice decizia de retragere și fără a suporta alte costuri decât cele prevăzute la art. 13 [alin. \(3\)](#) și la [art. 14](#).

(2) Fără a aduce atingere [art. 10](#), perioada de retragere menționată la alin. (1) expiră în termen de 14 zile de la:

a) data încheierii contractului, în cazul contractelor de prestări de servicii;

b) ziua în care consumatorul sau o parte terță, alta decât transportatorul și care este indicată de consumator, intră în posesia fizică a produselor, în cazul contractelor de vânzare, sau:

(i) în cazul în care consumatorul comandă printr-o singură comandă produse multiple care vor fi livrate separat, ziua în care consumatorul sau o parte terță, alta decât transportatorul și care este indicată de consumator, intră în posesia fizică a ultimului produs;

(ii) în cazul livrării unui produs care constă din mai multe loturi sau piese, ziua în care consumatorul sau o parte terță, alta decât transportatorul și care este indicată de consumator, intră în posesia fizică a ultimului produs sau a ultimei piese;

(iii) în cazul contractelor pentru livrarea periodică de produse pe o perioadă de timp determinată, ziua în care consumatorul sau o parte terță, alta decât transportatorul și care este indicată de consumator, intră în posesia fizică a primului produs;

c) în cazul contractelor pentru furnizarea de apă, gaze naturale, energie electrică, atunci când acestea nu prevăd vânzarea într-un volum limitat sau cantitate stabilită, de energie termică sau de conținuturi digitale care nu sunt livrate pe un suport material, data încheierii contractului.

(3) Părțile contractante își îndeplinesc obligațiile contractuale pe parcursul perioadei de retragere conform prevederilor prezentei ordonanțe de urgență.

ARTICOLUL 10 Omisiunea informațiilor privind dreptul de retragere (1) În cazul în care profesionistul nu a transmis consumatorului informațiile privind dreptul de retragere conform art. 6 alin. (1) [lit. h](#)), perioada de retragere expiră la 12 luni de la sfârșitul perioadei inițiale de retragere de 14 zile.

(2) În cazul în care profesionistul a transmis consumatorului informațiile prevăzute la alin. (1) din prezentul articol în termen de 12 luni de la data menționată la art. 9 [alin. \(2\)](#), perioada de retragere expiră în 14 zile de la data la care consumatorul primește informațiile respective.

ARTICOLUL 11 Exercițarea dreptului de retragere (1) Înainte de expirarea perioadei de retragere, consumatorul informează profesionistul cu privire la decizia sa de retragere din contract. În acest scop, consumatorul poate alege una dintre următoarele variante:

a) de a folosi modelul de formular de retragere prevăzut în partea B din anexă;

b) de a face orice altă declarație neechivocă în care își exprimă decizia de retragere din contract.

(2) Consumatorul și-a exercitat dreptul de retragere în perioada de retragere menționată la art. 9 [alin. \(2\)](#) și la [art. 10](#) în cazul în care comunicarea cu privire la exercițarea dreptului de retragere este transmisă de către consumator înaintea expirării perioadei respective.

(3) Profesionistul poate, în plus față de posibilitățile menționate la [alin. \(1\)](#), să acorde consumatorului opțiunea de a completa și de a transmite în format electronic, pe site-ul profesionistului, fie modelul de formular de retragere prevăzut în partea B din anexă, fie o declarație neechivocă de orice alt tip. În aceste cazuri, profesionistul comunică consumatorului, fără întârziere, pe un suport durabil, confirmarea de primire a formularului de retragere.

(4) Sarcina probei privind exercițarea dreptului de retragere în conformitate cu dispozițiile din prezentul articol revine consumatorului.

ARTICOLUL 12 Efectele retragerii Exercițarea dreptului de retragere pune capăt obligațiilor părților contractuale, după caz:

a) de a executa contractul la distanță sau contractul în afara spațiului comercial;

b) de a încheia un contract la distanță sau în afara spațiului comercial, în cazul în care consumatorul a efectuat o comandă.

ARTICOLUL 13 Obligațiile care revin profesionistului în cazul retragerii (1) Profesionistul rambursează toate sumele pe care le-a primit drept plată din partea consumatorului, inclusiv, după caz, costurile livrării, fără întârziere nejustificată și, în orice caz, nu mai târziu de 14 zile de la data la care este informat de decizia de retragere din contract a consumatorului în conformitate cu [art. 11](#).

(2) Profesionistul rambursează sumele menționate la alin. (1) folosind aceleași modalități de plată ca și cele folosite de consumator pentru tranzacția inițială, cu excepția cazului în care consumatorul a fost de acord cu o altă modalitate de plată și cu condiția de a nu cădea în sarcina consumatorului plata de comisioane în urma rambursării.

(3) Fără a aduce atingere [alin. \(1\)](#), profesionistul nu este obligat să ramburseze costurile suplimentare în cazul în care consumatorul a ales în mod explicit un alt tip de livrare decât livrarea standard oferită de profesionist.

(4) Cu excepția cazului în care profesionistul s-a oferit să recupereze el însuși produsele, în cazul contractelor de vânzare, profesionistul poate amâna rambursarea până la data recepționării produselor care au făcut obiectul vânzării sau până la momentul primirii unei dovezi din partea consumatorului conform căreia acesta a trimis produsele către profesionist, luându-se în considerare data cea mai apropiată.

ARTICOLUL 14 Obligațiile consumatorului în cazul retragerii (1) Cu excepția cazului în care profesionistul s-a oferit să recupereze el însuși produsele, consumatorul returnează produsele sau le înmânează profesionistului sau unei persoane autorizate de profesionist să recepționeze produsele, fără întârziere nejustificată și în decurs de cel mult 14 zile de la data la care acesta a comunicat profesionistului decizia sa de retragere din contract în conformitate cu [art. 11](#). Termenul este respectat dacă produsele sunt trimise înapoi de consumator înainte de expirarea perioadei de 14 zile.

(2) Consumatorul suportă doar costurile directe legate de returnarea produselor, cu excepția cazului în care profesionistul acceptă să suporte acele costuri sau în care profesionistul nu a informat consumatorul că aceste costuri trebuie suportate de consumator. În cazul contractelor în afara spațiilor comerciale, în cazul cărora produsele au fost livrate la domiciliul consumatorului la momentul încheierii contractului, profesionistul preia produsele pe cheltuiala sa dacă produsele, prin natura lor, nu pot fi returnate în mod normal prin poștă.

(3) Consumatorul este responsabil doar în ceea ce privește diminuarea valorii produselor rezultată din manipularea acestora, diferit de ceea ce este necesar pentru determinarea naturii, caracteristicilor și funcționării produselor. Diminuarea valorii produselor nu trebuie să fie descurajantă pentru consumator în a-și exercita dreptul de retragere. Indiferent de situație, consumatorul nu este responsabil pentru diminuarea valorii produselor în cazul în care profesionistul a omis să îl informeze cu privire la dreptul de retragere în conformitate cu art. 6 alin. (1) [lit. h](#).

(4) Profesionistul trebuie să poată face dovada diminuării valorii produselor care rezultă diferit de ceea ce este necesar pentru determinarea naturii, caracteristicilor și funcționării produselor.

(5) Atunci când consumatorul își exercită dreptul de retragere după transmiterea cererii în conformitate cu art. 7 [alin. \(3\)](#) sau cu art. 8 [alin. \(8\)](#), consumatorul plătește profesionistului o sumă proporțională cu ceea ce s-a furnizat până la momentul în care consumatorul a informat profesionistul cu privire la exercitarea dreptului de retragere, în raport cu acoperirea totală a contractului. Suma

proporțională care trebuie plătită profesionistului de către consumator este calculată pe baza prețului total convenit în contract. Dacă prețul total este excesiv, suma proporțională este calculată pe baza valorii de piață a ceea ce s-a furnizat.

(6) Consumatorul nu suportă costurile pentru:

a) prestarea serviciilor sau furnizarea de apă, gaze naturale sau energie electrică, atunci când acestea nu sunt puse în vânzare într-un volum limitat sau cantitate prestabilită, sau energie termică furnizată, în totalitate sau parțial, în cursul perioadei de retragere, în una dintre următoarele situații:

(i) profesionistul nu a furnizat informații în conformitate cu art. 6 alin. (1) [lit. h](#)) sau [i](#));

(ii) consumatorul nu a cerut expres ca prestarea să înceapă în timpul perioadei de retragere în conformitate cu art. 7 [alin. \(3\)](#) și cu art. 8 [alin. \(8\)](#);

b) furnizarea, în totalitate sau parțial, de conținut digital care nu este livrat pe un suport material, în una dintre următoarele situații:

(i) consumatorul nu și-a dat acordul prealabil expres cu privire la începerea prestării înainte de sfârșitul perioadei de 14 zile menționate la [art. 9](#);

(ii) consumatorul nu a confirmat că a luat cunoștință de faptul că își pierde dreptul de retragere în momentul în care își dă consimțământul;

(iii) profesionistul nu a furnizat confirmarea în conformitate cu art. 7 [alin. \(2\)](#) sau cu art. 8 [alin. \(7\)](#).

(7) Cu excepția celor prevăzute la art. 13 [alin. \(3\)](#) și la prezentul articol, exercitarea dreptului de retragere nu atrage răspunderea consumatorului.

ARTICOLUL 15 Efectele exercitării dreptului de retragere asupra contractelor auxiliare Fără a aduce atingere [art. 63-65](#) din Ordonanța de urgență a Guvernului [nr. 50/2010](#) privind contractele de credit pentru consumatori, aprobată cu modificări și completări prin Legea [nr. 288/2010](#), cu modificările ulterioare, în cazul în care consumatorul exercită dreptul său de retragere din cadrul unui contract la distanță sau al unui contract în afara spațiilor comerciale în conformitate cu [art. 9-14](#) din prezenta ordonanță de urgență, orice contract auxiliar încetează în mod automat, fără costuri pentru consumator, cu excepția celor prevăzute la art. 13 [alin. \(3\)](#) și la [art. 14](#) din prezenta ordonanță de urgență.

ARTICOLUL 16 Excepții de la dreptul de retragere Sunt exceptate de la dreptul de retragere prevăzut la [art. 9-15](#) în ceea ce privește contractele la distanță și contractele în afara spațiilor comerciale următoarele:

a) contractele de prestări de servicii, după prestarea completă a serviciilor, dacă executarea a început cu acordul prealabil expres al consumatorului și după ce acesta a confirmat că a luat cunoștință de faptul că își va pierde dreptul la retragere după executarea completă a contractului de către profesionist;

b) furnizarea de produse sau servicii al căror preț depinde de fluctuațiile de pe piața financiară pe care profesionistul nu le poate controla și care pot avea loc pe parcursul perioadei de retragere;

c) furnizarea de produse confecționate după specificațiile prezentate de consumator sau personalizate în mod clar;

d) furnizarea de produse care sunt susceptibile a se deteriora sau a expira rapid;

- e) furnizarea de produse sigilate care nu pot fi returnate din motive de protecție a sănătății sau din motive de igienă și care au fost desigilate de consumator;
- f) furnizarea de produse care sunt, după livrare, potrivit naturii acestora, inseparabil amestecate cu alte elemente;
- g) furnizarea de băuturi alcoolice al căror preț a fost convenit în momentul încheierii contractului de vânzare, a căror livrare nu poate fi efectuată înainte de 30 de zile și a căror valoare reală depinde de fluctuațiile de pe piață pe care profesionistul nu le poate controla;
- h) contractele în cazul cărora consumatorul a solicitat în mod special profesionistului să se deplaseze la domiciliul său pentru a efectua lucrări urgente de reparație sau de întreținere. Dacă, cu ocazia unei astfel de vizite, profesionistul prestează alte servicii în afara celor solicitate în mod expres de consumator sau furnizează alte produse decât piesele de schimb indispensabile pentru executarea lucrărilor de întreținere sau de reparație, dreptul de retragere se aplică respectivelor servicii sau produse suplimentare;
- i) furnizarea de înregistrări audio sau video sigilate sau de programe informatice sigilate care au fost desigilate după livrare;
- j) furnizarea de ziare, periodice și reviste, cu excepția contractelor de abonament pentru furnizarea de astfel de publicații;
- k) contractele încheiate în cadrul unei licitații;
- l) prestarea de servicii de cazare, pentru alt scop decât cel rezidențial, transport de mărfuri, închiriere de mașini, catering sau serviciile privind activitățile de agrement, în cazul în care contractul prevede o dată sau o perioadă de executare specifică;
- m) furnizarea de conținut digital care nu este livrat pe un suport material, dacă prestarea a început cu acordul prealabil expres al consumatorului și după ce acesta a confirmat că a luat cunoștință de faptul că își va pierde dreptul la retragere.

CAPITOLUL IV

Alte drepturi ale consumatorilor

ARTICOLUL 17 Domeniul de aplicare (1) [Art. 18](#) și [20](#) se aplică în cazul contractelor de vânzare, cu excepția contractelor de furnizare a apei, gazelor naturale sau energiei electrice, atunci când acestea nu sunt puse în vânzare într-un volum limitat sau într-o cantitate fixă, precum și a contractelor de furnizare a energiei termice și a conținutului digital care nu este livrat pe un suport material.

(2) [Art. 21](#) și [22](#) se aplică și contractelor de vânzare și de prestări de servicii și contractelor de furnizare de apă, gaze naturale, energie electrică, energie termică sau conținut digital.

ARTICOLUL 18 Livrare (1) Cu excepția cazului în care părțile au convenit altfel cu privire la momentul livrării, profesionistul livrează produsele transferând posesia fizică sau controlul asupra produselor către consumator, fără întârziere nejustificată și, în orice caz, în decurs de cel mult 30 de zile de la încheierea contractului.

(2) În cazul în care profesionistul nu și-a îndeplinit obligația de a livra produsele în momentul convenit cu consumatorul sau în termenul stabilit la alin. (1), consumatorul îi solicită să efectueze livrarea într-un

termen suplimentar, corespunzător circumstanțelor. În cazul în care profesionistul nu livrează produsele în termenul suplimentar respectiv, consumatorul are dreptul, după caz, la rezoluțiunea sau rezilierea contractului.

(3) [Alineatul \(2\)](#) nu se aplică contractelor de vânzare în cazul în care profesionistul a refuzat să livreze produsele sau în cazul în care livrarea în termenul convenit este esențială având în vedere toate circumstanțele existente la încheierea contractului sau în cazul în care consumatorul informează profesionistul, înainte de încheierea contractului, că livrarea înainte de sau la o dată precizată este esențială. În aceste cazuri, dacă profesionistul nu livrează produsele în momentul convenit cu consumatorul sau în termenul stabilit la [alin. \(1\)](#), consumatorul are dreptul, după caz, la rezoluțiunea sau rezilierea contractului.

(4) Prin excepție de la prevederile [art. 1549-1554](#) din Legea nr. 287/2009 privind [Codul civil](#), republicată, cu modificările ulterioare, la rezoluțiunea sau, după caz, la rezilierea contractului, profesionistul rambursează fără întârzieri nejustificate toate sumele plătite în temeiul contractului de către consumator și în decurs de cel mult 7 zile de la data la care consumatorul a comunicat profesionistului decizia sa de terminare a contractului.

(5) În plus față de rezoluțiunea sau rezilierea contractului în conformitate cu [alin. \(2\)](#), consumatorul poate recurge la alte căi de atac prevăzute de legislația în vigoare.

ARTICOLUL 19 Comisioane pentru folosirea unor mijloace de plată [Abrogat\(ă\)](#)

ARTICOLUL 20 Transferarea riscului În cazul contractelor în care profesionistul livrează produsele către consumator, riscul de pierdere sau de deteriorare a produselor este transferat consumatorului în momentul în care acesta sau o parte terță desemnată de acesta, alta decât transportatorul, intră în posesia fizică a produselor. Cu toate acestea, riscul este transferat consumatorului în momentul livrării produselor către transportator, dacă transportatorul a fost însărcinat de către consumator să transporte produsele, iar această opțiune nu a fost oferită de către profesionist, fără a aduce atingere drepturilor consumatorului față de transportator.

ARTICOLUL 21 Comunicarea prin telefon (1) În cazul în care un profesionist operează o linie telefonică pentru a putea fi contactat prin telefon cu privire la contractul încheiat, consumatorul nu este obligat să plătească, la contactarea profesionistului, mai mult decât tariful de bază.

(2) Alineatul (1) nu aduce atingere dreptului furnizorilor de servicii de comunicații electronice de a taxa aceste apeluri.

ARTICOLUL 22 Plăți suplimentare Înainte ca un consumator să încheie un contract sau să accepte o ofertă, profesionistul solicită consimțământul explicit din partea consumatorului cu privire la orice plată suplimentară față de prețul stabilit anterior pentru obligația contractuală principală a profesionistului. În cazul în care profesionistul nu a obținut consimțământul expres al consumatorului, însă l-a dedus utilizând opțiuni incluse în mod automat pe care consumatorul trebuie să le respingă pentru a evita plata suplimentară, consumatorul poate pretinde rambursarea acestei plăți.

CAPITOLUL V Dispoziții generale

ARTICOLUL 23 Vânzarea nesolicitată Consumatorul este scutit de obligația de plată în caz de furnizare nesolicitată de produse, apă, gaze naturale, electricitate, energie termică sau conținut digital sau în caz de prestare nesolicitată de servicii interzise prin art. 4 [alin. \(4\)](#) și prin anexa [nr. 1](#) - Practici comerciale agresive, punctul 6, din Legea [nr. 363/2007](#) privind combaterea practicilor comerciale incorecte ale comercianților în relația cu consumatorii și armonizarea reglementărilor cu legislația europeană privind protecția consumatorilor, cu modificările ulterioare. În asemenea cazuri, absența unui răspuns din partea consumatorului în urma unei astfel de furnizări sau prestări nesolicitate nu reprezintă un consimțământ.

ARTICOLUL 24 Termene (1) Toate termenele incluse în prezenta ordonanță de urgență se interpretează drept termene exprimate în zile calendaristice.

(2) Dacă un termen exprimat în zile se calculează din momentul în care intervine un eveniment sau se realizează un act, ziua în cursul căreia a avut loc acest eveniment sau se realizează acest act nu se ia în seamă la calculul termenului, cu excepția cazului în care prezenta ordonanță de urgență prevede altfel.

(3) În cazul în care ultima zi a termenului este o zi nelucrătoare, profesionistul prelungește termenul în mod corespunzător.

ARTICOLUL 25 Caracterul imperativ al legii (1) Dacă legea aplicabilă contractului este cea a unui stat membru al Uniunii Europene, consumatorii nu pot renunța la drepturile care le sunt conferite prin prezenta ordonanță de urgență.

(2) Orice clauză contractuală prin care se renunță sau se restrâng în mod direct sau indirect drepturile prevăzute de prezenta ordonanță de urgență nu este obligatorie pentru consumator.

ARTICOLUL 26 Informare Autoritatea Națională pentru Protecția Consumatorilor va întreprinde măsurile necesare pentru informarea consumatorilor și a profesioniștilor cu privire la dispozițiile prezentei ordonanțe de urgență și, după caz, încurajează profesioniștii și responsabilii de cod, astfel cum sunt definiți la art. 2 [lit. g](#)) din Legea nr. 363/2007 privind combaterea practicilor incorecte ale comercianților în relația cu consumatorii și armonizarea reglementărilor cu legislația europeană privind protecția consumatorilor, cu modificările ulterioare, să informeze consumatorii cu privire la codurile lor de conduită.

CAPITOLUL VI

Competență, sesizare și control

ARTICOLUL 27 Sesizare (1) În vederea asigurării respectării prevederilor prezentei ordonanțe de urgență de către profesioniști, persoanele fizice sau organizațiile care, potrivit legii, au un interes legitim, inclusiv organizațiile de consumatori sau organizațiile profesionale, pot fie să sesizeze Autoritatea Națională pentru Protecția Consumatorilor ori Autoritatea Națională pentru Administrare și Reglementare în Comunicații în legătură cu încălcările prevederilor prezentei ordonanțe de urgență astfel ca aceasta să decidă asupra reclamațiilor, fie să inițieze acțiuni în justiție împotriva profesioniștilor care au săvârșit sau sunt susceptibili să săvârșescă încălcări ale prezentei ordonanțe de urgență.

(2) Profesioniștii concurenți pot informa Autoritatea Națională pentru Protecția Consumatorilor sau Autoritatea Națională pentru Administrare și Reglementare în Comunicații în legătură cu încălcarea prevederilor prezentei ordonanțe de urgență.

ARTICOLUL 28 Sancțiuni (1) Competența constatării contravențiilor și aplicării sancțiunilor revine Autorității Naționale pentru Protecția Consumatorilor și Autorității Naționale pentru Administrare și Reglementare în Comunicații.

(2) În sensul alin. (1), autoritățile administrative competente pot fi sesizate, pot constata și aplica sancțiuni după cum urmează:

a) Autoritatea Națională pentru Protecția Consumatorilor, prin reprezentanții împuterniciți, în cazul contravențiilor prevăzute la [alin. \(5\)](#), inclusiv atunci când acestea constau în fapte care vizează contractele încheiate de consumatori pentru a beneficia de servicii de acces și conectare la rețele publice de comunicații electronice ori de servicii de comunicații electronice destinate publicului;

b) Autoritatea Națională pentru Administrare și Reglementare în Comunicații, prin reprezentanții împuterniciți, în cazul contravențiilor prevăzute la alin. (5) [lit. e\) -k\)](#), [m\) -u\)](#) și [w\) -y\)](#), atunci când acestea constau în fapte care vizează contractele încheiate de consumatori pentru a beneficia de servicii de acces și conectare la rețele publice de comunicații electronice ori de servicii de comunicații electronice destinate publicului.

(3) Dispozițiile [art. 137](#), [138](#) și art. 141 [alin. \(1\)](#) și alin. (2) [lit. b\)](#) și [f\)](#), [art. 144](#), [146](#), 147 [lit. a\)](#), [art. 149](#) și [151](#) din cadrul Ordonanței de urgență a Guvernului [nr. 111/2011](#) privind comunicațiile electronice, aprobată cu modificări și completări prin Legea [nr. 140/2012](#), se aplică în mod corespunzător contravențiilor constatate de Autoritatea Națională pentru Administrare și Reglementare în Comunicații ca urmare a încălcării dispozițiilor prezentei ordonanțe de urgență.

(4) În vederea exercitării atribuțiilor prevăzute de prezenta ordonanță de urgență, Autoritatea Națională pentru Administrare și Reglementare în Comunicații poate solicita furnizorilor informații, în conformitate cu dispozițiile [art. 120](#) din Ordonanța de urgență a Guvernului nr. 111/2011, aprobată cu modificări și completări prin Legea [nr. 140/2012](#).

(5) Constituie contravenții următoarele fapte:

a) nerespectarea cerinței de a furniza informații într-un mod vizibil, lizibil și ușor de înțeles, conform părții introductive a art. 4 [alin. \(1\)](#), se sancționează cu amendă de la 2.000 lei la 5.000 lei;

b) nerespectarea cerințelor de informații precontractuale prevăzute la art. 4 alin. (1) [lit. a\) -j\)](#) se sancționează cu amendă de la 2.000 lei la 5.000 lei;

c) nerespectarea cerinței de a include informațiile precontractuale și în cadrul contractelor de furnizare a apei, gazelor naturale sau energiei electrice, atunci când acestea nu sunt puse în vânzare într-un volum limitat sau cantitate fixă, a energiei termice sau a conținuturilor digitale care nu sunt livrate pe un suport material, conform art. 4 [alin. \(2\)](#), se sancționează cu amendă de la 2.000 lei la 5.000 lei;

d) nerespectarea cerinței de a include informațiile precontractuale în cadrul contractului, conform art. 4 [alin. \(4\)](#), se sancționează cu amendă de la 2.000 lei la 5.000 lei;

e) nerespectarea cerinței de a furniza informații într-un mod clar și inteligibil, conform părții introductive a art. 6 [alin. \(1\)](#), se sancționează cu amendă de la 2.000 lei la 5.000 lei;

- f) nerespectarea prevederilor art. 6 alin. (1) [lit. a](#) -t) referitoare la informațiile precontractuale se sancționează cu amendă de la 2.000 lei la 5.000 lei;
- g) nerespectarea prevederilor art. 6 [alin. \(4\)](#) referitoare la completarea corectă a instrucțiunilor prevăzute în formularul tipizat de informare cu privire la retragere prevăzut la partea A din anexă, atunci când acesta este utilizat, se sancționează cu amendă de la 2.000 lei la 5.000 lei;
- h) nerespectarea prevederilor art. 6 [alin. \(5\)](#) referitoare la includerea informațiilor precontractuale în cadrul contractului și la situația în care aceste informații pot fi modificate se sancționează cu amendă de la 1.000 lei la 4.000 lei;
- i) nerespectarea prevederilor art. 6 [alin. \(6\)](#) referitoare la situația în care profesionistul nu îndeplinește cerințele în materie de informare se sancționează cu amendă de la 1.000 lei la 4.000 lei;
- j) nerespectarea prevederilor art. 6 [alin. \(7\)](#) referitoare la prezentarea informațiilor în limba română într-o formă accesibilă, astfel încât acestea să fie înțelese cu ușurință de consumator, se sancționează cu amendă de la 1.000 lei la 4.000 lei;
- k) nerespectarea prevederilor art. 7 [alin. \(1\)](#) referitoare la informații, a prevederilor art. 7 [alin. \(2\)](#) referitoare la contract, precum și a prevederilor art. 7 [alin. \(3\)](#) referitoare la solicitarea cererii de începere a prestării unor servicii se sancționează cu amendă de la 2.000 lei la 5.000 lei;
- l) nerespectarea prevederilor art. 7 alin. (4) [lit. a](#) referitoare la informații, precum și a prevederilor art. 7 alin. (4) [lit. b](#) referitoare la informațiile menționate în confirmarea contractului se sancționează cu amendă de la 2.000 lei la 5.000 lei;
- m) nerespectarea prevederilor art. 8 [alin. \(1\) - \(7\)](#) referitoare la informații, precum și a prevederilor art. 8 [alin. \(8\)](#) referitoare la solicitarea de a se face o cerere expresă se sancționează cu amendă de la 1.000 lei la 4.000 lei;
- n) nerespectarea de către profesionist a prevederilor art. 9 [alin. \(1\) - \(2\)](#) referitoare la dreptul de retragere, precum și a prevederilor art. 9 [alin. \(3\)](#) referitoare la obligațiile contractuale pe parcursul perioadei de retragere se sancționează cu amendă de la 2.000 lei la 5.000 lei;
- o) nerespectarea dreptului de retragere în condițiile [art. 10](#) se sancționează cu amendă de la 2.000 lei la 4.000 lei;
- p) nerespectarea prevederilor art. 11 [alin. \(3\)](#) referitoare la confirmarea de primire a formularului de retragere se sancționează cu amendă de la 1.000 lei la 4.000 lei;
- q) nerespectarea prevederilor [art. 12](#) de a pune capăt obligațiilor părților contractuale în cazul exercitării dreptului de retragere se sancționează cu amendă de la 2.000 lei la 5.000 lei;
- r) nerespectarea prevederilor art. 13 [alin. \(1\) și \(2\)](#) referitoare la obligațiile care revin profesionistului în cazul retragerii, precum și ale art. 13 [alin. \(4\)](#) referitoare la amânarea rambursării se sancționează cu amendă de la 2.000 lei la 5.000 lei;
- s) nerespectarea obligațiilor impuse de [art. 14](#) în condițiile în care consumatorul și-a respectat obligațiile sale se sancționează cu amendă de la 1.000 lei la 4.000 lei;
- t) nerespectarea prevederilor [art. 15](#) referitoare la drepturile consumatorilor în situația exercitării dreptului de retragere din contractele auxiliare se sancționează cu amendă de la 1.000 lei la 4.000 lei;
- u) nerespectarea prevederilor [art. 18](#) referitoare la livrare se sancționează cu amendă de la 1.000 lei la 4.000 lei;

v) ~~Abrogat(ă)~~

w) nerespectarea prevederilor [art. 20](#) referitoare la riscul de pierdere sau de deteriorare a produselor se sancționează cu amendă de la 2.000 lei la 5.000 lei;

x) nerespectarea prevederilor [art. 21](#) referitoare la plata tarifului de bază în cazul comunicărilor telefonice se sancționează cu amendă de la 2.000 lei la 4.000 lei;

y) nerespectarea prevederilor [art. 22](#) referitoare la plăți suplimentare și ale art. 24 [alin. \(3\)](#) referitoare la termene se sancționează cu amendă de la 2.000 lei la 4.000 lei.

(6) Contravențiilor prevăzute la [alin. \(5\)](#) le sunt aplicabile dispozițiile Ordonanței Guvernului [nr. 2/2001](#) privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea [nr. 180/2002](#), cu modificările și completările ulterioare.

(7) Prin derogare de la prevederile art. 16 [alin. \(1\)](#) și ale art. 28 [alin. \(1\)](#) din Ordonanța Guvernului nr. 2/2001, aprobată cu modificări și completări prin Legea [nr. 180/2002](#), cu modificările și completările ulterioare, și ale art. 22 [alin. \(2\)](#) din Legea nr. 203/2018 privind măsuri de eficientizare a achitării amenzilor contravenționale, cu modificările ulterioare, în cazul sancțiunilor aplicate pentru săvârșirea contravențiilor prevăzute la [alin. \(5\) lit. e\) -k\), m\) -u\) și w\) -y\)](#), atunci când acestea sunt în competența Autorității Naționale pentru Administrare și Reglementare în Comunicații potrivit [alin. \(2\) lit. b\)](#), contravenientul poate achita, în termen de cel mult 15 zile de la data înmânării sau comunicării procesului-verbal de constatare a contravenției și de aplicare a sancțiunii, jumătate din cuantumul amenzii aplicate, agentul constatator făcând mențiuni despre această posibilitate în procesul-verbal.

CAPITOLUL VII

Dispoziții finale

ARTICOLUL 29 Modificarea și completarea unor acte normative (1) După [articolul 17](#) din Legea nr. 193/2000 privind clauzele abuzive din contractele încheiate între profesioniști și consumatori, republicată în Monitorul Oficial al României, Partea I, nr. 543 din 3 august 2012, cu completările ulterioare, se introduce un nou articol, articolul 17¹, cu următorul cuprins:

"

Art. 17¹. - Autoritatea Națională pentru Protecția Consumatorilor informează Comisia Europeană cu privire la adoptarea sau menținerea unor prevederi mai stricte în prezenta ordonanță de urgență decât prevederile Directivei 93/13/CEE a Consiliului din 5 aprilie 1993 privind clauzele abuzive în contractele încheiate cu consumatorii, precum și în legătură cu orice modificare ulterioară a prezentei ordonanțe de urgență, în special în cazul în care respectivele prevederi fie extind testarea caracterului abuziv la clauzele contractuale negociate individual sau la caracterul adecvat al prețului sau remunerației, fie conțin liste de termeni contractuali care vor fi considerați abuzivi."

(2) După [articolul 27](#) din Legea nr. 449/2003 privind vânzarea produselor și garanțiile asociate acestora, republicată în Monitorul Oficial al României, Partea I, nr. 347 din 6 mai 2008, cu modificările și completările ulterioare, se introduce un nou articol, articolul 27¹, cu următorul cuprins:

"

Art. 27¹. - Autoritatea Națională pentru Protecția Consumatorilor informează Comisia Europeană cu privire la adoptarea sau menținerea unor prevederi mai stricte decât prevederile Directivei [1999/44/CE](#) a Parlamentului European și a Consiliului din 25 mai 1999 privind anumite aspecte ale vânzării de bunuri de consum și garanțiile conexe, în special cu privire la art. 16-18 și art. 22 alin. (1) și (2) din prezenta ordonanță de urgență, precum și în legătură cu orice modificare ulterioară."

(3) La [articolul 2](#) din Ordonanța Guvernului nr. 21/1992 privind protecția consumatorilor, republicată în Monitorul Oficial al României, Partea I, nr. 208 din 28 martie 2007, cu modificările și completările ulterioare, [punctul 8](#) se abrogă.

(4) Ordonanța de urgență a Guvernului [nr. 111/2011](#) privind comunicațiile electronice, publicată în Monitorul Oficial al României, Partea I, nr. 925 din 27 decembrie 2011, aprobată cu modificări și completări prin Legea [nr. 140/2012](#), se modifică și se completează după cum urmează:

1. La articolul 4 alineatul (1), [punctul 46](#) se modifică și va avea următorul cuprins:

"

46. contract la distanță - contractul de furnizare a unor servicii de comunicații electronice destinate publicului sau a unor servicii de acces și conectare la rețele publice de comunicații electronice, precum și de livrare a unor echipamente terminale care au legătură cu furnizarea serviciului, încheiat cu utilizatorii finali, persoane juridice, fără prezența fizică simultană a părților, care utilizează în mod exclusiv, înainte și inclusiv la momentul încheierii contractului, unul sau mai multe mijloace de comunicație la distanță;"

2. La articolul 4 [alineatul \(1\)](#), după [punctul 53](#) se introduce un nou punct, punctul 54, cu următorul cuprins:

"

54. contract în afara spațiilor comerciale - orice contract de furnizare a unor servicii de comunicații electronice destinate publicului sau a unor servicii de acces și conectare la rețele publice de comunicații electronice, precum și de livrare a unor echipamente terminale care au legătură cu furnizarea serviciului, încheiat între un furnizor și un utilizator final, persoană juridică, în una dintre următoarele situații:

a) încheiat în prezența fizică simultană a furnizorului și a utilizatorului final, într-un loc care nu este spațiul comercial al furnizorului;

b) încheiat ca urmare a unei oferte din partea utilizatorului final în aceleași circumstanțe ca cele prevăzute la lit. a);

c) încheiat în spațiile comerciale ale furnizorului sau prin orice mijloace de comunicare la distanță, imediat după ce utilizatorul final a fost abordat în mod personal și individual, într-un loc care nu este spațiul comercial al furnizorului, în prezența fizică simultană a acestuia și a utilizatorului final;

d) încheiat în cursul unei deplasări organizate de furnizor cu scopul sau efectul de a promova și a vinde utilizatorului final produse sau servicii."

3. La articolul 4, [alineatul \(2\)](#) se modifică și va avea următorul cuprins:

"

(2) În cuprinsul prezentei ordonanțe de urgență sunt, de asemenea, aplicabile definițiile relevante prevăzute la [art. 3](#) din Ordonanța de urgență a Guvernului nr. 34/2008 privind organizarea și funcționarea Sistemului național unic pentru apeluri de urgență, aprobată cu modificări și completări prin Legea [nr. 160/2008](#), la [art. 2](#) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare, la [art. 1](#) din Legea nr. 365/2002 privind comerțul electronic, republicată, cu modificările ulterioare, respectiv la [art. 1](#) din Legea audiovizualului nr. 504/2002, cu modificările și completările ulterioare, precum și definițiile relevante din legislația din domeniul protecției consumatorilor referitoare la drepturile consumatorilor la încheierea contractelor."

4. La articolul 50, [alineatul \(3\)](#) se modifică și va avea următorul cuprins:

"

(3) La cerere, alți utilizatori finali pot încheia contracte în condițiile alin. (1) și (2)."

5. La capitolul V secțiunea 1 subsecțiunea 2, titlul paragrafului 2 se modifică după cum urmează:

"

Încheierea contractelor la distanță și a contractelor în afara spațiilor comerciale"

6. La articolul 51 [alineatul \(1\)](#), partea introductivă se modifică și va avea următorul cuprins:

"

Art. 51. - (1) Contractele încheiate de utilizatorii finali pentru a beneficia de servicii de acces și conectare la rețele publice de comunicații electronice ori de servicii de comunicații electronice destinate publicului vor conține, într-o formă clară, inteligibilă și ușor accesibilă, următoarele clauze minime privitoare la:"

7. [Articolul 52](#) se modifică și va avea următorul cuprins:

"

Art. 52. - (1) Prevederile prezentului paragraf se aplică numai în cazul contractelor încheiate la distanță și al contractelor în afara spațiilor comerciale de către utilizatorii finali, persoane juridice.

(2) Prin excepție de la alin. (1), contractelor încheiate în afara spațiilor comerciale de către utilizatorii finali persoane juridice, pe baza unor oferte individuale privind prețuri sau servicii, propuse în cadrul unor negocieri directe, nu li se aplică dispozițiile art. 56-59².

(3) Prevederile prezentului paragraf nu se aplică acelor contracte încheiate cu furnizorii de servicii de comunicații electronice prin telefoane publice cu plată, pentru utilizarea acestora, sau încheiate pentru utilizarea unei conexiuni unice care presupune executarea unei singure prestații realizată simultan încheierii contractului și nemijlocit prin intermediul telefonului, internetului sau faxului, ca urmare a solicitării utilizatorului final."

8. [Articolul 53](#) se modifică și va avea următorul cuprins:

"

Art. 53. - (1) Înainte ca un contract la distanță sau în afara spațiilor comerciale sau orice ofertă similară să producă efecte obligatorii asupra utilizatorului final, furnizorul trebuie să îi furnizeze utilizatorului final următoarele informații în mod clar și inteligibil:

- a) identitatea furnizorului, cum ar fi denumirea sa comercială;
- b) caracteristicile esențiale ale serviciilor oferite, precum și perioada de valabilitate a ofertei sau a tarifelor;
- c) adresa poștală la care furnizorul este stabilit, precum și, în cazul în care există, numărul de telefon, numărul de fax și adresa de poștă electronică ale acestuia la care poate fi efectiv contactat, pentru a-i permite utilizatorului final să ia rapid legătura cu furnizorul și să comunice cu acesta în mod eficient și, dacă este cazul, adresa poștală și identitatea furnizorului în numele căruia acționează;
- d) în cazul în care este diferită de adresa furnizată în conformitate cu lit. c), adresa poștală a locului în care furnizorul își desfășoară activitatea și, după caz, adresa poștală a furnizorului în numele căruia acționează, la care utilizatorul final poate trimite eventualele reclamații;
- e) prețul total al echipamentelor terminale și al serviciilor cu toate taxele incluse sau, în cazul în care prețul nu poate fi calculat dinainte în mod rezonabil dată fiind natura echipamentelor terminale sau a serviciilor, modalitatea de calcul al prețului și, după caz, toate costurile suplimentare de transport, de livrare, taxele poștale sau de orice altă natură sau, în cazul în care acestea nu pot fi calculate dinainte în mod rezonabil, menționarea faptului că aceste costuri suplimentare ar putea fi suportate de utilizatorul final; contravaloarea planului tarifar, cu precizarea numărului de minute, a creditului sau a traficului de date inclus, precum și a condițiilor de utilizare a acestora, dacă este cazul, extraopțiunile disponibile și contravaloarea acestora, tarifele pentru apeluri și pentru minutele ori traficul de date suplimentar, după caz, tariful de conectare sau instalare, cu toate taxele incluse. În cazul unui contract pe durată nedeterminată sau al unui contract care include un abonament, prețul total va include costurile totale pe perioada de facturare. În cazul în care prețul acestor contracte este exprimat printr-un tarif fix, prețul total va cuprinde și costurile lunare totale. În cazul în care costul total nu poate fi calculat dinainte, trebuie indicat modul în care se calculează prețul;
- f) costul de utilizare a mijloacelor de comunicare la distanță în vederea încheierii contractului, atunci când este calculat pe baza unui alt tarif decât tariful de bază;
- g) modalitățile de plată, livrare, executare, data până la care furnizorul se angajează să presteze serviciile sau să livreze echipamentul terminal în cazul în care furnizarea serviciului include și livrarea unui echipament terminal, precum și procedura furnizorului de soluționare a reclamațiilor;
- h) în cazul în care există un drept de retragere, condițiile, termenele și procedurile de exercitare a dreptului de retragere, în conformitate cu art. 58 alin. (1);
- i) acolo unde este cazul, informația potrivit căreia utilizatorul final va trebui să suporte costul aferent returnării echipamentului terminal în caz de retragere și, dacă echipamentul terminal, prin însăși natura lui, nu poate fi, în mod normal, returnat prin poștă, costul aferent returnării acestuia;
- j) în cazul în care utilizatorul final își exercită dreptul de retragere după formularea unei cereri în conformitate cu art. 54 alin. (3) sau cu art. 55 alin. (8), informația potrivit căreia utilizatorul final este obligat să achite furnizorului costuri rezonabile, în conformitate cu art. 59² alin. (3);
- k) în cazul în care dreptul de retragere nu este prevăzut în conformitate cu art. 59³, informația conform căreia utilizatorul final nu va beneficia de un drept de retragere sau, după caz, circumstanțele în care utilizatorul final își pierde dreptul de retragere;
- l) o mențiune referitoare la existența unei garanții legale privind conformitatea produselor;

m) acolo unde este cazul, existența și condițiile de asistență după vânzare acordată utilizatorului final, serviciile prestate după vânzare și garanțiile comerciale;

n) existența codurilor de conduită relevante și modalitatea în care pot fi obținute copii ale acestora, după caz;

o) durata minimă a contractului, după caz, sau, dacă contractul este încheiat pe durată nedeterminată ori urmează să fie prelungit în mod automat, condițiile de încetare a contractului înainte de termen și penalitățile aplicabile, dacă este cazul;

p) acolo unde este cazul, durata minimă de valabilitate a obligațiilor care revin utilizatorului final conform contractului;

q) acolo unde este cazul, existența și condițiile aferente avansurilor sau altor garanții financiare care trebuie plătite sau oferite de utilizatorul final la cererea furnizorului;

r) acolo unde este cazul, posibilitatea și modalitatea de a recurge la un mecanism extrajudiciar de depunere și soluționare a reclamațiilor căruia i se supune furnizorul.

(2) Informațiile menționate la alin. (1) fac parte integrantă din contractul la distanță sau din contractul în afara spațiilor comerciale și nu pot fi modificate decât în cazul în care părțile contractante decid altfel în mod explicit.

(3) În cazul în care furnizorul nu îndeplinește cerințele în materie de informare cu privire la costuri suplimentare, conform celor menționate la alin. (1) lit. e), sau la costurile aferente returnării produselor, conform celor menționate la alin. (1) lit. i), utilizatorul final nu suportă respectivele costuri.

(4) Informațiile contractuale se prezintă în limba română într-o formă accesibilă, astfel încât acestea să fie înțelese cu ușurință de utilizatorul final, fără a exclude prezentarea acestora și în alte limbi.

(5) Cerințele în materie de informare prevăzute în prezenta ordonanță de urgență completează cerințele de informare conținute în Ordonanța de urgență a Guvernului [nr. 49/2009](#) privind libertatea de stabilire a prestatorilor de servicii și libertatea de a furniza servicii în România, aprobată cu modificări și completări prin Legea [nr. 68/2010](#), și, respectiv, Legea [nr. 365/2002](#), republicată, cu modificările ulterioare. Fără a aduce atingere primului paragraf, dacă o dispoziție privind conținutul și modul în care trebuie furnizate informațiile în cazul comerțului electronic din Ordonanța de urgență a Guvernului [nr. 49/2009](#), aprobată cu modificări și completări prin Legea [nr. 68/2010](#), contravine unei dispoziții din prezenta ordonanță de urgență, prevalează dispozițiile prezentei ordonanțe de urgență.

(6) Sarcina probei în ceea ce privește îndeplinirea cerințelor în materie de informare stabilite în prezentul articol revine furnizorului."

9. [Articolul 54](#) se modifică și va avea următorul cuprins:

"

Art. 54. - (1) În cazul contractelor în afara spațiilor comerciale, furnizorul transmite informațiile prevăzute la art. 53 alin. (1) utilizatorului final, persoană juridică, pe suport hârtie sau, în cazul în care utilizatorul final este de acord, pe un alt suport durabil. Aceste informații sunt lizibile și redactate într-un limbaj simplu și inteligibil.

(2) Furnizorul pune la dispoziția utilizatorului final un exemplar original al contractului semnat sau confirmarea contractului pe suport hârtie sau, dacă utilizatorul final este de acord, pe un alt suport durabil.

(3) În cazul în care utilizatorul final dorește ca prestarea unor servicii să înceapă în timpul perioadei de retragere prevăzute la art. 56 alin. (2), furnizorul solicită utilizatorului final să formuleze o astfel de cerere expresă pe un suport durabil.

(4) Îndeplinirea obligației de la alin. (1) nu este necesară în cazul în care exemplarul original al contractului sau confirmarea contractului pe suport hârtie, sau, dacă utilizatorul final este de acord, pe un alt suport durabil, care trebuie puse la dispoziția utilizatorului final potrivit prevederilor alin. (2), conțin informațiile prevăzute la art. 53 alin. (1)."

10. [Articolul 55](#) se modifică și va avea următorul cuprins:

"

Art. 55. - (1) În cazul contractelor la distanță, furnizorul transmite informațiile prevăzute la art. 53 alin.

(1) sau pune la dispoziția utilizatorului final respectivele informații într-un mod adecvat mijlocului de comunicare la distanță utilizat, folosind un limbaj simplu și inteligibil. În măsura în care respectiva informație este prezentată pe un suport durabil, aceasta trebuie să fie lizibilă.

(2) Dacă un contract la distanță care urmează să fie încheiat prin mijloace electronice obligă utilizatorul final să plătească, furnizorul aduce la cunoștința utilizatorului final de o manieră clară și foarte vizibilă, în mod direct, înainte ca acesta să facă comanda, informațiile prevăzute la art. 53 alin. (1) lit. b), e), o) și p). Furnizorul se asigură că, atunci când utilizatorul final face comanda, acesta din urmă recunoaște în mod explicit că această comandă implică o obligație de a plăti. Dacă pentru a face comanda este necesar să se activeze un buton sau o funcție similară, butonul sau funcția similară este etichetat/ă de o manieră lizibilă doar cu mențiunea "comandă ce implică o obligație de plată" sau o formulare neambiguă corespunzătoare, care să indice că a face comanda implică obligația de a plăti furnizorului. Dacă furnizorul încalcă prevederile prezentului alineat, utilizatorul final nu are nicio obligație în temeiul contractului sau al comenzii.

(3) Site-urile comerciale indică clar și lizibil, cel mai târziu la începutul procesului de formulare a comenzii, dacă se aplică vreo restricție în ceea ce privește livrarea și care sunt mijloacele de plată acceptate.

(4) În cazul în care contractul este încheiat printr-un mijloc de comunicare la distanță ce permite un spațiu sau un timp limitat pentru afișarea informației, furnizorul transmite prin mijlocul de comunicare respectiv, înaintea încheierii contractului, cel puțin informațiile precontractuale referitoare la principalele caracteristici ale produsului sau serviciului, identitatea furnizorului, prețul total, dreptul la retragere, durata contractului și, în cazul contractelor pe durată nedeterminată, modalitățile de încetare a contractului, prevăzute la art. 53 alin. (1) lit. a), b), e), h) și o). Celelalte informații menționate la art. 53 alin. (1) sunt furnizate utilizatorului final de furnizor într-un mod adecvat, în conformitate cu alin. (1) din prezentul articol.

(5) Fără a aduce atingere alin. (4), în cazul în care furnizorul apelează telefonic utilizatorul final în vederea încheierii unui contract la distanță, furnizorul își declină identitatea la începutul conversației cu

utilizatorul final și, dacă este cazul, declină identitatea persoanei în numele căreia a efectuat apelul telefonic și specifică scopul comercial al apelului.

(6) În cazul în care urmează să se încheie un contract la distanță prin intermediul telefonului, furnizorul trebuie să confirme oferta utilizatorului final, al cărui angajament începe doar după ce acesta a semnat oferta sau după ce și-a trimis consimțământul scris. Aceste confirmări trebuie făcute pe un suport durabil.

(7) Furnizorul transmite utilizatorului final confirmarea încheierii contractului, pe un suport durabil, într-un termen rezonabil din momentul încheierii contractului la distanță și cel târziu la momentul livrării echipamentului terminal sau înainte de începerea prestării serviciului solicitat. Respectiva confirmare include:

a) toate informațiile menționate la art. 53 alin. (1), cu excepția cazului în care furnizorul a transmis deja informațiile respective utilizatorului final, pe un suport durabil, înaintea încheierii contractului la distanță;

b) acolo unde este cazul, confirmarea acordului prealabil expres al utilizatorului final.

(8) În cazul în care utilizatorul final dorește ca prestarea unor servicii să înceapă în timpul perioadei de retragere prevăzute la art. 56 alin. (2), furnizorul solicită utilizatorului final să facă o cerere expresă în acest sens.

(9) Momentul încheierii contractului la distanță îl constituie momentul confirmării, pe un suport durabil, de către furnizor a acceptării comenzii transmise de utilizatorul final.

(10) Prezentul articol nu aduce atingere dispozițiilor privind încheierea prin mijloace electronice a contractelor și comenzile prin internet, astfel cum sunt stabilite la art. 7 și 9 din Legea nr. 365/2002, republicată, cu modificările ulterioare."

11. [Articolul 56](#) se modifică și va avea următorul cuprins:

"

Art. 56. - (1) Cu excepția cazurilor prevăzute la art. 59³, utilizatorul final beneficiază de o perioadă de 14 zile pentru a se retrage dintr-un contract la distanță sau dintr-un contract în afara spațiilor comerciale, fără a fi nevoit să justifice decizia de retragere și fără a suporta alte costuri decât cele prevăzute la art. 59¹ alin. (3) și la art. 59².

(2) Fără a aduce atingere art. 57, perioada de retragere menționată la alin. (1) din prezentul articol expiră în termen de 14 zile de la:

a) data încheierii contractului, în cazul contractelor de prestări servicii;

b) ziua în care utilizatorul final sau o parte terță alta decât transportatorul și care este indicată de utilizatorul final intră în posesia fizică a produselor, în cazul contractelor de vânzare, sau:

(i) în cazul în care utilizatorul final comandă printr-o singură comandă produse multiple care vor fi livrate separat, ziua în care utilizatorul final sau o parte terță, alta decât transportatorul și care este indicată de utilizatorul final, intră în posesia fizică a ultimului produs;

(ii) în cazul livrării unui produs care constă din mai multe loturi sau piese, ziua în care utilizatorul final sau o parte terță, alta decât transportatorul și care este indicată de utilizatorul final, intră în posesia fizică a ultimului produs sau piesă;

(iii) în cazul contractelor pentru livrarea periodică de produse pe o perioadă de timp determinată, ziua în care utilizatorul final sau o parte terță, alta decât transportatorul și care este indicată de utilizatorul final, intră în posesia fizică a primului produs;

(3) Părțile contractante își îndeplinesc obligațiile contractuale pe parcursul perioadei de retragere conform prevederilor prezentei ordonanțe de urgență."

12. [Articolul 57](#) se modifică și va avea următorul cuprins:

"

Art. 57. - (1) În cazul în care furnizorul nu a transmis utilizatorului final informațiile privind dreptul de retragere conform art. 53 alin. (1) lit. h), perioada de retragere expiră la 12 luni de la sfârșitul perioadei inițiale de retragere, astfel cum este stabilită în conformitate cu art. 56 alin. (2).

(2) În cazul în care furnizorul a transmis utilizatorului final informațiile prevăzute la alin. (1) din prezentul articol în termen de 12 luni de la data menționată la art. 56 alin. (2), perioada de retragere expiră în 14 zile de la data la care utilizatorul final primește informațiile respective."

13. [Articolul 58](#) se modifică și va avea următorul cuprins:

"

Art. 58. - (1) Înainte de expirarea perioadei de retragere, utilizatorul final informează furnizorul cu privire la decizia sa de retragere din contract. În acest scop, utilizatorul final poate utiliza orice declarație neechivocă în care își exprimă decizia de retragere din contract.

(2) Utilizatorul final și-a exercitat dreptul de retragere în perioada de retragere menționată la art. 56 alin. (2) și la art. 57 în cazul în care comunicarea cu privire la exercitarea dreptului de retragere este transmisă de către utilizatorul final înaintea expirării perioadei respective.

(3) Furnizorul poate, în plus față de posibilitatea menționată la alin. (1), să acorde utilizatorului final opțiunea de a completa și de a transmite în format electronic, pe site-ul furnizorului, declarația neechivocă în care își exprimă decizia de retragere din contract. În aceste cazuri, furnizorul comunică utilizatorului final, fără întârziere, pe un suport durabil, confirmarea de primire a declarației de retragere.

(4) Sarcina probei privind exercitarea dreptului de retragere în conformitate cu dispozițiile din prezentul articol revine utilizatorului final."

14. [Articolul 59](#) se modifică și va avea următorul cuprins:

"

Art. 59. - Exercițarea dreptului de retragere pune capăt obligațiilor părților contractuale, după caz:

a) de a executa contractul la distanță sau contractul în afara spațiului comercial;

b) de a încheia un contract la distanță sau în afara spațiului comercial, în cazul în care utilizatorul final a efectuat o comandă."

15. După [articolul 59](#) se introduc opt noi articole, articolele 59¹-59⁸, cu următorul cuprins:

"

Art. 59¹. - (1) Furnizorul rambursează toate sumele pe care le-a primit drept plată din partea utilizatorului final, inclusiv, după caz, costurile livrării, fără întârziere nejustificată și, în orice caz, nu mai

târziu de 14 zile de la data la care este informat de decizia de retragere din contract a utilizatorul final în conformitate cu art. 58.

(2) Furnizorul rambursează sumele menționate la alin. (1) utilizând aceleași modalități de plată ca și cele folosite de utilizatorul final pentru tranzacția inițială, cu excepția cazului în care utilizatorul final a fost de acord cu o altă modalitate de plată și cu condiția de a nu cădea în sarcina utilizatorului final plata de comisioane în urma rambursării.

(3) Fără a aduce atingere alin. (1), furnizorul nu este obligat să ramburseze costurile suplimentare în cazul în care utilizatorul final a ales în mod explicit un alt tip de livrare decât livrarea standard oferită de furnizor.

(4) Cu excepția cazului în care furnizorul s-a oferit să recupereze el însuși produsele, în cazul contractelor de vânzare, furnizorul poate amâna rambursarea până la data recepționării produselor care au făcut obiectul vânzării sau până la momentul primirii unei dovezi din partea utilizatorului final conform căreia acesta a trimis produsele către furnizor, luându-se în considerare data cea mai apropiată.

Art. 59². - (1) Cu excepția cazului în care furnizorul s-a oferit să recupereze el însuși produsele, utilizatorul final returnează produsele sau le înmânează furnizorului sau unei persoane autorizate de furnizor să recepționeze produsele, fără întârziere nejustificată și în decurs de cel mult 14 zile de la data la care acesta a comunicat furnizorului decizia sa de retragere din contract în conformitate cu art. 58. Termenul este respectat dacă produsele sunt trimise înapoi de utilizatorul final înainte de expirarea perioadei de 14 zile.

(2) Utilizatorul final suportă doar costurile directe legate de returnarea produselor, cu excepția cazului în care furnizorul acceptă să suporte acele costuri sau în care furnizorul nu a informat utilizatorul final că aceste costuri trebuie suportate de utilizatorul final. În cazul contractelor în afara spațiilor comerciale, în cazul cărora produsele au fost livrate la domiciliul utilizatorului final la momentul încheierii contractului, furnizorul preia produsele pe cheltuiala sa, dacă produsele, prin natura lor, nu pot fi returnate în mod normal prin poștă.

(3) Utilizatorul final este responsabil doar în ceea ce privește diminuarea valorii produselor rezultată din manipularea acestora, diferit de ceea ce este necesar pentru determinarea naturii, caracteristicilor și funcționării produselor. Diminuarea valorii produselor nu trebuie să fie descurajantă pentru utilizatorul final în a-și exercita dreptul de retragere. Indiferent de situație, utilizatorul final nu este responsabil pentru diminuarea valorii produselor în cazul în care furnizorul a omis să îl informeze cu privire la dreptul de retragere în conformitate cu art. 53 alin. (1) lit. h).

(4) Furnizorul trebuie să poată face dovada diminuării valorii produselor care rezultă diferit de ceea ce este necesar pentru determinarea naturii, caracteristicilor și funcționării produselor.

(5) Atunci când utilizatorul final își exercită dreptul de retragere după transmiterea cererii în conformitate cu art. 54 alin. (3) sau cu art. 55 alin. (8), utilizatorul final plătește furnizorului o sumă proporțională cu ceea ce s-a furnizat până la momentul în care utilizatorul final a informat furnizorul cu privire la exercitarea dreptului de retragere, în raport cu acoperirea totală a contractului. Suma proporțională care trebuie plătită furnizorului de către utilizatorul final este calculată pe baza prețului

total convenit în contract. Dacă prețul total este excesiv, suma proporțională este calculată pe baza valorii de piață a ceea ce s-a furnizat.

(6) Utilizatorul final nu suportă costurile pentru prestarea serviciilor în cursul perioadei de retragere, în una dintre următoarele situații:

a) furnizorul nu a furnizat informații în conformitate cu art. 53 alin. (1) lit. h) sau i);

b) utilizatorul final nu a cerut expres ca prestarea să înceapă în timpul perioadei de retragere în conformitate cu art. 54 alin. (3) și cu art. 55 alin. (8);

(7) Cu excepția celor prevăzute la art. 59¹ alin. (3) și la prezentul articol, exercitarea dreptului de retragere nu atrage răspunderea utilizatorului final.

Art. 59³. - Sunt exceptate de la dreptul de retragere prevăzut la art. 56-59² în ceea ce privește contractele la distanță și contractele în afara spațiilor comerciale contractele de prestări servicii, după prestarea completă a serviciilor, dacă executarea a început cu acordul prealabil expres al utilizatorului final și după ce acesta a confirmat că a luat cunoștință de faptul că își va pierde dreptul la retragere după executarea completă a contractului de către furnizor.

Art. 59⁴. - (1) Cu excepția cazului în care părțile au convenit altfel cu privire la momentul livrării, furnizorul livrează produsele transferând posesia fizică sau controlul asupra produselor către utilizatorul final, fără întârziere nejustificată și în orice caz în decurs de cel mult 30 de zile de la încheierea contractului.

(2) În cazul în care furnizorul nu și-a îndeplinit obligația de a livra produsele în momentul convenit cu utilizatorul final sau în termenul stabilit la alin. (1), utilizatorul final îi solicită să efectueze livrarea într-un termen suplimentar, corespunzător circumstanțelor. În cazul în care furnizorul nu livrează produsele în termenul suplimentar respectiv, utilizatorul final are dreptul, după caz, la rezoluțiunea sau rezilierea contractului.

(3) Alineatul (2) nu se aplică contractelor de vânzare în cazul în care furnizorul a refuzat să livreze produsele sau în cazul în care livrarea în termenul convenit este esențială având în vedere toate circumstanțele existente la încheierea contractului sau în cazul în care utilizatorul final informează furnizorul, înainte de încheierea contractului, că livrarea înainte de sau la o dată precizată este esențială. În aceste cazuri, dacă furnizorul nu livrează produsele în momentul convenit cu utilizatorul final sau în termenul stabilit la alin. (1), utilizatorul final are dreptul, după caz, la rezoluțiunea sau rezilierea contractului.

(4) Prin excepție de la [art. 1.549-1.554](#) din Codul civil, la rezoluțiunea sau, după caz, la rezilierea contractului, furnizorul rambursează fără întârzieri nejustificate toate sumele plătite în temeiul contractului de către utilizatorul final și în decurs de cel mult 7 zile de la data la care utilizatorul final a comunicat furnizorului decizia sa de terminare a contractului.

(5) În plus față de rezoluțiunea sau rezilierea contractului în conformitate cu alin. (2), utilizatorul final poate recurge la alte căi de atac prevăzute de legislația în vigoare.

Art. 59⁵. - (1) În cazul în care un furnizor operează o linie telefonică pentru a putea fi contactat prin telefon cu privire la contractul încheiat, utilizatorul final nu este obligat să plătească, la contactarea furnizorului, mai mult decât tariful de bază.

(2) Alineatul (1) nu aduce atingere dreptului furnizorilor de servicii de comunicații de a taxa aceste apeluri.

Art. 59⁶. - Înainte ca un utilizator final să încheie un contract sau să accepte o ofertă, furnizorul solicită consimțământul explicit din partea utilizatorului final cu privire la orice plată suplimentară față de prețul stabilit anterior pentru obligația contractuală principală a furnizorului. În cazul în care furnizorul nu a obținut consimțământul expres al utilizatorului final, însă l-a dedus utilizând opțiuni incluse în mod automat pe care utilizatorul final trebuie să le respingă pentru a evita plata suplimentară, utilizatorul final poate pretinde rambursarea acestei plăți.

Art. 59⁷. - (1) În cazul furnizării de servicii sau livrării de echipamente terminale fără consimțământul utilizatorului final, acesta este exonerat de efectuarea oricărei contraprestații.

(2) Lipsa răspunsului din partea utilizatorului final nu poate fi considerată consimțământ.

(3) În cazul prevăzut la alin. (1), cheltuielile de returnare a echipamentului terminal sunt suportate de către furnizor.

Art. 59⁸. - În cazul contractelor în care furnizorul livrează produsele către utilizatorul final, riscul de pierdere sau de deteriorare a produselor este transferat utilizatorului final în momentul în care acesta sau o parte terță desemnată de acesta, alta decât transportatorul, intră în posesia fizică a produselor. Cu toate acestea, riscul este transferat utilizatorului final în momentul livrării produselor către transportator, dacă transportatorul a fost însărcinat de către utilizatorul final să transporte produsele, iar această opțiune nu a fost oferită de către furnizor, fără a aduce atingere drepturilor utilizatorului final față de transportator."

16. La articolul 120, [alineatul \(1\)](#) și alineatul (2) [litera a\)](#) se modifică și vor avea următorul cuprins:

"

Art. 120. - (1) ANCOM are dreptul să solicite persoanelor care furnizează sau au furnizat rețele sau servicii de comunicații electronice ori facilități asociate informațiile, inclusiv de natură financiară, necesare în vederea exercitării atribuțiilor prevăzute de prezenta ordonanță de urgență, de legislația specială din domeniul comunicațiilor electronice sau de legislația din domeniul protecției consumatorilor în cazurile în care competența de monitorizare și verificare a acestor obligații aparține și ANCOM.

(2) Informațiile prevăzute la alin. (1) pot fi solicitate de ANCOM în special în următoarele scopuri:

a) verificarea respectării obligațiilor prevăzute de dispozițiile prezentei ordonanțe de urgență, de legislația din domeniul protecției consumatorilor în cazurile în care competența de monitorizare și verificare a acestor obligații aparține și ANCOM sau ale legislației speciale din domeniul comunicațiilor electronice ori impuse de ANCOM în conformitate cu aceste dispoziții, precum și punerea în aplicare și executarea regulamentelor Uniunii Europene din domeniul comunicațiilor electronice, în special în ceea ce privește monitorizarea pieței și verificarea respectării obligațiilor furnizorilor de rețele sau de servicii de comunicații electronice care decurg din aceste regulamente, în cazurile în care competența de monitorizare și verificare a acestor obligații aparține autorității naționale de reglementare;"

17. La articolul 142, [punctele 20-24](#) se modifică și vor avea următorul cuprins:

"

20. nerespectarea cerinței de a furniza informații într-un mod clar și inteligibil conform părții introductive a art. 53 alin. (1);

21. nerespectarea prevederilor art. 53 alin. (1) referitoare la informațiile precontractuale;

22. nerespectarea prevederilor art. 53 alin. (2) referitoare la includerea informațiilor precontractuale în cadrul contractului și la situația în care aceste informații pot fi modificate;

23. nerespectarea prevederilor art. 53 alin. (3) referitoare la exonerarea utilizatorului final de a suporta costurile suplimentare în situația în care furnizorul nu îndeplinește cerințele în materie de informare;

24. nerespectarea prevederilor art. 53 alin. (4) referitoare la prezentarea informațiilor în limba română într-o formă accesibilă, astfel încât acestea să fie înțelese cu ușurință de utilizatorul final;"

18. La [articolul 142](#), după [punctul 24](#) se introduc optsprezece noi puncte, punctele 24¹ -24¹⁸, cu următorul cuprins:

"

24¹. nerespectarea prevederilor art. 54 alin. (1) referitoare la informații;

24². nerespectarea prevederilor art. 54 alin. (2) referitoare la contract;

24³. nerespectarea prevederilor art. 54 alin. (3) referitoare la solicitarea cererii de începere a prestării unor servicii;

24⁴. nerespectarea prevederilor art. 55 alin. (1)-(7) referitoare la informații;

24⁵. nerespectarea prevederilor art. 55 alin. (8) referitoare la solicitarea de a se face o cerere expresă;

24⁶. nerespectarea prevederilor art. 56 alin. (1)-(2) referitoare la dreptul de retragere;

24⁷. nerespectarea prevederilor art. 56 alin. (3) referitoare la obligațiile contractuale pe parcursul perioadei de retragere;

24⁸. nerespectarea prevederilor art. 57 referitoare la informațiile privind dreptul de retragere;

24⁹. nerespectarea prevederilor art. 58 alin. (3) referitoare la confirmarea de primire a declarației de retragere;

24¹⁰. nerespectarea prevederilor art. 59 de a pune capăt obligațiilor părților contractuale în cazul exercitării dreptului de retragere;

24¹¹. nerespectarea prevederilor art. 59¹ alin. (1) și (2) referitoare la obligațiile care revin furnizorului în cazul retragerii;

24¹². nerespectarea prevederilor art. 59¹ alin. (4) referitoare la amânarea rambursării;

24¹³. nerespectarea obligațiilor impuse de art. 59² în condițiile în care utilizatorul final și-a respectat obligațiile sale;

24¹⁴. nerespectarea prevederilor art. 59⁴ referitoare la livrare;

24¹⁵. nerespectarea prevederilor art. 59⁵ referitoare la plata tarifului de bază în cazul comunicărilor telefonice;

24¹⁶. nerespectarea prevederilor art. 59⁶ referitoare la plăți suplimentare;

24¹⁷. nerespectarea dreptului utilizatorului final privind exonerarea de la efectuarea oricărei contraprestații exercitat în condițiile prevederilor art. 59⁷ referitoare la lipsa consimțământului;

24¹⁸. nerespectarea prevederilor art. 59⁸ referitoare la riscul de pierdere sau de deteriorare a produselor."

(5) Prevederile paragrafului 2 din [capitolul V](#) secțiunea 1 subsecțiunea 2 din Ordonanța de urgență a Guvernului [nr. 111/2011](#) privind comunicațiile electronice, publicată în Monitorul Oficial al României, Partea I, nr. 925 din 27 decembrie 2011, aprobată cu modificări și completări prin Legea [nr. 140/2012](#), astfel cum au fost modificate și completate de alin. (4) al prezentului articol, se aplică contractelor încheiate după data intrării în vigoare a prevederilor prezentei ordonanțe de urgență.

ARTICOLUL 30 Intrare în vigoare și aplicare (1) Prezenta ordonanță de urgență intră în vigoare la data de 13 iunie 2014.

(2) Dispozițiile prezentei ordonanțe de urgență se aplică contractelor încheiate după data intrării sale în vigoare.

(3) Contractelor în curs de derulare la data intrării în vigoare a prezentei ordonanțe de urgență li se aplică legislația în vigoare la data încheierii acestora.

ARTICOLUL 31 Informarea Comisiei Europene Autoritatea Națională pentru Protecția Consumatorilor informează Comisia Europeană cu privire la modul de transpunere a art. 3 [alin. \(4\)](#), art. 6 [alin. \(7\)](#) și [\(8\)](#), art. 8 [alin. \(6\)](#) și a art. 9 [alin. \(3\)](#) din prezenta ordonanță de urgență. În situația în care prevederile respective sunt ulterior modificate, Autoritatea Națională pentru Protecția Consumatorilor va informa Comisia Europeană cu privire la acestea.

ARTICOLUL 32 Abrogări (1) La data intrării în vigoare a prezentei ordonanțe de urgență se abrogă:

a) Ordonanța Guvernului [nr. 106/1999](#) privind contractele încheiate în afara spațiilor comerciale, republicată în Monitorul Oficial al României, Partea I, nr. 168 din 5 martie 2008;

b) Ordonanța Guvernului [nr. 130/2000](#) privind protecția consumatorilor la încheierea și executarea contractelor la distanță, republicată în Monitorul Oficial al României, Partea I, nr. 177 din 7 martie 2008, cu modificările ulterioare.

(2) Trimiterile din actele normative în vigoare la ordonanțele Guvernului abrogate prin alin. (1) se înțeleg ca trimiteri la prezenta ordonanță de urgență.

*

Prezenta ordonanță de urgență transpune prevederile Directivei [2011/83/UE](#) a Parlamentului European și a Consiliului din 25 octombrie 2011 privind drepturile consumatorilor, de modificare a Directivei [93/13/CEE](#) a Consiliului și a Directivei [1999/44/CE](#) a Parlamentului European și a Consiliului și de abrogare a Directivei [85/577/CEE](#) a Consiliului și a Directivei [97/7/CE](#) a Parlamentului European și a Consiliului, publicată în Jurnalul Oficial al Uniunii Europene, seria L, nr. 304 din 22 noiembrie 2011.

PRIM-MINISTRU
VICTOR-VIOREL PONTA

Contrasemnează:

Ministrul economiei,
Constantin Niță
Președintele Autorității Naționale
pentru Protecția Consumatorilor,
Marius Alexandru Dunca
Viceprim-ministru, ministrul dezvoltării
regionale
și administrației publice,
Nicolae-Liviu Dragnea
Ministrul finanțelor publice,
Ioana-Maria Petrescu
Ministrul delegat pentru buget,
Liviu Voinea
p. Ministrul afacerilor externe,
George Ciamba,
secretar de stat
Ministrul transporturilor,
Dan-Coman Șova
Ministrul pentru societatea
informațională,
Alexandru-Răzvan Cotovelea

București, 4 iunie 2014.

Nr. 34.

ANEXĂ

Informații privind exercitarea dreptului de retragere

A. Model de instrucțiuni privind retragerea

Dreptul de retragere

Aveți dreptul de a vă retrage din prezentul contract, fără a preciza motivele, în termen de 14 zile.

Perioada de retragere expiră după 14 zile începând de la ziua - a se vedea punctul 1 din Instrucțiuni de completare.

Pentru a vă exercita dreptul de retragere trebuie să ne informați - a se vedea punctul 2 din Instrucțiuni de completare - cu privire la decizia dumneavoastră de a vă retrage din prezentul contract, utilizând o

declarație neechivocă, de exemplu, o scrisoare trimisă prin poștă, fax sau e-mail. În acest scop, puteți folosi modelul de retragere alăturat; folosirea lui nu este însă obligatorie - a se vedea punctul 3 din Instrucțiuni de completare.

Pentru a respecta termenul-limită de retragere este suficient să trimiteți comunicarea privind exercitarea dreptului de retragere înainte de expirarea perioadei de retragere.

Consecințele retragerii

Dacă vă retrageți, vom rambursa orice sumă pe care am primit-o de la dumneavoastră, inclusiv costurile livrării, cu excepția costurilor suplimentare determinate de faptul că ați ales altă modalitate de livrare decât cel mai ieftin tip de livrare standard oferit de noi, fără întârzieri nejustificate și, în orice caz, nu mai târziu de 14 zile de la data la care suntem informați cu privire la decizia dumneavoastră de a vă retrage din prezentul contract. Vom efectua această rambursare folosind aceeași modalitate de plată ca și cea folosită pentru tranzacția inițială, cu excepția cazului în care v-ați exprimat acordul expres pentru o altă modalitate de rambursare; în orice caz, nu vi se vor percepe comisioane ca urmare a unei astfel de rambursări - a se vedea punctul 4 din Instrucțiuni de completare.

A se vedea punctul 5 din Instrucțiuni de completare.

A se vedea punctul 6 din Instrucțiuni de completare.

Instrucțiuni de completare

1. Introduceți următoarele formulări între ghilimele:

a) în cazul unui contract de prestări de servicii sau al unui contract pentru furnizarea de apă, gaze naturale, energie electrică, atunci când acestea nu prevăd vânzarea într-un volum limitat sau cantitate stabilită, de energie termică sau conținuturi digitale care nu sunt livrate pe un suport material: "încheierii contractului.";

b) în cazul unui contract de vânzare: "la care intrați dumneavoastră sau o parte terță, alta decât transportatorul, indicată de dumneavoastră, în posesia fizică a produselor.";

c) în cazul unui contract privind bunuri multiple comandate de consumator printr-o singură comandă și livrate separat: "la care intrați dumneavoastră sau o parte terță, alta decât transportatorul, indicată de dumneavoastră, în posesia fizică a ultimului produs";

d) în cazul unui contract privind livrarea unui produs constând din mai multe loturi sau părți: "la care intrați dumneavoastră sau o parte terță, alta decât transportatorul, indicată de dumneavoastră, în posesia fizică a ultimului lot sau a ultimei piese.";

e) în cazul unui contract pentru livrarea periodică de produse pe o perioadă de timp determinată: "la care intrați, dumneavoastră sau o parte terță, alta decât transportatorul, indicată de dumneavoastră, în posesia fizică a primului produs."

2. Introduceți numele dumneavoastră, adresa dumneavoastră poștală și, dacă este cazul, numărul dumneavoastră de telefon, numărul de fax și adresa de e-mail.

3. Dacă pe site-ul dumneavoastră oferiți consumatorului opțiunea de a completa și transmite electronic informațiile privind retragerea sa din contract, introduceți următoarele: "De asemenea, puteți completa și transmite electronic de pe site-ul nostru [introduceți adresa de internet] formularul standard de retragere sau orice altă declarație neechivocă. Dacă folosiți această opțiune, vă vom

transmite fără întârziere, pe un suport durabil, de exemplu prin e-mail, confirmarea de primire a cererii de retragere."

4. În cazul contractelor de vânzări în care nu v-ați oferit să recuperați produsele în caz de retragere, introduceți următoarele: "Putem amâna rambursarea până la data la care primim înapoi produsele sau până la momentul la care ne-ați furnizat dovada că ați trimis înapoi produsele, fiind valabilă data cea mai apropiată."

5. În cazul în care consumatorul a recepționat produse în legătură cu contractul, introduceți următoarele:

a) introduceți:

- "Vom recupera produsele."; sau

- "Expediați produsele sau înmânați-le direct nouă sau. . . [se introduce numele și, dacă este cazul, adresa poștală a persoanei autorizate de dumneavoastră să primească produsele], fără întârzieri nejustificate și, în orice caz, în decurs de maximum 14 zile de la data la care ne-ați comunicat retragerea. Termenul este respectat dacă produsele sunt trimise înapoi înainte de expirarea perioadei de 14 zile.";

b) introduceți:

- "Vom suporta costul returnării produselor.";

- "Va trebui să suportați costul direct al returnării produselor.";

- Dacă, într-un contract la distanță, nu vă oferiți să suportați costul returnării produselor, iar produsele, prin natura lor, în mod normal nu pot fi returnate prin poștă: "Va trebui să suportați costul direct al returnării produselor, . . . lei/[introduceți cuantumul]."; sau, dacă costul returnării produselor nu poate fi calculat cu anticipație în mod rezonabil: "Va trebui să suportați costul direct al returnării produselor. Costul aproximativ este estimat la maximum lei/[introduceți cuantumul]."; sau

- Dacă, în cazul contractelor în afara spațiilor comerciale, produsele, prin natura lor, nu pot fi returnate în mod normal prin poștă și au fost livrate la domiciliul consumatorului în momentul încheierii contractului: "Vom recupera produsele și vom suporta costurile aferente."; și

c) introduceți: "Sunteți responsabil doar pentru diminuarea valorii produselor care rezultă din manipulări, altele decât cele necesare pentru determinarea naturii, calităților și funcționării produselor."

6. În cazul unui contract de prestări de servicii sau privind furnizarea de apă, gaze naturale sau electricitate, atunci când acestea nu prevăd vânzarea într-un volum limitat sau într-o cantitate stabilită, sau de energie termică, introduceți următoarele: "Dacă ați solicitat începerea prestării serviciilor sau a furnizării de apă/gaze naturale/energie electrică/energie termică [tăiați mențiunile inutile] în perioada de retragere, ne datorați o sumă proporțională cu serviciile furnizate până în momentul în care ne-ați comunicat exercitarea dreptului de retragere din prezentul contract, în raport cu acoperirea totală a contractului."

B. Model de formular de retragere

Prezentul formular se trimite înapoi completat doar dacă doriți să vă retrageți din contract.

- Către [aici se introduce numele, adresa poștală și, dacă este cazul, numărul de telefon, numărul de fax și adresa de e-mail ale profesionistului]:

- Vă informez/Vă informăm (*) prin prezenta cu privire la retragerea mea/noastră (*) din contractul referitor la vânzarea următoarelor produse (*) /prestarea următoarelor servicii (*)

- Comandate la data (*) /primite la data (*)

(*) A se elimina mențiunea inutilă, după caz.

- Numele consumatorului (consumatorilor)

- Adresa consumatorului (consumatorilor)

- Semnătura consumatorului (consumatorilor) (doar în cazul în care acest formular este notificat pe hârtie)

- Data

Ordonanța nr. 85/2004 privind protecția consumatorilor la încheierea și executarea contractelor la distanță privind serviciile financiare

În vigoare de la 26 septembrie 2004

Formă aplicabilă de la 13 mai 2008

Consolidarea din data de **05 noiembrie 2019** are la bază [republicarea din Monitorul Oficial, Partea I](#) nr. 365 din 13 mai 2008

Include modificările aduse prin următoarele acte: OUG [65/2009](#); L [196/2010](#).

Ultimul amendament în 01 noiembrie 2010.

Art. 1. - Prezenta ordonanță reglementează condițiile de informare a consumatorilor în vederea încheierii și executării contractelor la distanță privind serviciile financiare dintre furnizorii de servicii financiare și consumatori.

Art. 2. - (1) În cazul contractelor pentru servicii financiare care includ un contract inițial de prestări servicii, urmat în timp de executarea unor operațiuni financiare succesive sau a unei serii de operațiuni distincte de aceeași natură, care pot fi considerate ca formând un întreg, indiferent dacă acestea fac obiectul unui singur contract sau al mai multor contracte succesive, denumite în continuare operațiuni, prevederile prezentei ordonanțe se aplică numai contractului inițial.

(2) În cazul în care nu există un contract inițial de prestări servicii în sensul celui prevăzut la alin. (1), dar între aceleași părți contractuale se execută, eșalonat în timp, operațiuni succesive sau operațiuni distincte de aceeași natură, prevederile art. 4-6 se aplică numai în momentul în care se execută prima operațiune.

(3) În situația prevăzută la alin. (2), în cazul în care timp de peste un an nu se execută nicio operațiune de aceeași natură, următoarea operațiune pusă în executare va fi considerată ca fiind prima dintr-o nouă serie de operațiuni, dispozițiile art. 4-6 aplicându-se în mod corespunzător.

Art. 3. - În sensul prezentei ordonanțe, termenii și expresiile de mai jos se definesc după cum urmează:

a) contract la distanță - contractul de furnizare de servicii financiare încheiat între un furnizor și un consumator, în cadrul unui sistem de vânzare la distanță sau al unui sistem de furnizare de servicii organizat de către furnizor care utilizează în mod exclusiv, înainte și la încheierea acestui contract, una sau mai multe tehnici de comunicație la distanță;

b) serviciu financiar - orice serviciu bancar, de credit, de asigurare, pensii individuale, servicii de investiții financiare reglementate de Legea [nr. 297/2004](#) privind piața de capital, cu modificările și completările ulterioare, sau orice servicii referitoare la plata în natură;

c) furnizor - orice persoană juridică sau persoană fizică, publică sau privată, abilitată conform legii, care, în cadrul activităților sale profesionale sau comerciale, are calitatea de furnizor de servicii financiare stipulate în contractul la distanță;

d) consumator - orice persoană fizică sau grup de persoane fizice constituite în asociații, care, în cadrul contractelor reglementate de prezenta ordonanță, acționează în scopuri din afara activității sale comerciale, industriale sau de producție, artizanale ori liberale;

e) tehnică de comunicație la distanță - orice mijloc care, fără a necesita prezența fizică simultană a celor două părți, consumator și furnizor, poate fi folosit pentru comercializarea ori promovarea la distanță a serviciilor financiare;

f) suport durabil - orice instrument ce permite consumatorului păstrarea informațiilor ce îi sunt comunicate și accesul la acestea pentru o perioadă de timp corespunzătoare scopului informației, cu posibilitatea de a fi consultate ori de câte ori este necesar, și care să permită reproducerea nemodificată a conținutului lor;

g) operator sau furnizor de comunicație - orice persoană fizică sau juridică, publică sau privată, a cărei activitate profesională, economică sau comercială constă în a pune la dispoziția furnizorilor definiți la lit. c) una sau mai multe tehnici de comunicație la distanță.

Art. 4. - (1) Înainte de încheierea unui contract la distanță sau la momentul prezentării ofertei, furnizorul are obligația de a informa consumatorul în timp util, corect și complet asupra următoarelor elemente referitoare la identificarea sa privind, cel puțin:

a) denumirea furnizorului, forma de organizare, activitatea sa principală, adresa sediului social sau, după caz, domiciliul stabil și modalitățile de contactare a acestuia, telefon/fax, e-mail, registrul comerțului în care este înregistrat și codul unic de înregistrare;

b) denumirea reprezentantului din țara unde consumatorul are reședința, activitatea principală, adresa sediului social sau, după caz, domiciliul stabil al acestuia și modalitățile de contactare a acestuia, numărul de telefon/fax, adresa de e-mail, registrul comerțului în care este înregistrat și codul unic de înregistrare, dacă un astfel de reprezentant există;

c) denumirea intermediarului, calitatea în care acesta acționează în relația cu consumatorul, adresa sediului social sau, după caz, domiciliul stabil al acestuia și modalitățile de contactare a acestuia, numărul de telefon/fax, adresa de e-mail, registrul comerțului în care este înregistrat și codul unic de înregistrare, atunci când consumatorul tratează cu un intermediar;

d) în cazul în care activitatea furnizorului necesită o autorizare specială, acesta este obligat să furnizeze, complementar informațiilor prevăzute la lit. a) și b), și datele de identificare, adresa și modalitățile de contactare a autorității emitente a autorizației, inclusiv numărul de telefon/fax și adresa de e-mail ale acesteia.

(2) Informațiile referitoare la serviciul financiar ce urmează a fi prestat trebuie să fie oferite consumatorului de către furnizor în timp util, corect și complet, înainte de încheierea unui contract la distanță sau la momentul prezentării ofertei, asupra următoarelor elemente:

a) descrierea caracteristicilor esențiale ale serviciului financiar respectiv;

b) prețul total pe care consumatorul îl are de plătit pentru achiziționarea serviciului financiar, inclusiv toate comisioanele, taxele, costurile suplimentare ori cheltuielile aferente și toate tarifele, achitate direct de către consumator ori achitate prin intermediul furnizorului, iar în cazul în care nu poate fi indicat un preț total precis al serviciului financiar respectiv, furnizorul este obligat să informeze consumatorul asupra modalității de calcul necesare verificării costului total;

- c) elementele specifice anumitor operațiuni privind existența unor riscuri speciale asociate contractării serviciilor financiare ori caracteristicile specifice acestora sau referitoare la posibilitatea unei variații a prețului total în funcție de piețele financiare ori bursiere, asupra cărora furnizorul nu are influență și nu poate fi prezentată o estimare a evoluției viitoare raportată la performanțele statistice precedente;
- d) existența sau posibilitatea existenței unor taxe și/sau costuri suplimentare care nu sunt plătite prin intermediul furnizorului sau impuse de acesta;
- e) orice limită de timp sau data până la care informațiile furnizate sunt valabile;
- f) modalitățile de plată și de realizare a plății;
- g) orice cost suplimentar contractat de consumator, rezultat din utilizarea de către acesta a mijloacelor de comunicare la distanță, dacă se percep de către furnizor astfel de costuri adiționale.

(3) Informațiile referitoare la contractul la distanță ce urmează a fi încheiat trebuie să fie oferite consumatorului de către furnizor în timp util, corect și complet, înainte de încheierea unui contract la distanță sau la momentul prezentării ofertei, asupra următoarelor elemente:

- a) existența sau inexistența dreptului de denunțare unilaterală prevăzut la art. 9 și, în situația în care acest drept este stipulat, se vor preciza termenul și condițiile în care acesta poate fi exercitat, inclusiv o precizare a informațiilor privind plata sumelor pe care consumatorul poate fi obligat să le plătească potrivit art. 13 alin. (1), precum și a consecințelor ce decurg din neexercitarea acestui drept;
- b) durata minimă pentru care se încheie contractul la distanță, în cazul prestării unor servicii financiare cu caracter permanent sau periodic;
- c) informarea privind dreptul părților de a rezilia contractul înainte de termen sau de denunțare unilaterală a contractului, în temeiul unei clauze contractuale, dar în alte cazuri decât cele prevăzute la art. 9, inclusiv informarea cu privire la orice penalități impuse prin contract în astfel de cazuri;
- d) indicarea modalităților practice de exercitare a dreptului de denunțare unilaterală a contractului, între altele și indicarea adresei la care poate fi expediată notificarea de denunțare unilaterală a contractului;
- e) statul sau statele ale căror norme sunt avute în vedere de către furnizor ca temei juridic al raportului contractual cu consumatorul, în scopul încheierii unui contract la distanță;
- f) orice clauză contractuală prin care este indicată legea aplicabilă și/sau instanța competentă în soluționarea eventualelor litigii între părți;
- g) în ce limbă sau în care dintre limbile oficiale ale unui stat sunt formulați termenii și condițiile contractuale, informațiile prelabile prevăzute la art. 4 și 5, care va/vor fi limba sau limbile în care furnizorul a convenit de comun acord cu consumatorul să comunice pe durata derulării contractului la distanță.

(4) Furnizorul este obligat să ofere consumatorului, înainte de încheierea unui contract la distanță sau la momentul prezentării ofertei, informații privind căile de soluționare a litigiilor dintre părți, și anume:

- a) posibilitatea apelării la proceduri extrajudiciare anterioare sesizării instanței de judecată, de către consumator, care are calitatea de parte contractuală, și, de asemenea, care sunt modalitățile consumatorului de apelare la aceste proceduri;
- b) existența unor fonduri de garantare sau a altor mecanisme de compensare, altele decât cele prevăzute de Ordonanța Guvernului [nr. 39/1996](#) privind înființarea și funcționarea Fondului de

garanțare a depozitelor în sistemul bancar, republicată, cu modificările și completările ulterioare, de Legea [nr. 297/2004](#), cu modificările și completările ulterioare, și de reglementările privind Fondul de compensare a investitorilor emise de Comisia Națională a Valorilor Mobiliare în aplicarea Legii nr. 297/2004, cu modificările și completările ulterioare.

(5) Informațiile prevăzute la alin. (1)-(4), al căror scop comercial trebuie să rezulte fără echivoc, vor fi comunicate în mod clar, ușor de înțeles de către consumator, prin orice mijloc adaptat tehnicii de comunicație la distanță utilizate, ținându-se seama de principiile de bună practică comercială în tranzacții și de principiile care guvernează protecția minorilor și a altor persoane lipsite de capacitate de exercițiu, precum și de principiile referitoare la bunele moravuri.

Art. 5. - (1) În cazul în care mijlocul de comunicație la distanță este telefonul sau orice alt mijloc ce implică vorbirea directă, la începutul convorbirii furnizorul are obligația de a informa consumatorul, în mod complet, corect și precis asupra:

- a) datelor sale de identificare;
- b) scopului comercial al apelului.

(2) Cu condiția obținerii consimțământului expres al consumatorului, furnizorul trebuie să prezinte numai următoarele informații:

- a) identitatea persoanei care a contactat consumatorul din partea furnizorului și în ce calitate reprezintă furnizorul;
- b) descrierea caracteristicilor esențiale ale serviciului financiar;
- c) prețul total pe care consumatorul îl are de plătit pentru achiziționarea serviciului financiar, inclusiv toate comisioanele, taxele, costurile suplimentare ori cheltuielile aferente și toate tarifele, achitate direct de către consumator ori achitate prin intermediul furnizorului, iar în cazul în care nu poate fi indicat un preț total precis al serviciului financiar respectiv, furnizorul este obligat să informeze consumatorul asupra modalității de calcul necesare verificării costului total;
- d) existența sau posibilitatea existenței unor taxe și/sau costuri suplimentare care nu sunt plătite prin intermediul furnizorului sau impuse de acesta;
- e) existența sau inexistența dreptului de denunțare unilaterală prevăzut la art. 9 și, în situația în care acest drept este stipulat, se vor preciza termenul și condițiile în care acesta poate fi exercitat, inclusiv o precizare a informațiilor privind plata sumelor pe care consumatorul poate fi obligat să le plătească potrivit art. 13 alin. (1), precum și a consecințelor ce decurg din neexercitarea acestui drept.

(3) Furnizorul este obligat să informeze consumatorul despre faptul că orice alte informații suplimentare sunt disponibile la cerere și, totodată, să indice natura acestor informații. În toate situațiile furnizorul trebuie să ofere informațiile complete atunci când își îndeplinește obligațiile ce îi revin potrivit art. 7.

Art. 6. - (1) Informațiile referitoare la obligațiile contractuale vor fi comunicate consumatorului în faza precontractuală. Aceste informații trebuie să fie în conformitate cu obligațiile contractuale rezultate din legea aplicabilă contractului la distanță, în cazul încheierii lui.

(2) În cazul în care în legislația națională care transpune prevederi comunitare există dispoziții care reglementează serviciile financiare, precum și care conțin condiții de informare prealabilă, suplimentare față de cele menționate la art. 4 alin. (1)-(4), acestea se aplică în continuare.

(3) Obligația de a-l informa pe consumator ori pe furnizor, potrivit dispozițiilor prezentei ordonanțe, nu poate fi înlăturată prin invocarea secretului comercial sau profesional și nu poate fi limitată sau înlăturată prin clauze contractuale.

(4) În cazul în care serviciilor financiare ce fac obiectul prezentei ordonanțe le sunt aplicabile și prevederile Ordonanței de urgență a Guvernului [nr. 113/2009](#) privind serviciile de plată, cu modificările ulterioare, dispozițiile privind informarea prevăzute la art. 4 alin. (1)-(4), cu excepția celor cuprinse la art. 4 alin. (2) lit. c)-g), la art. 4 alin. (3) lit. a), d) și e), precum și la art. 4 alin. (4) lit. b) din prezenta ordonanță se înlocuiesc cu dispozițiile art. 91-93 și cu cele ale art. 97-99 din Ordonanța de urgență a Guvernului nr. 113/2009, cu modificările ulterioare.

Art. 7. - (1) Furnizorul va comunica consumatorului, în totalitate, termenii și condițiile contractuale și informațiile prevăzute la art. 4 și 6, în scris, pe hârtie sau pe orice suport durabil disponibil și accesibil consumatorului, în timp util, înainte ca acesta să aibă obligații rezultate din semnarea unui contract la distanță sau din acceptarea unei oferte a unui astfel de serviciu financiar la distanță.

(2) În cazul în care, la cererea expresă a consumatorului, contractul a fost încheiat prin utilizarea unor mijloace de comunicare la distanță care nu permit îndeplinirea procedurii prealabile de informare prevăzute la alin. (1), furnizorul își va îndeplini obligațiile ce îi revin, imediat după încheierea contractului la distanță.

(3) Pe toată durata derulării contractului, consumatorul are dreptul să solicite comunicarea condițiilor și prevederilor contractuale potrivit alin. (1), pe suport hârtie. Complementar, consumatorul are dreptul de a schimba mijlocul de comunicație folosit, exceptând situația în care mijlocul ales este incompatibil cu contractul încheiat sau cu natura serviciului financiar furnizat.

Art. 8. - Dacă părțile nu au convenit altfel, momentul încheierii contractului la distanță privind serviciile financiare îl constituie momentul primirii mesajului de confirmare de către consumator, referitor la comanda sa.

Art. 9. - Consumatorul are dreptul de a denunța unilateral contractul la distanță, în termen de 14 zile calendaristice, fără penalități și fără a fi necesară invocarea vreunui motiv. În cazul contractelor la distanță care au ca obiect asigurările de viață și contractele referitoare la operațiuni privind pensiile individuale, termenul în care consumatorul își poate exercita dreptul de denunțare unilaterală este de 30 de zile calendaristice.

Art. 10. - Termenul prevăzut la art. 9 începe să curgă:

a) din ziua încheierii contractului la distanță, cu excepția cazurilor referitoare la contractul care are ca obiect asigurarea de viață menționată la art. 9 și pentru care acesta va începe să curgă de la data când consumatorul este informat că s-a încheiat contractul la distanță; sau

b) din ziua în care consumatorul primește termenii și condițiile contractuale și informațiile în condițiile prevăzute de art. 7 alin. (1) sau (2), dacă această dată este ulterioară datei la care se face referire la lit. a).

Art. 11. - (1) Dreptul de denunțare unilaterală a contractului nu se aplică în cazul serviciilor financiare al căror preț depinde de fluctuațiile pieței financiare și care nu poate fi influențat de furnizor, care pot apărea în perioada de denunțare unilaterală a contractului, cum ar fi serviciile referitoare la:

a) operațiuni de schimb valutar;

- b) instrumente ale pieței monetare, inclusiv titluri de stat cu scadența mai mică de un an și certificate de depozit;
- c) valori mobiliare;
- d) titluri de participare la organisme de plasament colectiv;
- e) contracte futures financiare, inclusiv contracte similare cu decontare finală în fonduri;
- f) contracte forward pe rata dobânzii - FRA;
- g) swapuri pe rata dobânzii, curs de schimb și acțiuni;
- h) opțiuni pe orice instrument financiar prevăzut la lit. b)-e), inclusiv contracte similare de decontare finală în fonduri; această categorie include și opțiuni pe curs de schimb și rata dobânzii.

(2) Dreptul de denunțare unilaterală a contractului nu se aplică:

- a) polițelor de asigurare de călătorie și pentru bagaje sau altor polițe de asigurare pe termen scurt cu o durată de cel mult o lună calendaristică;
- b) contractelor executate integral de ambele părți la cererea expresă a consumatorului, formulată înainte ca acesta să-și exercite dreptul de denunțare unilaterală a contractului;

c) ~~Abrogat(ă)~~

d) ~~Abrogat(ă)~~

e) ~~Abrogat(ă)~~

(3) Prevederile prezentei ordonanțe, referitoare la dreptul de denunțare, nu se aplică contractelor de credit reglementate de art. 8 din Legea [nr. 282/2004](#) privind protecția dobânditorilor cu privire la unele aspecte ale contractelor purtând asupra dobândirii unui drept de utilizare pe durată limitată a unor bunuri imobiliare și de art. 9 din Ordonanța Guvernului [nr. 130/2000](#) privind protecția consumatorilor la încheierea și executarea contractelor la distanță, republicată.

Art. 12. - (1) În cazul exercitării dreptului de denunțare unilaterală a contractului, consumatorul va notifica furnizorul, conform informațiilor primite de la acesta potrivit art. 4 alin. (3) lit. d), înainte de expirarea termenului prevăzut de art. 9, prin orice mijloc care poate fi probat. Termenul va fi considerat respectat dacă notificarea formulată pe suport hârtie sau alt suport durabil, disponibil și accesibil destinatarului, este expediată înaintea expirării termenului în care acest drept poate fi exercitat.

(2) Dacă unui contract la distanță pentru un serviciu financiar încheiat la un anumit moment i se conexează un alt contract la distanță pentru servicii oferite de furnizor sau de un terț pe baza unui contract între terț și furnizor, acest contract adițional la distanță se va rezilia, fără plata unor penalități sau costuri suplimentare, dacă consumatorul își exercită dreptul său de denunțare unilaterală prevăzut de art. 9.

Art. 13. - (1) În cazul exercitării dreptului de denunțare unilaterală a contractului conform art. 9, consumatorului îi poate fi solicitată achitarea, fără întârzieri nejustificate, a cheltuielilor aferente serviciului deja furnizat, în conformitate cu clauzele contractuale, fără alte costuri suplimentare. Executarea contractului poate începe numai după ce consumatorul și-a dat consimțământul în acest sens.

(2) Cheltuielile prevăzute la alin. (1) nu vor putea:

- a) să depășească o sumă stabilită proporțional cu perioada în care serviciul financiar a fost furnizat, raportată la durata totală a contractului;

b) să fie prevăzute ca plată în orice situație în care suma respectivă poate fi considerată ca penalitate.

(3) Prin excepție de la prevederile alin. (1), în cazul denunțării contractelor de asigurare, consumatorul nu va fi obligat la cheltuieli.

(4) Furnizorul nu poate solicita consumatorului să plătească cheltuielile prevăzute la alin. (1) fără a face dovada că acesta a fost informat în timp util în ceea ce privește obligativitatea plății acestor cheltuieli, conform art. 4 alin. (3) lit. a). Consumatorul nu poate fi obligat să efectueze plata dacă furnizorul a început executarea contractului înaintea expirării perioadei de denunțare, fără existența unei cereri prealabile a consumatorului sau a unui acord expres al acestuia.

(5) În termen de 30 de zile calendaristice de la primirea notificării, furnizorul este obligat să ramburseze fără nicio întârziere orice sume primite conform contractului la distanță, cu excepția sumelor prevăzute la alin. (1), termen ce curge din ziua în care furnizorul a primit notificarea de denunțare unilaterală a contractului.

(6) Consumatorul este obligat să restituie furnizorului orice sumă și/sau bunuri ce i-au fost furnizate de acesta, fără întârziere, în termen de maximum 30 de zile calendaristice, termen ce curge din ziua în care consumatorul a expediat notificarea de denunțare unilaterală a contractului.

Art. 14. - [Abrogat\(ă\)](#)

Art. 15. - În cazul livrărilor pentru care nu există o comandă prealabilă, consumatorul este exonerat de orice contraprestație, lipsa răspunsului neavând valoare de consimțământ.

Art. 16. - Necesită acordul prealabil al consumatorului, exprimat în mod expres, următoarele tehnici de comunicație la distanță:

a) sistem automatizat de apel fără intervenție umană de tipul automatelor de apel;

b) telecopiator sau fax.

Art. 17. - (1) Utilizarea altor tehnici de comunicație individuală la distanță în afara celor prevăzute la art. 16 nu este permisă dacă există un refuz manifestat de consumator.

(2) Cheltuielile de utilizare a tehnicilor de comunicare la distanță în situațiile prevăzute la art. 16 și la alin. (1) nu vor fi suportate de către consumator.

Art. 18. - (1) Constituie contravenție încălcarea prevederilor art. 4, 6 și 7, referitoare la nerespectarea obligației de informare, și se sancționează cu amendă de la 500 lei la 3.000 lei.

(2) Constituie contravenție încălcarea prevederilor art. 13 alin. (5) privind nerespectarea termenelor de rambursare, precum și ale art. 16 și se sancționează cu amendă de la 1.000 lei la 4.000 lei.

(3) Constituie contravenție încălcarea prevederilor art. 17 și se sancționează cu amendă de la 500 lei la 1.000 lei.

Art. 19. - (1) Constatarea contravențiilor și aplicarea sancțiunilor prevăzute la art. 18 se fac la sesizarea consumatorilor sau din oficiu de către reprezentanții împuterniciți ai Autorității Naționale pentru Protecția Consumatorilor.

(2) Contravențiilor prevăzute la art. 18 le sunt aplicabile prevederile Ordonanței Guvernului [nr. 2/2001](#) privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea [nr. 180/2002](#), cu modificările și completările ulterioare.

Art. 20. - Consumatorii au dreptul de a solicita rezilierea contractului în situația în care furnizorul nu respectă prevederile art. 7, fără plata de penalități și fără costuri suplimentare.

Art. 21. - (1) Contractele pentru furnizarea de servicii financiare la distanță nu pot conține, chiar cu acordul expres al consumatorului, clauze de renunțare la drepturile prevăzute de prezenta ordonanță.

(2) În cazul în care părțile contractante aleg ca lege aplicabilă contractului la distanță legea unui stat ce nu face parte din Uniunea Europeană, iar contractul are o strânsă legătură cu teritoriul României sau cu al altor state membre ale Uniunii Europene și în cazul în care prezenta ordonanță are prevederi mai favorabile pentru consumator, se vor aplica acestea din urmă.

Art. 22. - (1) Prevederile prezentei ordonanțe se completează, în mod corespunzător, cu dispozițiile Legii [nr. 148/2000](#) privind publicitatea, cu modificările și completările ulterioare, ale Ordonanței Guvernului [nr. 21/1992](#) privind protecția consumatorilor, republicată, cu modificările și completările ulterioare, ale Legii [nr. 193/2000](#) privind clauzele abuzive din contractele încheiate între comercianți și consumatori, republicată, cu modificările și completările ulterioare, ale Ordonanței Guvernului [nr. 130/2000](#) privind protecția consumatorilor la încheierea și executarea contractelor la distanță, republicată, ale Legii [nr. 365/2002](#) privind comerțul electronic, republicată, ale Legii [nr. 296/2004](#) privind Codul consumului, republicată, ale Legii [nr. 297/2004](#) privind piața de capital, cu modificările și completările ulterioare, și ale reglementărilor Comisiei Naționale a Valorilor Mobiliare emise în aplicarea acesteia, ale Codului penal, ale Codului comercial, precum și cu cele ale Codului civil.

(2) Reglementările emise în aplicarea prezentei ordonanțe, care vizează activitățile prevăzute de Legea nr. 297/2004, cu modificările și completările ulterioare, vor fi elaborate de Autoritatea Națională pentru Protecția Consumatorilor împreună cu Comisia Națională a Valorilor Mobiliare.

Art. 23. - (1) Prevederile prezentei ordonanțe nu îngăduiesc dreptul consumatorilor de a formula reclamații și sesizări în apărarea intereselor lor pentru rezolvarea neînțelegerilor legate de încheierea și executarea contractelor la distanță privind serviciile financiare.

(2) Autoritatea competentă pentru soluționarea reclamațiilor și sesizărilor consumatorilor ce decurg din încheierea și executarea contractelor la distanță privind serviciile financiare este Autoritatea Națională pentru Protecția Consumatorilor.

(3) Plângerile consumatorilor și stabilirea procedurilor de despăgubire în materie de contracte pentru furnizarea de servicii financiare la distanță pot fi rezolvate și pe cale extrajudiciară, în baza dispozițiilor Legii [nr. 192/2006](#) privind medierea și organizarea profesiei de mediator.

Art. 24. - (1) Sarcina probei privind îndeplinirea obligațiilor furnizorului de informare a consumatorului, precum și sarcina probei existenței consimțământului consumatorului la încheierea contractului și, după caz, la executarea acestuia cad în sarcina furnizorului.

(2) Orice clauză contractuală prin care sarcina probei privind respectarea de către furnizor a unora sau a tuturor obligațiilor care îi incumbă în baza prezentei ordonanțe este atribuită consumatorului va fi considerată clauză abuzivă, conform Legii nr. 193/2000, republicată, cu modificările și completările ulterioare.

Art. 25. - Prezenta ordonanță transpune Directiva 2002/65/CE a Parlamentului European și a Consiliului din 23 septembrie 2002 privind comercializarea la distanță a serviciilor financiare de consum și de modificare a Directivei 90/619/CEE a Consiliului și a directivelor 97/7/CE și 98/27/CE, publicată în Jurnalul Oficial al Comunităților Europene (JOCE) nr. L 271 din 9 octombrie 2002, precum și prevederile art. 90 din Directiva 2007/64/CE a Parlamentului European și a Consiliului din 13

noiembrie 2007 privind serviciile de plată în cadrul pieței interne, de modificare a directivelor 97/7/CE, 2002/65/CE, 2005/60/CE și 2006/48/CE și de abrogare a Directivei 97/5/CE, publicată în Jurnalul Oficial al Uniunii Europene nr. L 319 din 5 decembrie 2007.

Art. 26. - Prezenta ordonanță intră în vigoare la 30 de zile de la data publicării în Monitorul Oficial al României, Partea I.

Ordinul nr. 553/2019 privind reglementarea procedurii de avizare a instrumentelor de plată electronică cu acces la distanță

În vigoare de la 14 iunie 2019

Publicat în Monitorul Oficial, Partea I nr. 485 din 14 iunie 2019. Formă aplicabilă la [05 noiembrie 2019](#).

În temeiul art. 4 alin. (1) [pct. 53](#) din Hotărârea Guvernului nr. 36/2017 privind organizarea și funcționarea Ministerului Comunicațiilor și Societății Informaționale, cu modificările și completările ulterioare, având în vedere prevederile art. 129 alin. (1) pct. 2 [lit. c](#)) din Regulamentul Băncii Naționale a României nr. 3/2018 privind monitorizarea infrastructurilor pieței financiare și a instrumentelor de plată și prevederile Legii [nr. 135/2007](#) privind arhivarea documentelor în formă electronică, republicată, ministrul comunicațiilor și societății informaționale emite prezentul ordin.

CAPITOLUL I Dispoziții generale

Art. 1. - Prezentul ordin reglementează procedura de eliberare a avizului Ministerului Comunicațiilor și Societății Informaționale pentru instrumentele de plată electronică cu acces la distanță furnizate de către prestatorii de servicii de plată autorizați de Banca Națională a României, de tip internet- banking, home-banking, phone-banking sau mobile-banking, necesar pentru notificarea acestora către BNR, precum și înscrierea auditorilor IT, conform procedurii prevăzute în cap. III.

Art. 2. - Prezentul ordin stabilește cerințele minime de securitate ale sistemelor informatice pe care trebuie să le îndeplinească prestatorii de servicii de plată prevăzuți la [art. 1](#), prin intermediul cărora este furnizat instrumentul de plată electronică cu acces la distanță.

Art. 3. - În înțelesul prezentului ordin, termenii, expresiile și abrevierile de mai jos au următoarele semnificații:

1. amenințare - cauza potențială a unui incident nedorit, care poate dăuna unui sistem sau unei organizații;

2. administrator al arhivei electronice - persoana fizică sau juridică acreditată de autoritatea de reglementare și supraveghere specializată în domeniu să administreze sistemul electronic de arhivare și documentele arhivate în cadrul arhivei electronice;
3. arhivă electronică - sistemul electronic de arhivare, împreună cu totalitatea documentelor în formă electronică arhivate;
4. atac etic/test de penetrare - un test direct al eficacității de apărare a securității prin mimarea acțiunilor atacatorilor reali/test al sistemelor informatice realizat printr-o simulare a unui atac real asupra rețelelor, sistemelor și programelor informatice utilizate de entitatea testată sau auditată, după caz, efectuat cu acordul managementului prestatorului;
5. audit IT - activitatea de colectare și evaluare a unor probe pentru a determina dacă sistemul informatic respectă parametrii de performanțe și de lucru conform cerințelor de proiectare, dacă asigură funcționalitățile necesare cerințelor de afaceri și respectarea legislației în domeniu, dacă este securizat, dacă menține integritatea datelor prelucrate și stocate, dacă permite atingerea obiectivelor strategice ale entității și utilizarea eficientă a resurselor informaționale;
6. auditor IT - persoana fizică autorizată care deține certificat de auditor IT sau persoana juridică cu personal certificat care derulează o activitate de auditare a sistemelor informatice, conform reglementărilor și bunelor practici în domeniu;
7. autentificare - procedură care permite prestatorului de servicii de plată să verifice identitatea unui utilizator al serviciilor de plată sau valabilitatea utilizării unui anumit instrument de plată și care include utilizarea elementelor de securitate personalizate ale utilizatorului;
8. aviz - actul administrativ emis de către Ministerul Comunicațiilor și Societății Informaționale în conformitate cu prevederile art. 129 alin. (1) pct. 2 [lit. c](#)) din Regulamentul Băncii Naționale a României nr. 3/2018;
9. BNR - Banca Națională a României;
10. centru de date - spațiu securizat, dotat cu tehnică de calcul și echipamente de comunicații prin intermediul cărora se primesc, se stochează și se transmit date în formă electronică;
11. comunicații/telecomunicații - sisteme de transmisie, precum și orice alte resurse care permit transportul semnalelor prin fir, radio, fibră optică sau orice alte mijloace electromagnetice, precum și tehnologiile utilizate în cadrul proceselor de comunicare, care presupun existența unui mediu informatic constituit din echipamente hardware, software specializat, precum și dispozitive electronice de transmisie/recepție date;
12. continuitatea activității - starea de funcționare neîntreruptă a operațiunilor, ce presupune măsuri organizaționale, tehnice și de personal utilizate pentru a asigura continuitatea serviciilor critice după o întrerupere cauzată de producerea unui eveniment perturbator și pentru reluarea treptată a tuturor serviciilor în cazul unui eveniment perturbator major;

13. controale informatice - totalitatea politicilor, procedurilor, practicilor, ghidurilor, mijloacelor de gestionare a riscurilor și a structurilor organizaționale informatice proiectate să ofere o asigurare rezonabilă asupra faptului că obiectivele afacerii vor fi atinse, evenimentele nedorite vor fi prevenite sau detectate și corectate;
14. date (informatice) - orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic, incluzându-se și orice program informatic care poate determina realizarea unei funcții similare de către un sistem informatic;
15. disponibilitate - capacitatea unui serviciu IT sau a unui element de configurație IT de a efectua funcțiile agreate;
16. emitent - prestator de servicii de plată care emite și pune la dispoziția deținătorului un instrument de plată electronică, în baza unui contract încheiat cu deținătorul;
17. externalizare servicii IT - utilizarea de către o entitate a unui furnizor extern de servicii IT, în vederea desfășurării de către aceasta, pe bază contractuală și în mod continuu sau pentru o anumită perioadă, a operațiunilor aferente suportului tehnic sau procesării, necesare desfășurării activității efectuate în mod obișnuit de către entitatea în cauză;
18. furnizor de servicii de arhivare electronică - orice persoană fizică sau juridică acreditată să presteze servicii legate de arhivarea electronică;
19. furnizor de servicii IT externalizate - furnizori care oferă servicii de mentenanță, administrare software (aplicații), servicii de administrare rețea, baze de date și sisteme de operare, furnizori de software, servicii de hosting, co-locare și cloud. Furnizorii de servicii de comunicații nu fac obiectul prezentei definiții;
20. incident operațional sau de securitate - un eveniment unic sau o serie de evenimente corelate, neprevăzute de către prestatorul serviciului de plată, care are un impact negativ asupra integrității, disponibilității, confidențialității, autenticității și/sau continuității serviciilor aferente plăților;
21. instrument de plată electronică cu acces la distanță - set de proceduri, care se bazează pe o soluție informatică, de tipul: internet-banking, home-banking, phone-banking, mobile-banking, care permite utilizatorului inițierea de operațiuni de plată;
22. instrument de plată electronică cu acces la distanță tip internet-banking - acel instrument de plată cu acces la distanță care se bazează pe tehnologia internet (world wide web) și pe sistemele informatice ale emitentului;
23. instrument de plată la distanță tip home-banking - acel instrument de plată cu acces la distanță care se bazează pe o aplicație software a emitentului instalată la sediul deținătorului, pe o stație de lucru individuală sau în rețea;
24. instrument de plată electronică cu acces la distanță tip mobile-banking - acel instrument de plată cu acces la distanță care presupune utilizarea unui echipament mobil (telefon, tabletă, PDA - Personal Digital Assistant etc.) și a unor servicii oferite de către operatorii de telecomunicații;
25. instrument de plată electronică cu acces la distanță tip phone-banking - acel instrument de plată cu acces la distanță care facilitează accesul clienților la produsele și serviciile unui prestator de servicii de plată prin utilizarea telefonului drept canal alternativ de acces de la distanță;

26. MCSI - Ministerul Comunicațiilor și Societății Informaționale;
27. operațiune de plată - acțiune inițiată de plătitor sau de o altă persoană în numele și pe seama plătitorului ori de beneficiarul plății cu scopul de a depune, de a transfera sau de a retrage fonduri, indiferent de orice obligații subsecvente între plătitor și beneficiarul plății;
28. ordin de autorizare centru de date - document emis de MCSI care atestă că un centru de date îndeplinește toate condițiile cerute de legislația în vigoare în vederea desfășurării operațiunilor de arhivare electronică;
29. prelucrarea datelor - orice operațiune sau set de operațiuni efectuate asupra datelor sau asupra seturilor de date, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;
30. procedură de autorizare a unui centru de date - metodă de evaluare sistematică, documentată, periodică și obiectivă a performanței centrului de date, a sistemului de management și a proceselor destinate protecției arhivelor electronice, în scopul verificării respectării cerințelor prevăzute de legislația în vigoare;
31. prestator de servicii de plată - entitate autorizată să presteze servicii de plată pe teritoriul României, respectiv instituții de credit, instituții de plată și instituții emitente de monedă electronică;
32. prestator - prestator de servicii de plată specifice instrumentelor financiare de plată electronică cu acces la distanță;
33. plan de securitate - documentul ce descrie totalitatea măsurilor tehnice și administrative care sunt luate de către emitent pentru utilizarea în condiții de siguranță a instrumentului de plată electronică cu acces la distanță;
34. raport de audit IT - instrumentul prin care se comunică scopul auditării, obiectivele urmărite, normele/standardele aplicate, perioada acoperită, natura, procedurile, constatările și concluziile auditului, precum și orice rezervă pe care auditorul IT o are asupra sistemului informatic auditat;
35. raport de testare IT - instrumentul prin care se comunică scopul testării, obiectivele urmărite, normele/standardele aplicate, perioada acoperită, natura, întinderea, procedurile, constatările și concluziile testării, precum și orice rezervă pe care echipa de testare o are asupra sistemului informatic testat;
36. Regulamentul Băncii Naționale a României [nr. 3/2018](#) - Regulamentul Băncii Naționale a României nr. 3/2018 privind monitorizarea infrastructurilor pieței financiare și a instrumentelor de plată, publicat în Monitorul Oficial al României, Partea I, nr. 713 din 16 august 2018;
37. risc de securitate - riscul care rezultă din procesele interne sau evenimentele externe eșuate sau necorespunzătoare, care au sau ar putea avea un impact negativ asupra disponibilității, integrității, confidențialității și asupra sistemelor de tehnologie a informației și a comunicațiilor și/sau asupra informațiilor utilizate pentru furnizarea serviciilor de plată;

38. securitate informatică - capacitatea unui sistem informatic, rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive, de a rezista, la un nivel de încredere dat, unei acțiuni accidentale sau răuvoitoare care ar putea compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate sau transmise ori a serviciilor conexe oferite de rețeaua sau de sistemul informatic respectiv sau accesibile prin intermediul acestora;

39. siguranță în funcționare - modalitate de gestionare a riscurilor specifice infrastructurii pieței financiare, respectiv a instrumentului de plată, în scopul asigurării funcționării conform nivelurilor de calitate a serviciilor și/sau orarului de funcționare asumat, fără a afecta în mod negativ încrederea participanților și a publicului;

40. sistem informatic - ansamblu de elemente intercorelate funcțional în scopul automatizării obținerii informațiilor necesare activităților operaționale și manageriale într-o entitate, prin intermediul serviciilor IT, al echipamentelor hardware și produselor software, proceduri manuale, baze de date și modele matematice pentru analiză, planificare, control și luarea deciziilor, utilizând componente de introducere și prelucrare date, componente de procesare precum servere, calculatoare, sisteme software de operare de bază, programe informatice, rețele de calculatoare și telecomunicații, componente de stocare și utilizatori, fără ca enumerarea să fie limitativă;

41. vulnerabilitate - este un punct slab (defect) în proiectarea, implementarea, operarea sau controlul intern al unui proces care ar putea expune sistemul la un risc de securitate.

Art. 4. - Cerințele minime de securitate ale sistemelor informatice pe care trebuie să le îndeplinească prestatorii de servicii de plată prevăzuți la [art. 1](#), prin intermediul cărora este furnizat instrumentul de plată electronică cu acces la distanță, se referă la:

1. confidențialitatea și integritatea comunicațiilor între emitent și beneficiarul instrumentului financiar de plată electronică cu acces la distanță;
2. mecanismele care să garanteze confidențialitatea și nerepudierea operațiunilor efectuate utilizând instrumentul de plată electronică cu acces la distanță;
3. autenticitatea părților care participă la tranzacții și existența metodelor de autentificare în concordanță cu nivelul de securitate al platformei software, precum și mijloacele de garantare a identității;
4. confidențialitatea, autenticitatea și integritatea informațiilor/datelor aferente tranzacțiilor efectuate cu ajutorul instrumentului de plată electronică, prin sistemul informatic al emitentului, în timpul procesării, stocării și arhivării acestora;
5. păstrarea secretului bancar;
6. trasabilitatea tranzacțiilor;
7. respectarea protecției datelor cu caracter personal în sistemele informatice;

8. controlul accesului fizic și logic la sistemul informatic și la platforma/aplicația software utilizate în procesul de furnizare a instrumentului financiar de plată electronică cu acces la distanță;
9. stocarea, păstrarea datelor înregistrate și jurnalizarea acestora, precum și păstrarea în siguranță a unor copii de rezervă ale datelor și aplicațiilor;
10. prevenirea/limitarea/înlăturarea impactului incidentelor de securitate informatică, reluarea în siguranță a activității și recuperarea informațiilor afectate;
11. detectarea, înregistrarea și gestionarea incidentelor de securitate informatică;
12. evaluarea riscurilor de securitate informatică și măsuri de gestionare a acestora;
13. asigurarea unui proces formal și continuu (cel puțin anual) de pregătire a resurselor umane implicate în operarea, mentenanța și administrarea instrumentelor de plată electronică cu acces la distanță și o evaluare anuală a acestora;
14. continuitatea serviciilor oferite clienților;
15. gestionarea și administrarea sistemului informatic;
16. impactul operațiilor de modificare a:
 - a) arhitecturii din cadrul sistemului informatic (componente hardware/software) și aplicațiilor software utilizate în ciclul de viață al instrumentului de plată electronică cu acces la distanță; și
 - b) planului de securitate specific securității aferente instrumentului de plată cu acces la distanță;
17. orice alte activități sau măsuri tehnice întreprinse pentru exploatarea în siguranță a sistemului informatic al emitentului.

Art. 5. - Măsurile tehnice și organizatorice întreprinse pentru îndeplinirea cerințelor enumerate la art. 4 vor fi în concordanță cu tehnologia utilizată și cu riscurile potențiale.

Art. 6. - Prestatorii au obligația de a implementa măsuri de securitate informatică, de a monitoriza continuu și de a evalua anual riscurile operaționale generate de utilizarea sistemelor informatice prin intermediul cărora este furnizat instrumentul de plată electronică cu acces la distanță, cu respectarea legislației interne și a reglementărilor comunitare.

Art. 7. - Documentele elaborate în format electronic, aferente instrumentului de plată electronică cu acces la distanță, vor fi arhivate conform legislației naționale privind arhivarea electronică, pe baza nomenclatorului arhivistic al prestatorului, în concordanță cu cerințele Legii Arhivelor Naționale [nr. 16/1996](#), republicată.

Art. 8. - (1) Prestatorii au obligația ca, anual, să efectueze teste de penetrare a aplicațiilor software și sistemelor informatice utilizate în ciclul de viață al instrumentului de plată electronică cu acces la distanță.

(2) Testele de penetrare menționate la alin. (1) se vor realiza de către echipe externe/interne, certificate în acest scop, care vor evalua securitatea informatică a aplicațiilor și sistemului informatic al prestatorului care furnizează instrumentul de plată electronică cu acces la distanță și vor fi finalizate cu un raport de testare.

(3) Raportul de testare pentru testele prevăzute la alin. (2) trebuie să fie aprobat de către reprezentantul legal al prestatorului și păstrat la sediul acestuia, care are obligația să îl prezinte auditorului IT, precum și MCSI, la solicitarea acestuia.

CAPITOLUL II Eliberarea avizului

Art. 9. - (1) Documentele necesare pentru eliberarea avizului sunt:

- a) cererea adresată MCSI, conform modelului prevăzut în anexa [nr.1](#);
- b) licența de funcționare/autorizația acordată de BNR sau notificarea transmisă către BNR de autoritatea competentă din statul membru de origine;
- c) descrierea funcțională a sistemului informatic și a aplicației software prin intermediul cărora este furnizat instrumentul de plată electronică cu acces la distanță;
- d) planul de securitate al sistemului informatic, semnat de către prestatorii de servicii de plată prevăzuți la [art.1](#), cuprinzând descrierea măsurilor tehnice și organizatorice prevăzute pentru asigurarea cerințelor cuprinse la [art.4](#);
- e) declarația reprezentantului legal din care să rezulte efectuarea testelor de penetrare menționate la [art.8](#), perioada de efectuare a testelor, precum și datele de identificare ale echipei de testare;
- f) certificările profesionale ale echipei de testare, recunoscute internațional. Certificările profesionale agreeate pentru efectuarea testelor de penetrare acceptate trebuie să fie în termenul de valabilitate și să se regăsească în lista prevăzută în anexa [nr.2](#);
- g) raportul de audit, care trebuie să îndeplinească următoarele condiții:
 1. să cuprindă elementele prevăzute în raportul de audit prezentat în anexa [nr.3](#), fără a se limita la acestea;
 2. să fie întocmit de către un auditor selectat din Lista auditorilor IT;
 3. data de întocmire a raportului de audit nu trebuie să depășească 180 de zile față de data depunerii documentației de avizare;
- h) declarația pe propria răspundere, din care să rezulte independența auditorului față de sistemul informatic auditat și față de prestatorul auditat;
- i) declarația pe propria răspundere a reprezentantului legal al prestatorului cu privire la respectarea, în cadrul procesului de furnizare a instrumentelor de plată electronică cu acces la distanță, a cerințelor Legii [nr.190/2018](#) privind măsuri de punere în aplicare a Regulamentului (UE)

[2016/679](#) al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei [95/46/CE](#) (Regulamentul general privind protecția datelor);

j) ordinul de acreditare ca administrator de arhivă electronică, în conformitate cu prevederile Legii [nr. 135/2007](#) privind arhivarea documentelor în formă electronică, republicată, sau contractul încheiat cu un administrator de arhivă electronică acreditat.

(2) MCSI va retrage avizul eliberat prestatorului dacă contractul de externalizare sau ordinul de acreditare a serviciilor de arhivare este suspendat/retras sau își pierde valabilitatea.

Art. 10. - (1) Documentele prevăzute la art. 9 [alin. \(1\)](#) se vor transmite către MCSI, în limba română, vor fi semnate de către reprezentantul legal al prestatorului de servicii de plată sau de către o persoană împuternicită de către acesta, în scris, și vor avea mențiunea "Conform cu originalul".

(2) Documentația va fi paginată și însoțită de un opis.

Art. 11. - Documentația aferentă planului de securitate va avea următoarea structură:

1. informații de identificare:

- a) denumirea prestatorului;
- b) denumirea instrumentului de plată electronică cu acces la distanță;
- c) categoria (internet-banking, home-banking, mobile-banking, phone-banking);
- d) statutul operațional al sistemului prin intermediul căruia este oferit instrumentul de plată electronică cu acces la distanță;
- e) anul intrării în producție;
- f) descrierea generală a soluției tehnice și dezvoltatorului aplicației;
- g) interconectarea sistemului;
- h) aria geografică în care instrumentul de plată cu acces la distanță poate fi utilizat;
- i) datele de contact ale persoanelor responsabile;

2. sensibilitatea sistemului:

- a) legislația aplicabilă;
- b) descrierea generală a sensibilității informațiilor gestionate de către sistem;

3. măsuri pentru securitatea sistemului:

- a) evaluarea și managementul riscurilor potențiale;
- b) identificarea, analizarea și remedierea riscurilor de securitate în conformitate cu cele mai bune practici în gestionarea acestora;
- c) măsurile tehnice de securitate implementate;

- d) situația cu înregistrarea și analizarea incidentelor de securitate informatică;
 - e) metodologia de recuperare a informațiilor în caz de dezastru și continuarea activității;
 - f) rapoartele de testare a funcționalității instrumentului efectuate în ultimele 12 luni;
 - g) codurile de conduită/condițiile de utilizare/contractul prin care este oferit instrumentul de plată electronică cu acces la distanță;
 - h) procedurile operaționale de exploatare;
 - i) măsurile aplicate pentru asigurarea securității fizice;
 - j) instruirea personalului propriu în legătură cu administrarea sistemului informatic;
 - k) instrucțiunile de utilizare a instrumentului de plată cu acces la distanță (manual de utilizare oferit clienților);
 - l) suportul tehnic oferit clienților care utilizează instrumentul de plată electronică cu acces la distanță;
4. orice alte informații relevante legate de măsurile luate de către emitent pentru a asigura exploatarea în siguranță a instrumentului de plată electronică cu acces la distanță.

CAPITOLUL III

Înscrierea în Lista auditorilor IT

Art. 12. - Lista auditorilor IT este gestionată de către MCSI și publicată pe site-ul acestuia.

Art. 13. - Auditorul IT care intenționează să presteze servicii de audit IT pentru prestatorii cărora le sunt incidente prevederile prezentului ordin are obligația înscrierii în Lista auditorilor IT prevăzută la [art. 12](#).

Art. 14. - Auditorul IT înscris în lista menționată la [art. 9](#) poate întocmi și raportul de audit în vederea autorizării centrelor de date, prevăzute în [Legea nr. 135/2007](#), republicată.

Art. 15. - Documentele necesare pentru înscrierea în Lista auditorilor IT, prevăzută la [art. 12](#), sunt următoarele:

1. cererea adresată MCSI, conform modelului prevăzut în anexa [nr. 4](#);
2. datele de identificare ale auditorului IT:
 - a) numele complet/denumirea și adresa/sediul - adresa completă;
 - b) adresa unde își desfășoară activitatea;
 - c) telefon/fax, e-mail, adresa paginii de internet;
 - d) certificat de înregistrare la Oficiul Național al Registrului Comerțului;

3. pentru auditorul IT persoană fizică certificată și pentru reprezentantul societății de audit IT, care vor semna raportul de audit, se depun următoarele documente:

- a) actul de identitate al auditorului IT, în copie;
- b) curriculum vitae al auditorului IT, datat și semnat, cu prezentarea experienței profesionale în auditarea IT a sistemelor informatice;
- c) dovada deținerii uneia dintre certificările profesionale specifice domeniului de audit al sistemelor informatice, menționate în anexa [nr. 5](#) (certificatul de auditor, în copie semnată și cu mențiunea "Conform cu originalul");
- d) dovada experienței în audit IT, concretizată în participarea la minimum cinci misiuni de audit în domeniul securității sistemelor informatice aparținând prestatorilor de servicii de plată, cu un total de cel puțin 30 de zile;
- e) certificat constatator emis de Oficiul Național al Registrului Comerțului, cu starea la zi a persoanei juridice, nu mai vechi de 30 de zile, în original;
- f) certificatul de cazier judiciar și certificatul de cazier fiscal, aflate în termenul de valabilitate, în original;
- g) contractul de asigurare de răspundere civilă profesională a auditorului IT, pentru suma asigurată de minimum 100.000 euro, valabil la data depunerii documentației, în copie semnată și cu mențiunea "Conform cu originalul".

Art. 16. - Înscrierea auditorului IT în Lista auditorilor IT sau transmiterea refuzului motivat al înscrierii se efectuează de MCSI în termen de maximum 30 de zile de la primirea dosarului complet al solicitantului.

Art. 17. - Orice modificare a documentației prevăzute la [art. 15](#) trebuie transmisă către MCSI în termen de maximum 30 de zile de la data efectuării modificării.

Art. 18. - Radierea auditorilor IT din lista prevăzută la [art. 12](#) se va efectua în oricare dintre următoarele situații:

- a) la cererea acestora;
- b) în cazul lichidării sau la declanșarea insolvenței;
- c) în cazul nerespectării prevederilor prezentului ordin;
- d) la expirarea contractului de asigurare de răspundere civilă profesională;
- e) la expirarea certificării profesionale.

Art. 19. - MCSI va transmite auditorului IT o notificare prealabilă prin care i se aduc la cunoștință motivele pentru care se va proceda la inițierea demersurilor pentru radierea din Lista auditorilor IT.

CAPITOLUL IV

Condiții privind desfășurarea auditului IT

Art. 20. - (1) Auditarea se va efectua în baza unui contract încheiat între prestatorul care a solicitat auditarea și un auditor înscris în Lista auditorilor IT.

(2) Prestatorul nu poate contracta auditarea cu același auditor IT pentru mai mult de 2 auditări consecutive.

(3) Prestatorul are obligația de a se asigura că în contractul de auditare sunt cuprinse în mod obligatoriu clauze cu privire la faptul că auditorul IT trebuie să respecte cerințele impuse pentru efectuarea auditului sistemelor informatice, în conformitate cu prevederile prezentului ordin și cu bunele practici în domeniu.

(4) Activitatea de auditare trebuie să respecte conduita etică și profesională, nu presupune încălcarea secretului profesional impus prin clauze contractuale sau prin prevederi legale și nu atrage niciun fel de răspundere asupra persoanei fizice și/sau juridice în cauză ca urmare a respectării prevederilor prezentului ordin.

Art. 21. - Perioada supusă auditării reprezintă perioada cuprinsă între două auditări consecutive.

Art. 22. - Pe timpul auditării, auditorul IT are obligația de a analiza situația deficiențelor și vulnerabilităților identificate, întocmită cu ocazia auditării precedente, precum și măsurile întreprinse de către prestator.

Art. 23. - Auditorul IT notifică MCSI, în scris, în maximum 10 zile de la constatare, orice fapt sau act care:

- a) este de natură să afecteze utilizarea în siguranță a instrumentului financiar de plată electronică cu acces la distanță;
- b) poate conduce la o opinie de audit cu rezerve, negativă sau imposibilitatea exprimării acesteia.

Art. 24. - În termen de maximum 10 zile de la solicitarea scrisă a MCSI, auditorul IT trebuie să comunice următoarele, fără a se limita la acestea:

- a) orice raport sau document care a fost adus la cunoștința prestatorului auditat;
- b) motivația de încetare a contractului de audit, dacă aceasta a avut loc înainte de finalizarea auditării.

Art. 25. - La finalizarea auditării, auditorii IT au obligația de a întocmi un raport de audit IT, care să cuprindă cel puțin elementele enumerate în raportul de audit prevăzut în anexa [nr. 3](#), dar fără a se limita la acestea.

Art. 26. - Pentru cazurile în care sistemul informatic și platforma/aplicația software utilizate în procesul de furnizare a instrumentului financiar de plată electronică cu acces la distanță sunt situate în afara țării, auditarea sistemului se va face astfel:

- auditorul IT extern român va audita sistemele din străinătate; sau

- auditorul IT extern român agreează auditarea sistemului din străinătate de către un auditor cu o certificare cuprinsă în lista certificărilor menționate în anexa [nr. 5](#) și preia responsabilitatea auditării.

Art. 27. - MCSI poate verifica derularea procesului de auditare, atât prin participarea la activitatea de auditare a auditorului IT, cât și prin prisma discuțiilor legate de dosarul de audit.

CAPITOLUL V

Cerințe aplicabile furnizorilor de servicii IT externalizate pentru sistemele informatice ale prestatorului

Art. 28. - Orice externalizare de servicii IT se realizează cu respectarea legislației naționale aplicabile Prestatorului.

Art. 29. - (1) Prestatorul are obligația de a specifica în documentația de avizare următoarele informații și documente, după caz:

a) descrierea serviciilor furnizate/externalizate;

b) datele de identificare ale furnizorului: adresa sediului social, telefon/fax, e-mail, pagina de internet;

c) certificat constatator emis de Oficiul Național al Registrului Comerțului, cu starea la zi a persoanei juridice, sau echivalentul acestuia pentru furnizorii externi înregistrați în alte state, în original sau copie conformă cu originalul;

d) documente în funcție de tipul serviciului sau activității desfășurate, astfel:

1. SR ISO/IEC 27001 sau certificări pentru standarde echivalente - pentru toți furnizorii de servicii IT externalizate;

2. certificări pentru furnizarea și dezvoltarea de programe informatice software;

3. act doveditor de respectare a condițiilor tehnice conform standardelor internaționale privind serviciile de găzduire sau externalizare prin intermediul centrelor de date;

4. acreditare pentru furnizarea de servicii de arhivare electronică.

(2) Certificările trebuie să fie emise de entități/organisme recunoscute pe plan intern și/sau internațional.

Art. 30. - (1) Prestatorul are obligația de a notifica MCSI încheierea contractului cu furnizorul de servicii IT externalizate în termen de maximum 14 zile de la data încheierii.

(2) Prestatorul are obligația ca, în cazul modificării unor informații și/sau documente prevăzute la [art. 29](#), să notifice MCSI și să depună originalul sau copia documentelor modificate în termen de maximum 60 de zile de la data efectuării modificării.

Art. 31. - (1) Prestatorul are obligația să se asigure că prevederile prezentului ordin sunt respectate de către toți furnizorii de servicii IT externalizate, inclusiv în cazul externalizărilor în lanț.

(2) Furnizorii de servicii IT externalizate vor permite MCSI și auditorului IT să verifice și/sau să auditeze sistemele sale informatice în contextul aplicării prevederilor prezentului ordin sau vor pune la dispoziția auditorului IT un raport de audit IT întocmit în conformitate cu standardele internaționale în domeniu.

CAPITOLUL VI

Cerințe privind raportarea

Art. 32. - (1) Prestatorul va raporta către MCSI, trimestrial, referitor la instrumentele de plată electronică cu acces la distanță, următoarele: numărul de utilizatori, numărul de plăți efectuate, valoarea plăților efectuate prin intermediul acestora, în formatul prezentat în anexa [nr. 6](#).

(2) Raportările pot fi transmise prin poștă, pe adresa Ministerului Comunicațiilor și Societății Informaționale, Bd. Libertății nr. 14, sectorul 5, cod 050706, sau prin e-mail, ca fișier atașat, pe adresa e-banking@comunicații.gov.ro, până la sfârșitul lunii următoare trimestrului pentru care se face raportarea.

CAPITOLUL VII

Dispoziții tranzitorii și finale

Art. 33. - (1) Documentele prevăzute la [art. 9](#) se înaintează către MCSI cu minimum 40 de zile înainte expirării avizului anterior și vor fi întocmite într-un singur exemplar.

(2) Avizul acordat este valabil 1 an de la data eliberării acestuia.

(3) Avizul acordat este netransmisibil.

Art. 34. - (1) MCSI va comunica solicitantului [decizia](#) sa cu privire la acordarea avizului, în termen de 40 de zile calendaristice de la data înregistrării cererii de eliberare a avizului.

(2) MCSI va remite solicitantului un exemplar al avizului, în termen de 3 zile calendaristice după acordarea acestuia.

(3) Forma avizului acordat este prevăzută în anexa [nr. 7](#).

Art. 35. - (1) Prestatorul va notifica MCSI orice dezvoltare, modificare a condițiilor de exploatare și a procedurilor operaționale, precum și a măsurilor tehnice de securitate aplicabile instrumentului, în termen de 30 de zile de la data când devin operaționale.

(2) Prestatorul va notifica MCSI, în termen de maximum 10 zile, orice incident de securitate care a afectat în mod direct clienții. Notificarea va cuprinde cauza și măsurile ce urmează a fi luate în vederea remedierii situației apărute.

(3) MCSI poate solicita un nou raport de audit pentru instrumentul financiar de plată electronică cu acces la distanță, după analizarea notificărilor prevăzute la [alin. \(1\)](#) și [\(2\)](#).

(4) MCSI poate retrage avizul și informează BNR dacă în termen de 60 de zile prestatorul nu prezintă raportul de audit prevăzut la alin. (3).

Art. 36. - (1) MCSI poate efectua verificări la sediul prestatorului avizat sau în curs de avizare prin personal desemnat prin ordin al ministrului comunicațiilor și societății informaționale.

(2) În cazul în care, în urma verificărilor, se constată nerespectarea prevederilor conținute în documentația de avizare, MCSI poate dispune neacordarea avizului sau, eventual, retragerea acestuia.

Art. 37. - Eliberarea de către MCSI a avizului pentru furnizarea instrumentului de plată electronică cu acces la distanță nu exonerează prestatorul și utilizatorii acestuia de răspunderile asumate prin contractul încheiat între aceștia.

CAPITOLUL VIII

Măsuri tranzitorii

Art. 38. - (1) Avizul eliberat de către MCSI conform Ordinului ministrului comunicațiilor și tehnologiei informației [nr. 389/2007](#) privind procedura de avizare a instrumentelor de plată cu acces la distanță, de tipul aplicațiilor internet-banking, home-banking sau mobile-banking, își prelungește valabilitatea cu 60 de zile de la data publicării prezentului ordin în Monitorul Oficial al României, Partea I.

(2) În perioada extinderii valabilității, prestatorul trebuie să depună documentația de avizare în condițiile prezentului ordin.

(3) Documentațiile întocmite și depuse de către prestatori la MCSI, după data publicării în Monitorul Oficial al României, Partea I, a Regulamentului Băncii Naționale a României [nr. 3/2018](#), pentru avizarea instrumentelor de plată electronică cu acces la distanță, se vor completa în concordanță cu cerințele prezentului ordin.

(4) Raportul de audit deja întocmit sau în curs de realizare la data intrării în vigoare a prezentului ordin poate fi depus împreună cu documentația de avizare, cu respectarea prevederilor art. 9 [alin. \(1\)](#).

Art. 39. - Anexele [nr. 1-7](#) fac parte integrantă din prezentul ordin.

Art. 40. - Prezentul ordin intră în vigoare la data publicării acestuia în Monitorul Oficial al României, Partea I.

Art. 41. - Ordinul ministrului comunicațiilor și tehnologiei informației [nr. 389/2007](#) privind procedura de avizare a instrumentelor de plată cu acces la distanță, de tipul aplicațiilor internet-banking, home-banking sau mobile-banking, publicat în Monitorul Oficial al României, Partea I, nr. 485 din 19 iulie 2007, se abrogă la data publicării prezentului ordin în Monitorul Oficial al României, Partea I.

Ministrul comunicațiilor și societății
informaționale,
Alexandru Petrescu

București, 5 iunie 2019.
Nr. 553.

ANEXA Nr. 1

CERERE de eliberare a avizului

..... (denumirea prestatorului de servicii de plată), având sediul în..... (adresa completă, inclusiv telefon și fax), înmatriculat (ă) /înregistrat (ă) la oficiul registrului comerțului cu nr..... (numărul de înregistrare/codul unic de înregistrare), cod fiscal....., având Autorizația de funcționare nr....., eliberată de Banca Națională a României, reprezentat (ă) legal prin..... (numele și prenumele), domiciliat (ă) în..... (adresa completă, inclusiv telefon), identificat (ă) prin..... (actul de identitate: seria, numărul și emitentul, precum și codul numeric personal), în conformitate cu prevederile Hotărârii Guvernului [36/2017](#) privind organizarea și funcționarea Ministerului Comunicațiilor și Societății Informaționale, cu modificările și completările ulterioare, prevederile art. 129 alin. (1) pct. 2 [lit. c](#) din Regulamentul Băncii Naționale a României nr. 3/2018 privind monitorizarea infrastructurilor pieței financiare și a instrumentelor de plată și cu prevederile Ordinului ministrului comunicațiilor și societății informaționale [nr. 553/2019](#) privind reglementarea procedurii de avizare a instrumentelor de plată electronică cu acces la distanță, vă

solicităm eliberarea/menținerea avizului pentru emiterea și punerea în circulație a instrumentului de plată electronică cu acces la distanță...../menținerea în circulație a instrumentului..... cu următoarele caracteristici generale (scurtă descriere) :

.....
.....
.....
.....
.....

Sistemul funcționează (va funcționa) la sediul din

Numele și prenumele solicitantului

Ștampila solicitantului

.....

Data

ANEXA Nr. 2

LISTA

certificărilor profesionale agreate pentru efectuarea testelor de penetrare

Echipa de testare ce efectuează testele de penetrare trebuie să dețină cel puțin una din certificările menționate mai jos.

Certificări recunoscute internațional:

CEPT - Certified Expert Penetration Tester;

CPT - Certified Penetration Tester;

GPEN - GIAC Certified Penetration Tester;

GWAPT - GIAC Web Application;
LPT - Licensed Penetration Tester;
OPST - OSSTMM Professional Security Tester Accredited Certification;
OSCE - Offensive Security Certified Expert;
OSCP - Offensive Security Certified Professional;
PTC - MILLE2 Certified Penetration Testing Consultant.

ANEXA Nr. 3

RAPORT DE AUDIT

Secțiunea I "Raport"

| Nr. crt. | Capitol | Observații |
|-------------|---|------------|
| 1. | Titlul raportului | |
| 2. | Destinatarii raportului și orice restricții privind conținutul și circulația raportului | |

| | | |
|----|--|--|
| 3. | Paragraf introductiv | <p>Identificarea prestatorului de servicii de plată auditat (denumire/numărul de înregistrare la Oficiul Național al Registrului Comerțului/adresă)</p> <p>Identificarea instrumentului de plată electronică cu acces la distanță auditat (menționarea denumirii instrumentului).</p> <p>Includerea afirmației că sistemele/aplicațiile informatice au fost auditate ca urmare a obligației legale impuse de Ordinul ministrului comunicațiilor și societății informaționale nr. 553/2019 privind reglementarea procedurii de avizare a instrumentelor de plată electronică cu acces la distanță</p> |
| 4. | Asumarea responsabilității conducerii entității privind auditul efectuat asupra sistemelor informatice | |
| 5. | Responsabilitatea auditorului IT | <p>Raportul de audit IT va include cel puțin afirmațiile:</p> <ul style="list-style-type: none"> - că "este responsabilitatea auditorului IT să exprime o opinie cu privire la conformitatea sistemelor informatice cu prevederile Ordinului ministrului comunicațiilor și societății informaționale nr. 553/2019"; - că "raportul de audit IT a fost elaborat în conformitate cu standardul de audit utilizat, respectiv (menționarea acestuia)". |
| 6. | Datele de identificare ale coordonatorului certificat al echipei de audit IT/auditorului IT persoană fizică/auditorului IT intern certificat | Numele, prenumele, telefon, fax, adresa de e-mail și adresa unde își desfășoară activitatea |
| 7. | Semnătura coordonatorului certificat al echipei de audit și semnătura reprezentantului legal al auditorului persoană juridică/semnătura | |

| | | |
|-----|---|---|
| | auditorului IT persoană fizică/semnătura auditorului IT certificat | |
| 8. | Obiectivele activității de audit IT, perioada auditată | |
| 9. | Sediul desfășurării activității de audit IT, data întocmirii raportului de audit IT | Adresa sediului unde a avut loc activitatea de audit IT (sediul central/sucursală/filială), data întocmirii raportului de audit IT |
| 10. | Descrierea ariei auditului IT | <p>Identificarea sistemului informatic utilizat de către prestatorul de servicii de plată folosit în procesul de emiter/exploatare a instrumentului financiar de plată electronică cu acces la distanță (menționarea denumirii instrumentului de plată electronică)</p> <p>Raportarea componentelor sistemului informatic se va face într-un tabel care să cuprindă următoarele:</p> <p>Nr. crt.; Denumire echipament/aplicație; Descriere hardware/software; Serial number; Funcția Îndeplinită;</p> <p>Administrarea sistemului informatic (internă/externalizată)</p> <p>Pentru sistemele informatice supuse auditului IT se vor menționa următoarele:</p> <ul style="list-style-type: none"> - măsurile organizatorice: politicile aplicabile și procedurile implementate; - un sumar conținând analiza riscurilor aferente activității, a posibilelor deficiențe ale sistemului informatic auditat și a măsurilor de reducere a riscurilor asociate, în baza controalelor generale sau specifice implementate conform prevederilor Ordinului ministrului comunicațiilor și societății informaționale nr. 553/2019 |

| | | |
|-----|--|---|
| 11. | Referiri cu privire la implementarea planului de acțiune asumat de prestatorul de servicii de plată rezultat în urma activității de audit IT anterioare, dacă este cazul | Verificarea modului de implementare a măsurilor și respectarea termenelor asumate prin raportul de audit anterior |
| 12. | Referiri cu privire la modul de efectuare a evaluării anuale de către prestatorul de servicii de plată a riscurilor operaționale generate de utilizarea sistemelor informatice importante (Entitățile au obligația să evalueze anual și să monitorizeze continuu riscurile operaționale generate de utilizarea sistemelor informatice importante, să prioritizeze resursele, să implementeze măsuri de securitate informatică și să monitorizeze eficacitatea acestora prin aplicarea managementului de risc.) | Opinie cu privire la plauzibilitatea metodologiei/tehnichilor utilizate, precum și asupra măsurilor de control implementate în vederea gestionării riscurilor operaționale identificate |
| 13. | Rezultatul obținut în urma efectuării testului de penetrare | Conform raportului privind testul de penetrare se consemnează următoarele elemente: - nr. de înregistrare/data raportului privind testele de penetrare; - perioada în care s-au desfășurat testele de penetrare; - descrierea metodologiei/tehnichilor utilizate; - menționarea rezultatelor obținute în urma testului; - concluziile raportului; - recomandările adresate entității și răspunsul managementului entității. |
| 14. | Afirmarea de conformitate, reflectată prin opinia auditorului IT | Opinie pozitivă, opinie cu rezerve/calificată, opinie negativă, după caz |

Secțiunea II
"Anexe la raportul de audit IT"

1. Sumarul observațiilor - anexa nr. R1

Anexa este însoțită de către entitatea auditată prin semnarea acesteia de către reprezentantul legal și conține, fără a se limita la acestea:

- a) descrierea neconformității/constatării;
- b) importanța neconformității/constatării;
- c) riscurile asociate;
- d) probabilitatea ca aceste constatări să aibă un impact semnificativ; recomandările auditorului IT pentru acțiuni corective și răspunsul conducerii entității auditate pentru fiecare constatare din raport (inclusiv în urma testului de penetrare);
- e) planul de acțiune asumat de către entitatea auditată care conține măsurile efective, termenul de implementare și persoanele responsabile de implementare.

2. Analiza internă a riscurilor operaționale și registrul riscurilor - anexa nr. R2

Anexa conține următoarele informații, fără a se limita la acestea:

- a) descrierea politicii/metodologiei utilizate de către entitate;
- b) rezultatele revizuirii riscurilor generate de utilizarea sistemelor informatice;
- c) rezultatele evaluării de către auditorul IT a măsurilor de control implementate în vederea gestionării riscurilor operaționale identificate (pentru riscuri semnificative).

3. Cerințe referitoare la furnizorii de servicii IT externalizate pentru sistemele informatice auditate - anexa nr. R3

(Raportarea se efectuează prin completarea tabelului prezentat.)

| Sisteme/Servicii externalizate | Funcția sistemelor/serviciilor externalizate - descriere | Furnizor - date de identificare (denumire, sediul entității, datele de înregistrare fiscală, telefon/fax/website) | Certificare SR ISO/IEC 27001 sau echivalent (emitent, număr | Alte certificări | Concluzie - Conformitate Da/Nu/Parțial | Observații |
|--------------------------------|--|---|---|------------------|--|------------|
|--------------------------------|--|---|---|------------------|--|------------|

| | | | | | | |
|--|--|--|--|--|--|--|
| | | | certificare, data emiterii, perioada de valabilitate) | | | |
| | | | | | | |

4. Concluzii ale echipei de audit privind respectarea cerințelor impuse de Ordinul ministrului comunicațiilor și societății informaționale [nr. 553/2019](#)
- anexa nr. R4

NOTĂ:

Anexele prevăzute la secțiunea II "Anexe la raportul de audit" R1-R4 fac parte integrantă din raport.

ANEXA Nr. 4

CERERE de înscriere în Lista auditorilor IT

..... (denumirea auditorului IT), având sediul în..... (adresa completă, inclusiv telefon și fax, adresa de e-mail, adresa paginii de internet), înmatriculat (ă) /înregistrat (ă) la oficiul registrului comerțului cu nr..... (numărul de înregistrare/codul unic de înregistrare) cod fiscal....., reprezentat (ă) legal prin dl/dna....., identificat (ă) prin..... (actul de identitate: seria, numărul și emitentul), intenționez să prestez servicii de audit IT pentru prestatorii de servicii de plată care emit instrumente financiare de plată electronică cu acces la distanță cărora le sunt incidente prevederile Ordinului ministrului comunicațiilor și societății informaționale [nr. 553/2019](#) privind reglementarea procedurii de avizare a instrumentelor de plată electronică cu acces la distanță și vă solicit înscrierea în Lista auditorilor IT publicată pe site-ul instituției dumneavoastră.

Anexez prezentei cereri documentația de calificare prevăzută la [art. 15](#) din Ordinul ministrului comunicațiilor și societății informaționale nr. 553/2019.

Numele și prenumele reprezentantului legal Ștampila solicitantului

.....

Data

ANEXA Nr. 5

LISTA certificărilor profesionale agreeate pentru auditorii IT

Raportul de audit se întocmește de către un auditor IT care trebuie să dețină cel puțin una din certificările menționate mai jos.

Certificări recunoscute internațional:

ISACA - CISA - Certified Information Systems Auditor (auditorul pentru sisteme informatice, certificat de ISACA);

GIAC(SANS) - GSNA Systems and Network Auditors;

GIAC - GCCC Critical Controls Certification;

CISSP - Certified Information Systems Security Professional.

ANEXA Nr. 6

Prestatorul de servicii de plată:

| Instrumentul de plată electronică cu acces la distanță | Numărul de utilizatori1 | Numărul de plăți/tranzacții2 - lei - | Numărul de tranzacții - valută - | Valoarea plăților/tranzacțiilor3 - lei - | Valoarea tranzacțiilor în valută (echivalent euro) | Perioada de raportare Trimestrul |
|--|-------------------------|---|-------------------------------------|---|--|-------------------------------------|
|--|-------------------------|---|-------------------------------------|---|--|-------------------------------------|

| | | | | | | |
|--|--|--|--|--|--|--|
| | | | | | | |
|--|--|--|--|--|--|--|

¹ Numărul de utilizatori se referă la numărul de utilizatori cu care există încheiat un contract pentru utilizarea instrumentului de plată cu acces la distanță, pe parcursul trimestrului pentru care se face raportarea. Se iau în considerare toate contractele în vigoare de la data lansării instrumentului de plată electronică cu acces la distanță.

² Numărul de plăți efectuate prin intermediul instrumentelor de plată cu acces la distanță se referă la plățile efectuate doar pe perioada trimestrului raportat și care vor fi prezentate, defalcat, în numărul de plăți în lei și în numărul de plăți în valută.

³ Valoarea plăților efectuate prin intermediul instrumentelor de plată cu acces la distanță în perioada trimestrului raportat va fi prezentată astfel: valoarea plăților efectuate în lei și valoarea plăților efectuate în valută. Plățile efectuate în valută vor fi exprimate în echivalent euro, la cursul de schimb BNR din ultima zi a trimestrului pentru care se face raportarea.

Semnătură reprezentant legal

.....

ANEXA Nr. 7

MINISTERUL COMUNICAȚIILOR ȘI SOCIETĂȚII INFORMAȚIONALE

Având în vedere prevederile Hotărârii Guvernului [nr. 36/2017](#) privind organizarea și funcționarea Ministerului Comunicațiilor și Societății Informaționale, cu modificările și completările ulterioare,

având în vedere prevederile art. 129 alin. (1) pct. 2 [lit. c\)](#) din Regulamentul Băncii Naționale a României nr. 3/2018 privind monitorizarea infrastructurilor pieței financiare și a instrumentelor de plată și ale Ordinului ministrului comunicațiilor și societății informaționale [nr. 553/2019](#) privind reglementarea procedurii de avizare a instrumentelor de plată electronică cu acces la distanță,

ministrul comunicațiilor și societății informaționale eliberează prezentul aviz.

....., având sediul în..... (adresa completă, inclusiv telefon și fax), înmatriculat (ă) /înregistrat (ă) la oficiul registrului comerțului cu nr....., cod fiscal....., având Autorizația de funcționare, nr....., eliberată de Banca Națională a României, reprezentat (ă) legal prin..... (numele și prenumele), a obținut avizul pentru furnizarea instrumentului de plată cu acces la distanță..... cu următoarele caracteristici generale:

.....
.....
.....
.....
.....

Sistemul funcționează (va funcționa) la sediul din

Observații:

Prezentul document s-a eliberat prestatorului de servicii de plată în scopul acordării/menținerii avizului Ministerului Comunicațiilor și Societății Informaționale necesar pentru emiterea/punerea în circulație a instrumentului de plată electronică cu acces la distanță și are valabilitate un an de la data eliberării acestuia.

Ministrul comunicațiilor și societății
informaționale,

.....

Nr.....

Data

Banca Națională a României - BNR

Regulamentul nr. 3/2018 privind monitorizarea infrastructurilor pieței financiare și a instrumentelor de plată

În vigoare de la 16 august 2018

Consolidarea din data de **05 noiembrie 2019** are la bază [publicarea din Monitorul Oficial, Partea I](#) nr. 713 din 16 august 2018

Include modificările aduse prin următoarele acte: Rectificare [2018](#).

Ultimul amendament în 17 septembrie 2018.

Având în vedere prevederile art. 2 alin. (2) [lit. b](#)) și ale art. 22 [alin. \(1\)](#) și [\(2\)](#) din Legea nr. 312/2004 privind Statutul Băncii Naționale a României, ale art. 404, 407 și art. 408 alin. (1) din Ordonanța de urgență a Guvernului [nr. 99/2006](#) privind instituțiile de credit și adecvarea capitalului, aprobată cu modificări și completări prin Legea [nr. 227/2007](#), cu modificările și completările ulterioare, ale art. 13 [alin. \(4\)](#) din Legea nr. 253/2004 privind caracterul definitiv al decontării în sistemele de plăți și în sistemele de decontare a operațiunilor cu instrumente financiare, cu modificările și completările ulterioare, ale art. 187 [alin. \(2\)](#) din Legea nr. 126/2018 privind piețele de instrumente financiare, ale [art. 62](#) din Ordonanța de urgență a Guvernului nr. 113/2009 privind serviciile de plată, aprobată cu modificări prin Legea [nr. 197/2010](#), cu modificările și completările ulterioare, ale [art. 61](#) din Legea nr. 127/2011 privind activitatea de emisie de monedă electronică, cu modificările ulterioare, în temeiul art. 48 [alin. \(2\)](#) din Legea nr. 312/2004, [art. 405](#) din Ordonanța de urgență a Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, aprobată cu modificări și completări prin Legea [nr. 227/2007](#), cu modificările și completările ulterioare, art. 186 [alin. \(1\)](#) din Ordonanța de urgență a Guvernului nr. 113/2009 privind serviciile de plată, aprobată cu modificări prin Legea [nr. 197/2010](#), cu modificările și completările ulterioare,
Banca Națională a României emite prezentul regulament.

TITLUL I

Obiect, domeniu de aplicare și definiții

Art. 1. - (1) Prezentul regulament stabilește cerințele pentru:

- a) autorizarea și monitorizarea infrastructurilor pieței financiare, denumite în continuare IPF;
- b) monitorizarea participanților la aceste infrastructuri;
- c) punerea în circulație, emiterea și monitorizarea instrumentelor de plată.

(2) Prezentul regulament se aplică:

- a) infrastructurilor pieței financiare, inclusiv administratorilor acestora, care funcționează pe teritoriul României;
- b) participanților la infrastructurile pieței financiare menționate la lit. a);

c) prestatorilor de servicii de plată care pun în circulație și/sau acceptă instrumente de plată pe teritoriul României.

(3) IPF operate pe teritoriul României de către Eurosistem, Banca Centrală Europeană și Banca Națională a României nu li se aplică prevederile următoarelor articolele: [art. 6-8](#) Cerințele generale privind guvernanta, art. 16 [alin. \(3\)](#) - [\(5\)](#) Cerințe privind cadrul pentru gestionarea cuprinzătoare a riscurilor, [art. 17-22](#) Cerințe pentru gestionarea riscului de credit, [art. 23-29](#) Cerințe privind aranjamentele de garantare, [art. 72-77](#) Cerințe privind riscul general de afaceri, [art. 78-81](#) Cerințe privind riscul de custodie și de investiție și [art. 89-91](#) Cerințe privind criteriile de acces și participare.

Art. 2. - În înțelesul prezentului regulament, termenii și expresiile de mai jos au următoarele semnificații:

1. acceptant - un prestator de servicii de plată care încheie un contract cu beneficiarul plății privind acceptarea și prelucrarea tranzacțiilor de plată cu instrumente de plată electronică, efectuate în scopul executării unui transfer de fonduri către beneficiarul plății;
2. administrator al unei infrastructuri a pieței financiare - persoana juridică care stabilește regulile de funcționare a unei infrastructuri a pieței financiare și este responsabil legal de operarea infrastructurii;
3. agent de decontare sau bancă de decontare - are semnificația prevăzută la art. 2 alin. (1) [pct. 4](#) din Legea nr. 253/2004 privind caracterul definitiv al decontării în sistemele de plăți și în sistemele de decontare a operațiunilor cu instrumente financiare, cu modificările și completările ulterioare;
4. agent nostro - instituție de credit utilizată de participanții la o infrastructură a pieței financiare pentru decontare;
5. autentificare - o procedură care permite prestatorului de servicii de plată să verifice identitatea unui utilizator al serviciilor de plată sau valabilitatea utilizării unui anumit instrument de plată, inclusiv utilizarea elementelor de securitate personalizate ale utilizatorului;
6. bancă custode - instituție de credit ce păstrează și protejează activele financiare ale terților;
7. beneficiar al plății - persoana fizică sau juridică care este destinatarul vizat al fondurilor care au făcut obiectul unei operațiuni de plată;
8. card - dispozitiv fizic sau instrument virtual care poate fi utilizat de către deținătorul său pentru a efectua operațiuni de plată. În această categorie sunt incluse, dar fără a se limita la, cardurile de debit, de credit, de debit amânat, preplătit, virtual;
9. card de debit - cardul prin intermediul căruia utilizatorul dispune de fondurile din contul său de plăți pentru a efectua operațiuni de plată;
10. card de debit amânat - cardul prin intermediul căruia utilizatorul dispune de fondurile oferite de instituția emitentă sub forma unei linii de credit pentru a efectua operațiuni de plată. Întreaga sumă datorată instituției emitente trebuie rambursată integral până la sfârșitul perioadei specificate în contract;
11. card de credit - cardul prin intermediul căruia utilizatorul dispune de fondurile oferite de instituția emitentă sub forma unei linii de credit pentru a efectua operațiuni de plată. Suma datorată poate fi rambursată total sau parțial, existând obligația de rambursare a sumei minime stabilite în contract până la data stabilită în acesta;

12. card preplătit - cardul reîncărcabil sau nereîncărcabil, personalizat sau nepersonalizat, prin intermediul căruia utilizatorul dispune de fondurile depuse în scopul efectuării unor operațiuni de plată specifice;
13. card virtual - cardul fără suport fizic, utilizat pentru efectuarea plăților în mediul on-line;
14. clearing - procesul de transmitere, reconciliere și, după caz, confirmare a ordinelor de transfer înainte de decontare, cu posibilitatea de includere a compensării pe bază netă a ordinelor de transfer și de stabilire a pozițiilor finale pentru decontare;
15. compensare - conform prevederilor art. 2 alin. (1) [pct. 11](#) din Legea nr. 253/2004 privind caracterul definitiv al decontării în sistemele de plăți și în sistemele de decontare a operațiunilor cu instrumente financiare, cu modificările și completările ulterioare;
16. condiții de piață extreme, dar plauzibile - set cuprinzător de condiții istorice și ipotetice, incluzând cele mai volatile perioade care au fost suportate de piețele deservite de infrastructura pieței financiare;
17. conducere - directori executivi, respectiv membri ai consiliului de administrație, în cazul sistemului de conducere unitar, care sunt implicați în gestionarea zilnică a activității administratorului infrastructurii pieței financiare sau membrii directoratului administratorului infrastructurii pieței financiare într-un sistem dualist;
18. conexiune - un set de contracte și acorduri operaționale între două sau mai multe infrastructuri ale pieței financiare care conectează aceste infrastructuri direct sau printr-un intermediar;
19. conexiune directă - conexiune stabilită între două infrastructuri ale pieței financiare, fără a exista intermedierea realizată de un terț;
20. conexiune indirectă - conexiune stabilită între două infrastructuri ale pieței financiare prin intermediul unui terț care nu este o infrastructură a pieței financiare;
21. conexiune releu - conexiune care implică minimum trei infrastructuri ale pieței financiare, în care o infrastructură a pieței financiare realizează intermedierea între alte două infrastructuri ale pieței financiare. Conexiunea releu poate fi percepută ca un lanț de două conexiuni directe;
22. continuitatea activității - starea de funcționare neîntreruptă a operațiunilor, ce presupune măsuri organizaționale, tehnice și de personal utilizate pentru a asigura continuitatea serviciilor critice după o întrerupere cauzată de producerea unui eveniment perturbator și pentru reluarea treptată a tuturor serviciilor în cazul unui eveniment perturbator major, prelungit sau cu efecte pe scară largă;
23. consiliu - consiliul de administrație și/sau consiliul de supraveghere al administratorului infrastructurii pieței financiare;
24. contraparte centrală (CPC) - conform prevederilor art. 2 [pct.1 din](#) Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții;
25. dată prevăzută pentru decontare - ziua în care fondurile și/sau instrumentele financiare sunt datorate și trebuie să fie puse la dispoziția beneficiarului acestora, în conformitate cu regulile infrastructurii pieței financiare respective;
26. decontare finală - transferul necondiționat și irevocabil al fondurilor și/sau instrumentelor financiare sau stingerea unei obligații de către o infrastructură a pieței financiare sau de către participanții la aceasta, în concordanță cu prevederile contractuale;

27. decontare în banii băncii centrale - serviciul furnizat de o bancă centrală, în calitate de agent de decontare pentru o infrastructură a pieței financiare, pentru stingerea obligațiilor de plată prin efectuarea de înregistrări în conturile de decontare deschise și administrate de banca centrală, ale participanților la acea IPF sau ale agenților nostro;
28. decontare în banii băncii comerciale - serviciul furnizat de o bancă comercială, în calitate de agent de decontare pentru o infrastructură a pieței financiare, pentru stingerea obligațiilor de plată prin efectuarea de înregistrări în conturile de decontare deschise și administrate de banca comercială, ale participanților la acea IPF sau ale agenților nostro;
29. depozitar central de instrumente financiare (DC) - are semnificația prevăzută la art. 2 alin. (1) [pct.1](#) din Regulamentul (UE) nr. 909/2014;
30. emitent - prestator de servicii de plată care emite și pune la dispoziția deținătorului un instrument de plată electronică, în baza unui contract încheiat cu deținătorul;
31. expuneri curente - pierderea financiară pe care administratorul unei infrastructuri a pieței financiare sau participanții la aceasta ar suporta-o imediat dacă unul dintre participanți nu ar putea să își îndeplinească obligațiile rezultate din participarea la respectiva infrastructură a pieței financiare. Valoarea expunerii este stabilită ca maxim dintre zero și valoarea de piață sau costul de înlocuire a unei tranzacții sau a unui portofoliu de tranzacții cu o contrapartidă, care s-ar pierde implicit ca urmare a imposibilității contrapartidei de a-și îndeplini obligațiile asumate;
32. expunere la riscul de credit - o sumă sau valoare expusă riscului ca un participant să nu o deconteze în întregime, atunci când este scadentă sau la orice moment ulterior;
33. externalizarea - utilizarea de către o entitate a unui furnizor extern, în vederea desfășurării de către acesta, pe bază contractuală și în mod continuu, a unor activități efectuate în mod obișnuit de către entitatea în cauză;
34. furnizor de lichiditate - o entitate cu care o infrastructură a pieței financiare a încheiat un acord de furnizare a fondurilor;
35. furnizor de serviciu critic - furnizor al unui serviciu care este indispensabil pentru funcționarea unei infrastructuri a pieței financiare, a unui participant, a unui prestator de servicii de plată. În categoria furnizorilor de servicii critice sunt incluse și entitățile către care au fost externalizate activități, servicii sau funcții critice;
36. garanție - orice activ care se poate valorifica, inclusiv o sumă de bani, instrumente financiare și creanțe private, și care face obiectul oricărei forme de garantare, al unui contract de report ori al unui contract similar și care este constituit în scopul garantării drepturilor și obligațiilor care pot rezulta în legătură cu participarea la un sistem sau care este pus la dispoziția Băncii Naționale a României ori a băncilor centrale din statele membre ale Spațiului Economic European sau a Băncii Centrale Europene;
37. guvernanză - set de relații între proprietarii infrastructurii pieței financiare, consiliu, conducere și alte părți relevante ce includ participanți, autorități, clienți ai participanților, infrastructuri ale pieței financiare interdependente și piața deservită;
38. infrastructură a pieței financiare (IPF) - sistem multilateral organizat între instituțiile participante, inclusiv administratorul infrastructurii pieței financiare, utilizat pentru clearing, decontare sau înregistrare a plăților sau a tranzacțiilor cu instrumente financiare, inclusiv a instrumentelor financiare

derivate, sau a altor tranzacții financiare. În sensul prezentului regulament, în categoria infrastructurilor pieței financiare sunt incluse sistemele de plăți și sistemele de decontare a operațiunilor cu instrumente financiare din cadrul depozitarilor centrali și contrapărților centrale;

39. instrucțiune critică - ordin de transfer care trebuie efectuat cu prioritate, în cazul apariției unei perturbări, pentru evitarea manifestării și propagării riscurilor în cadrul unei infrastructuri a pieței financiare sau a riscului sistemic;

40. instrument de plată - un dispozitiv sau un set de proceduri care permite transferul de fonduri de la plătitor la beneficiar. Acestea includ instrumentele de plată electronică și cele pe suport hârtie;

41. instrument de plată electronică - un card sau un instrument de plată electronică cu acces la distanță;

42. instrument de plată electronică cu acces la distanță - set de proceduri, care se bazează pe o soluție informatică, de tipul: internet-banking, home-banking, phone-banking, mobile-banking, care permite utilizatorului inițierea de operațiuni de plată, în baza fondurilor de care dispune;

43. marjă - garanție constituită în favoarea contrapartidei pentru a proteja împotriva expunerilor curente sau potențiale viitoare cauzate de evoluția prețului de piață sau a eventualei incapacități de îndeplinire a obligațiilor;

44. membru independent al consiliului - un membru neexecutiv al consiliului care nu are nicio relație de afaceri, familială sau de altă natură care creează un conflict de interese în legătură cu IPF sau administratorul IPF, acționarii majoritari ai acestora, conducerea acestora sau participanții la acestea și care nu a avut astfel de relații în cei 2 ani care precedă numirea sa în consiliu;

45. modificare majoră - schimbarea semnificativă a arhitecturii infrastructurii pieței financiare, introducerea unor noi funcționalități ori activități sau schimbări cu un impact semnificativ asupra profilului de risc al infrastructurii pieței financiare;

46. modificare minoră - modificare care nu afectează semnificativ profilul de risc al infrastructurii pieței financiare sau arhitectura acesteia;

47. monedă electronică - are semnificația prevăzută la art. 4 [lit. f](#)) din Legea nr. 127/2011, cu modificările și completările ulterioare;

48. monitorizare - funcție a băncii centrale prin care se urmărește promovarea funcționării sigure și eficiente a infrastructurilor pieței financiare, precum și evitarea riscului sistemic, constând în: (i) obținerea de informații cu privire la arhitectura și funcționarea infrastructurilor pieței financiare prezente sau planificate, emiterea, acceptarea și utilizarea instrumentelor de plată și a monedei electronice, (ii) evaluarea informațiilor obținute și (iii) inducerea de schimbări ori dispunerea unor măsuri de remediere și sancțiuni;

49. operațiune de plată - acțiune inițiată de plătitor sau de o altă persoană în numele și pe seama plătitorului ori de beneficiarul plății cu scopul de a depune, de a transfera sau de a retrage fonduri, indiferent de orice obligații subsecvente între plătitor și beneficiarul plății;

50. ordin de plată - o dispoziție a unui plătitor sau a unui beneficiar al plății către prestatorul său de servicii de plată prin care se solicită executarea unei operațiuni de plată;

51. ordin de transfer - așa cum este definit prin prevederile art. 2 alin. (1) [pct. 9](#) din Legea nr. 253/2004 privind caracterul definitiv al decontării în sistemele de plăți și în sistemele de decontare a operațiunilor cu instrumente financiare, cu modificările și completările ulterioare;
52. participant - entitate care este identificată sau recunoscută de un administrator al unei infrastructuri a pieței financiare și căreia i se permite, direct sau indirect, să trimită ordine de transfer către respectiva infrastructură a pieței financiare și care este capabilă să primească ordine de transfer de la aceasta;
53. participant critic - un participant la o infrastructură a pieței financiare care, datorită volumelor sau valorilor tranzacțiilor sau serviciilor prestate către acea infrastructură a pieței financiare, în cazul unei probleme operaționale majore cu care s-ar confrunta acest participant, poate afecta semnificativ ceilalți participanți sau infrastructura pieței financiare;
54. participant direct - o entitate juridică care are o relație contractuală cu un administrator al unei IPF, are permisiunea să trimită ordine de transfer către acea IPF și este capabilă să primească ordine de transfer de la aceasta;
55. participant indirect - o entitate juridică care nu are acces direct la serviciile unei IPF și ale cărei ordine de transfer sunt compensate, decontate și înregistrate de IPF printr-un participant direct, în baza unei relații contractuale pe care un participant indirect o are cu un participant direct;
56. părți interesate relevante - participanți, alte infrastructuri ale pieței financiare care au impact asupra riscurilor specifice unei infrastructuri a pieței financiare și, de la caz la caz, alți actori afectați de pe piață;
57. plan de lichidare ordonată - plan elaborat de administratorul infrastructurii pieței financiare pentru închiderea ordonată a infrastructurii;
58. plan de redresare - plan elaborat de administratorul infrastructurii pieței financiare pentru restabilirea bunei funcționări a infrastructurii pieței financiare;
59. plătitor - persoana fizică sau juridică care este titularul unui cont de plăți și care autorizează un ordin de plată din acel cont de plăți sau, în cazul în care nu există un cont de plăți, persoana fizică sau juridică care emite un ordin de plată;
60. portabilitate - aspectele operaționale aferente transferurilor pozițiilor contractuale, de fonduri sau de instrumente financiare de la o infrastructură a pieței financiare sau de la un participant la o altă infrastructură a pieței financiare sau participant;
61. prestator de servicii de plată - entitate autorizată să presteze servicii de plată pe teritoriul României, respectiv instituții de credit, instituții de plată și instituții emitente de monedă electronică;
62. punerea în circulație - punerea la dispoziția clienților a unui instrument de plată, în baza unui contract încheiat cu aceștia;
63. reziliența cibernetică - capacitatea unei IPF de a: anticipa amenințările ciberneticе, rezista la atacurile ciberneticе, limita amploarea consecințelor și relua activitatea după atacuri ciberneticе;
64. risc de credit - riscul ca o contraparte, indiferent dacă este participant sau altă entitate, să nu își poată îndeplini în întregime obligațiile financiare atunci când acestea devin scadente sau oricând în viitor;

65. risc de custodie - riscul de a suporta o pierdere a activelor deținute în custodie din cauza insolvenței, neglijenței, fraudei, administrării defectuoase sau evidenței necorespunzătoare ale custodelui;

66. risc de decontare - riscul ca decontarea fondurilor sau a instrumentelor financiare în cadrul unei infrastructuri a pieței financiare să nu aibă loc integral la data preconizată pentru decontare;

67. risc general de afaceri - orice depreciere potențială a situației financiare a administratorului unei infrastructuri a pieței financiare, ca urmare a unui declin al încasărilor sau a unei creșteri a cheltuielilor acestuia, astfel încât cheltuielile depășesc încasările și conduc la o pierdere care trebuie acoperită din capitalul propriu;

68. risc de investiție - riscul de pierdere cu care se confruntă un administrator al unei infrastructuri a pieței financiare sau un participant atunci când administratorul infrastructurii investește resursele proprii sau ale participanților;

69. risc juridic - riscul care rezultă din neaplicarea sau aplicarea defectuoasă a cadrului legal sau de reglementare sau a prevederilor contractuale, de obicei determinând o pierdere;

70. risc de lichiditate - riscul ca o contraparte, participant sau altă entitate să nu dispună de suficiente fonduri care să îi permită să își îndeplinească integral obligațiile asumate la scadență, deși, în viitor, ar putea avea fonduri suficiente în acest sens;

71. risc operațional - riscul ca deficiențele sistemelor de informații sau ale proceselor interne, erorile umane, deficiențele în administrare sau perturbările provocate de evenimente externe sau de servicii externalizate să conducă la reducerea, deteriorarea sau întreruperea serviciilor furnizate de administratorul unei infrastructuri a pieței financiare sau de emitenții/acceptanții instrumentelor de plată;

72. risc de piață - riscul înregistrării de pierderi, în poziții bilanțiere și extrabilanțiere, care rezultă din variația prețurilor de pe piață;

73. risc principal - riscul ca o contraparte să piardă întreaga valoare implicată într-o tranzacție, respectiv riscul ca un vânzător al unui activ financiar să livreze activul în mod irevocabil, dar să nu primească contravaloarea acestuia, sau riscul ca un cumpărător al unui activ financiar să plătească pentru un activ în mod irevocabil și să nu îl primească;

74. risc sistemic - riscul ca neîndeplinirea obligațiilor ce revin unui participant sau administratorului infrastructurii pieței financiare din participarea la o infrastructură să determine alți participanți și/sau administratorul infrastructurii să nu își poată îndeplini obligațiile atunci când acestea devin scadente, generând eventuale efecte de contagiune care ar amenința stabilitatea sau încrederea în sistemul financiar;

75. semnificativ - califică un risc, o dependență și/sau o modificare ce poate afecta capacitatea unei entități de a funcționa sau de a furniza servicii conform așteptărilor;

76. serviciu critic - un serviciu esențial pentru funcționarea unei infrastructuri a pieței financiare sau a unui prestator de servicii de plată, a cărui indisponibilitate sau absență poate determina apariția unei perturbări majore în funcționarea normală și care nu poate fi reprodus sau a cărui reproducere ar presupune costuri care nu sunt rezonabile;

77. siguranță în funcționare - modalitate de gestionare a riscurilor specifice infrastructurii pieței financiare, respectiv a instrumentului de plată, în scopul asigurării funcționării conform nivelurilor de calitate a serviciilor și/sau a orarului de funcționare asumat, fără a afecta în mod negativ încrederea participanților și a publicului;

78. sistem de decontare a operațiunilor cu instrumente financiare (SD) - un aranjament formal între trei sau mai mulți participanți, fără a include posibile bănci de decontare, contrapărți centrale, case de compensare sau participanți indirecti, cu reguli comune și aranjamente standardizate, a cărei activitate constă în executarea ordinelor de transfer de instrumente financiare;

79. sistem de plăți (SP) - un aranjament formal între trei sau mai mulți participanți, fără a include posibile bănci de decontare, contrapărți centrale, case de compensare sau participanți indirecti, cu reguli comune și aranjamente standardizate pentru executarea ordinelor de transfer de fonduri între participanți;

80. sistem de plăți de mare valoare - sistem de plăți care procesează ordine de transfer de mare valoare și/sau urgențe;

81. sistem de plăți de mică valoare - sistem de plăți care procesează ordine de transfer de mică valoare inițiate cu instrumente de plată de tipul transferurilor de credit, cecurilor, cambiiilor, biletelor la ordin, cardurilor etc.;

82. situație de urgență - un eveniment, o situație sau o împrejurare care are capacitatea de a determina nefuncționarea sau perturbarea operațiunilor, serviciilor sau funcțiilor unei IPF, inclusiv perturbarea sau împiedicarea decontării finale;

83. societate afiliată - o societate care îl controlează pe participant sau care este controlată de acesta sau care se află sub același control ca participantul. Controlul unei societăți este definit drept: a) deținerea în proprietate, controlul sau deținerea a cel puțin 20 % sau mai mult dintr-o clasă de acțiuni care dau drept de vot în cadrul societății; sau b) consolidarea societății în scopul raportării financiare;

84. teste de stres - cuantificarea expunerilor la riscul de credit și de lichiditate care ar rezulta din evoluția și volatilitatea prețurilor în scenarii extreme, dar plauzibile.

TITLUL II

Dispoziții generale

CAPITOLUL I

Cerințe generale aplicabile administratorilor infrastructurilor pieței financiare

SECȚIUNEA 1

Cerințele privind siguranța juridică

Art. 3. - (1) În vederea asigurării unui climat de siguranță din punct de vedere juridic, administratorul IPF evaluează măsura în care legislația aplicabilă în toate sistemele juridice relevante asigură un grad ridicat

de certitudine și sprijină fiecare aspect semnificativ al activităților IPF operat de acesta. În acest sens, administratorul IPF stabilește normele și procedurile IPF și încheie contracte care sunt clare și în conformitate cu legislația aplicabilă în toate sistemele juridice relevante.

(2) În aplicarea prevederilor alin. (1) administratorul IPF dispune următoarele măsuri:

a) comunică Băncii Naționale a României, participanților și, dacă este cazul, clienților participanților, într-un mod clar și ușor de înțeles, legislația, normele, procedurile și contractele aplicabile pentru funcționarea IPF;

b) ia măsurile necesare pentru a se asigura că normele, procedurile și contractele sale produc efecte juridice în toate sistemele juridice relevante și depune toate diligențele pentru ca acțiunile pe care le ia în baza acestor norme, proceduri și contracte să nu fie anulate, reversibile sau suspendate;

c) identifică și diminuează riscurile care decurg din orice potențial conflict de legi, în măsura în care își desfășoară activitatea în mai multe sisteme juridice.

SECȚIUNEA a 2-a

Cerințele generale privind guvernarea

Art. 4. - (1) În vederea asigurării unui cadru de administrare responsabil, administratorul IPF stabilește obiective documentate care acordă prioritate ridicată siguranței și eficienței IPF.

(2) Obiectivele stabilite potrivit alin. (1) susțin în mod explicit stabilitatea financiară și alte considerente relevante de interes public, în special piețele financiare eficiente și deschise.

Art. 5. - (1) Administratorul IPF deține mecanisme de guvernare documentate și efective, care stabilesc ierarhii clare și directe de responsabilitate și răspundere.

(2) La solicitarea Băncii Naționale a României, a deținătorilor sau a participanților, administratorul IPF pune la dispoziția acestora orice informații cu privire la mecanismele prevăzute la alin. (1).

(3) Administratorul IPF trebuie să facă disponibile public versiuni prescurtate ale informațiilor prevăzute la [alin. \(1\)](#).

Art. 6. - (1) Administratorul IPF stabilește și definește în mod clar rolul și responsabilitățile și raporturile ierarhice ale consiliului, incluzând în mod cumulativ următoarele elemente:

a) stabilirea unor obiective strategice clare pentru IPF;

b) stabilirea unor proceduri documentate pentru funcționarea IPF, inclusiv proceduri pentru identificarea, abordarea și gestionarea conflictelor de interese ale membrilor acestuia;

c) asigurarea eficacității selectării, monitorizării și, dacă este cazul, a îndepărtării din funcție a membrilor conducerii;

d) stabilirea unor politici de compensare corespunzătoare, în conformitate cu cele mai bune practici și bazate pe realizările pe termen lung;

e) aprobarea emiterii deciziilor care au un impact semnificativ asupra profilului de risc al IPF, precum și asupra documentelor- cheie privind riscul care reglementează operațiunile IPF;

f) aprobarea și reexaminarea anuală a cadrului cuprinzător de gestionare a riscurilor, cadrului privind riscul operațional și planul aferent de continuitate a activității, planul de redresare și lichidare ordonată și planul privind capitalul, cadrele privind riscul de credit și riscul de lichiditate, cadrul privind

aranjamentele de garantare care reglementează gestionarea riscurilor, strategia de investiții a IPF, precum și cadrul de reziliență cibernetică.

Art. 7. - Consiliul își analizează cel puțin anual atât performanța de ansamblu, cât și performanța individuală a membrilor săi.

Art. 8. - Componenta consiliului asigură integritatea și o gamă adecvată de competențe tehnice, cunoștințe și experiență, atât în privința IPF, cât și a pieței financiare în general, permițând consiliului să își îndeplinească rolurile și responsabilitățile. Consiliul include membri neexecutivi și cel puțin un membru independent.

Art. 9. - (1) Administratorul IPF stabilește și definește în mod clar rolul, responsabilitățile și raporturile ierarhice ale conducerii.

(2) Componenta conducerii asigură integritatea și o gamă adecvată de competențe tehnice, cunoștințe și experiență, atât în privința IPF, cât și asupra pieței financiare în general, permițând conducerii să își îndeplinească responsabilitățile privind funcționarea și gestionarea riscurilor administratorului IPF.

(3) Sub coordonarea consiliului, responsabilitățile conducerii implică asigurarea următoarelor:

- a) consecvența activităților administratorului IPF cu obiectivele, strategia și toleranța la risc a acestuia;
- b) proiectarea, executarea și monitorizarea corespunzătoare a controalelor interne și a procedurilor aferente, pentru promovarea obiectivelor administratorului IPF;
- c) evaluarea și testarea periodică a controalelor interne și a procedurilor aferente de către echipe de gestionare a riscului și audit intern bine pregătite și cu personal suficient;
- d) implicare activă în procesul de control al riscurilor;
- e) alocarea de resurse suficiente cadrului de gestionare a riscurilor IPF.

Art. 10. - (1) Consiliul stabilește și monitorizează un cadru documentat de gestionare a riscurilor, care:

- a) include politica de toleranță la risc a administratorului IPF;
- b) atribuie responsabilități și răspunderi pentru deciziile privind riscul;
- c) tratează procesul decizional în cursul situațiilor de criză și de urgență;
- d) tratează funcțiile de control intern.

(2) Consiliul se asigură că există trei linii de apărare clare și eficiente (operațiuni, gestionarea riscurilor și audit intern), care sunt separate una de cealaltă și care beneficiază de suficientă autoritate, independență, resurse și acces la consiliu.

Art. 11. - (1) Consiliul se asigură că deciziile majore care afectează structura tehnică și funcțională a IPF, regulile și strategia de ansamblu, în special în ceea ce privește alegerea unui mecanism de compensare și decontare, structura de operare, gama de produse compensate sau decontate și utilizarea tehnologiei și procedurilor, protejează în mod corespunzător interesele legitime ale părților interesate relevante ale IPF.

(2) Administratorul IPF consultă părțile interesate relevante și, după caz, orice persoană interesată, într-un interval de timp rezonabil înainte de luarea deciziilor prevăzute la alin. (1).

SECȚIUNEA a 3-a

Cerințe privind cadrul pentru gestionarea cuprinzătoare a riscurilor

Art. 12. - În vederea asigurării și menținerii unui cadru solid de gestionare a riscurilor, administratorul IPF stabilește și menține proceduri și mecanisme adecvate pentru a identifica, măsura, monitoriza și gestiona în mod cuprinzător gama de riscuri care apar în IPF sau sunt suportate de către aceasta.

Art. 13. - Administratorul IPF trebuie să revizuiască cel puțin anual cadrul de gestionare a riscului, care presupune îndeplinirea următoarelor cerințe:

- a) include politica de toleranță la risc a administratorului IPF și instrumente corespunzătoare de gestionare a riscurilor;
- b) atribuie responsabilități și răspunderi pentru deciziile privind riscul;
- c) include descrierea procesului decizional în situații de urgență legate de o IPF, inclusiv a evoluțiilor de pe piețele financiare care pot avea un efect advers asupra lichidității pieței și asupra stabilității sistemului financiar național.

Art. 14. - (1) Administratorul IPF oferă stimulente participanților și, dacă este cazul, clienților acestora, pentru a gestiona și limita riscurile pe care le induc IPF și pe care le suportă din partea acestora.

(2) În ceea ce privește participanții, administratorul IPF impune un regim de sancțiuni pecuniare eficiente, proporționale și descurajante, acorduri de împărțire a pierderilor sau ambele.

Art. 15. - Pentru o gestionare adecvată a riscurilor administratorul IPF revizuieste, cel puțin anual, riscurile semnificative pe care IPF le suportă din partea altor entități și cele pe care le induce altor entități, inclusiv IPF, bănci de decontare, furnizori de lichiditate și prestatori de servicii, ca urmare a interdependențelor dintre acestea. Administratorul IPF elaborează instrumente de gestionare a riscurilor care sunt robuste și proporționale cu nivelul identificat de risc.

Art. 16. - (1) Administratorul IPF definește operațiunile și serviciile critice ale IPF și identifică scenarii specifice care îl pot împiedica să furnizeze aceste operațiuni și servicii critice în mod continuu și evaluează eficacitatea tuturor opțiunilor de redresare sau de lichidare ordonată.

(2) Administratorul IPF reexaminează cel puțin anual operațiunile și serviciile critice ale IPF.

(3) În baza evaluării stabilite la [alin. \(1\)](#), administratorul IPF pregătește un plan viabil de redresare a IPF și de lichidare ordonată.

(4) Planul de redresare și lichidare ordonată cuprinde, fără a se limita la acestea:

- a) un rezumat cuprinzător al principalelor strategii de redresare și lichidare ordonată;
- b) operațiunile și serviciile critice ale IPF, precum și o descriere a măsurilor necesare pentru a pune în aplicare strategiile-cheie.

(5) Administratorul IPF transmite Băncii Naționale a României informațiile necesare în vederea planificării închiderii ordonate.

SECȚIUNEA a 4-a

Cerințe pentru gestionarea riscului de credit

Art. 17. - (1) Administratorul IPF trebuie să stabilească un cadru robust de măsurare, monitorizare și gestionare a expunerilor sale la riscul de credit față de participanții săi și a expunerilor la riscul de credit între participanți, care decurg din procesele IPF de plată, compensare și decontare, și să identifice toate sursele de risc de credit.

(2) Măsurarea și monitorizarea expunerilor la riscul de credit se efectuează pe întreaga durată a zilei, utilizând informații actualizate și instrumente corespunzătoare de gestionare a riscurilor.

Art. 18. - (1) Administratorul IPF, în cazul unui sistem de decontare pe bază netă amânată, se asigură că:

a) obligațiile financiare sunt stabilite cel târziu în momentul în care un ordin de transfer este inclus în calcularea pozițiilor de decontare netă accesibile fiecărui participant; și

b) sunt deținute suficiente resurse pentru a acoperi expunerile la riscul de credit rezultate potrivit [alin. \(2\)](#) și [\(3\)](#), cel târziu în momentul menționat la lit. a).

(2) Administratorul IPF, inclusiv cel care operează un sistem de decontare pe bază netă amânată cu garantarea decontării, care în cursul operațiunilor IPF suportă expuneri la riscul de credit față de participanții săi, își acoperă expunerea la riscul de credit față de fiecare participant utilizând garanțiile, fondurile de garantare, capitalul propriu (după deducerea sumei dedicate acoperirii riscului general de afaceri) sau alte resurse financiare echivalente.

(3) Administratorul IPF, inclusiv cel care operează un sistem de decontare pe bază netă amânată fără garantarea decontării, dar în care participanții se confruntă cu expuneri la riscul de credit care rezultă din procesele de plată, compensare și decontare ale IPF, dispune de norme sau de acorduri contractuale cu acești participanți.

(4) Normele sau acordurile contractuale prevăzute la alin. (3) trebuie să asigure că participanții vor furniza suficiente resurse, astfel cum sunt prevăzute la [alin. \(2\)](#), pentru a acoperi expunerile la riscul de credit care rezultă din procesele IPF de plată, compensare și decontare în raport cu cei doi participanți care, împreună cu societățile afiliate, generează în sistem cea mai mare expunere agregată la riscul de credit.

(5) Suplimentar, administratorul IPF stabilește reguli și proceduri:

a) pentru gestionarea pierderilor care rezultă direct din neîndeplinirea obligațiilor unuia sau mai multor participanți la IPF;

b) pentru alocarea pierderilor potențial neacoperite, inclusiv rambursarea oricăror fonduri pe care administratorul IPF le poate împrumuta de la furnizorii de lichiditate;

c) pentru reconstituirea, la nivelul prevăzut la [alin. \(2\)](#) și [\(4\)](#), a oricăror resurse financiare utilizate de IPF în cursul unui eveniment de criză.

Art. 19. - (1) Administratorul unei CPC trebuie să asigure decontarea obligațiilor financiare.

(2) În sensul alin. (1), administratorul unei CPC trebuie să acopere complet expunerile curente și potențiale viitoare față de fiecare participant cu un grad ridicat de încredere, utilizând marje și alte resurse financiare prefinanțate potrivit secțiunii a 5-a și a 6-a din prezentul capitol.

(3) În situația unei CPC, care este implicată în activități cu un profil de risc mai complex sau care este de importanță sistemică în mai multe jurisdicții, administratorul trebuie să asigure deținerea unor resurse financiare suplimentare pentru a acoperi o gamă largă de scenarii potențiale de stres, care includ, fără a se limita însă la: intrarea în incapacitate de plată a acelor doi participanți și a societăților afiliate, care ar putea produce cea mai mare expunere agregată la riscul de credit pentru CPC, în condiții de piață extreme, dar plauzibile.

(4) Toate CPC trebuie să asigure deținerea unor resurse financiare suplimentare pentru a acoperi o gamă largă de scenarii potențiale de stres, care includ, fără a se limita însă la: intrarea în incapacitate de

plată a aceluși participant și a societăților afiliate, care ar putea produce cea mai mare expunere agregată la riscul de credit pentru CPC, în condiții de piață extreme, dar plauzibile.

(5) În toate cazurile, administratorul unei CPC documentează justificarea care stă la baza stabilirii valorii resurselor financiare totale pe care le păstrează și trebuie să dispună de aranjamente de guvernare potrivite referitoare la această valoare.

Art. 20. - (1) Administratorul CPC determină valoarea și testează cu regularitate, prin teste de stres riguroase, suficiența resurselor financiare totale disponibile în cazul unei intrări sau al unor intrări multiple în incapacitate de plată, în condiții de piață extreme, dar plauzibile.

(2) Administratorul unei CPC dispune de proceduri clare de raportare a rezultatelor testelor sale de stres către organismele de decizie ale CPC, precum și de utilizare a acestor rezultate pentru a evalua caracterul adecvat al resurselor sale financiare totale și pentru a le ajusta.

(3) Testele de stres sunt realizate zilnic, folosind parametri și ipoteze standard și predeterminate.

(4) Cel puțin o dată pe lună, administratorul unei CPC efectuează o analiză cuprinzătoare și amănunțită a scenariilor testelor de stres, a modelelor, a parametrilor și ipotezelor aferente, pentru a se asigura că acestea sunt adecvate pentru a determina nivelul cerut de protecție al CPC împotriva intrării în incapacitate de plată, având în vedere condițiile de piață curente și evoluția lor.

(5) Administratorul unei CPC efectuează analiza testelor de stres mai des atunci când produsele compensate sau piețele deservite sunt caracterizate de volatilitate ridicată, devin mai puțin lichide sau atunci când dimensiunea sau gradul de concentrare a pozițiilor deținute de către participanții la CPC cresc în mod semnificativ.

Art. 21. - Administratorul unei CPC realizează o validare completă a modelului de administrare a riscului cel puțin o dată pe an.

Art. 22. - (1) Pentru efectuarea testelor de stres, administratorul unei CPC ia în considerare efectul unei game largi de scenarii relevante de stres, atât în privința pozițiilor participanților intrați în incapacitate de plată, cât și din perspectiva posibilelor modificări de preț în perioadele de lichidare a acestor poziții.

(2) Scenariile de stres includ vârfurile istorice relevante ale volatilității prețurilor, schimbările altor factori ai pieței, precum determinanții prețului sau curbele de randament, intrările multiple în incapacitate de plată pe diverse orizonturi de timp, presiunile simultane în cadrul piețelor de finanțare și de active, precum și un spectru de scenarii de stres prospective, într-o varietate de condiții de piață extreme, dar plauzibile.

SECȚIUNEA a 5-a

Cerințe privind aranjamentele de garantare

Art. 23. - În situația în care administratorul unei IPF stabilește aranjamente de garantare pentru a gestiona riscul de credit la care se expune sau la care sunt expuși participanții, va accepta numai garanții cu risc de credit, de lichiditate și de piață scăzut.

Art. 24. - (1) Administratorul unei IPF acceptă cu titlu de garanție numai următoarele active:

a) fonduri bănești; și

b) active cu riscuri scăzute de credit, de lichiditate și de piață, respectiv active pentru care administratorul IPF poate demonstra Băncii Naționale a României, în baza unei evaluări interne adecvate, că îndeplinesc toate condițiile următoare:

- (i) au fost emise de un emitent cu risc scăzut de credit;
- (ii) sunt liber transferabile fără a fi afectate de nicio constrângere juridică sau creanțe ale terților;
- (iii) sunt exprimate într-o monedă al cărei risc este gestionat de administratorul IPF;
- (iv) au date fiabile privind prețurile, publicate în mod periodic;
- (v) nu fac altfel obiectul unor riscuri semnificative de corelare nefavorabilă;
- (vi) nu sunt emise de participantul care furnizează garanția sau de o entitate care face parte din același grup cu respectivul participant, cu excepția cazului de obligațiuni garantate și numai atunci când activele din fondul de acoperire sunt separate în mod corespunzător într-un cadru juridic robust și îndeplinesc cerințele prevăzute la pct. (i)-(v).

(2) Administratorul IPF definește, documentează și aplică o metodologie obiectivă cu privire la analiza îndeplinirii condițiilor aferente evaluării interne asupra activelor, prevăzută la alin. (1) [lit. b](#)).

Art. 25. - (1) Administratorul IPF stabilește și pune în aplicare politici și proceduri de monitorizare a calității creditului, a lichidității pieței și a volatilității prețurilor pentru fiecare activ acceptat drept garanție.

(2) Administratorul IPF monitorizează periodic, cel puțin anual, caracterul adecvat al politicilor și procedurilor prevăzute la alin. (1).

(3) Reexaminarea politicilor și procedurilor prevăzute la alin. (1) este realizată de fiecare dată când are loc o schimbare semnificativă ce afectează expunerea la risc a IPF.

(4) Administratorul IPF evaluează garanțiile la prețul pieței, cel puțin zilnic.

Art. 26. - Administratorul IPF stabilește marje de ajustare a valorii stabile și conservatoare, le testează cel puțin anual și ține seama de condițiile pieței în situație de criză. Procedurile de ajustare a valorii sunt validate, cel puțin anual, de alt personal decât cel care a conceput și aplicat procedurile de ajustare a valorii.

Art. 27. - Administratorul IPF ia măsuri de evitare a concentrării deținerilor de anumite active, atunci când acest lucru ar afecta semnificativ capacitatea de a lichida rapid aceste active, fără efecte adverse semnificative asupra prețului.

Art. 28. - Administratorul IPF care acceptă garanții transfrontaliere identifică și diminuează riscurile asociate utilizării acestora și se asigură că respectiva garanție transfrontalieră poate fi utilizată în timp util.

Art. 29. - Administratorul IPF utilizează un sistem de gestionare a garanțiilor adecvat și flexibil din punct de vedere operațional.

SECȚIUNEA a 6-a **Cerințe privind marjele**

Art. 30. - (1) Administratorul unei CPC trebuie să acopere expunerile sale la riscul de credit față de participanți, pentru toate produsele, prin intermediul unui sistem efectiv de marje, determinat pe baza riscurilor și revizuit cu regularitate.

(2) Nivelurile marjelor trebuie să fie proporționale cu riscurile și caracteristicile particulare ale fiecărui produs, portofoliu și piață pe care o deservește.

(3) Administratorul CPC dispune, în timp util, de o sursă sigură de informații referitoare la preț, pentru sistemul său de marje. Administratorul CPC stabilește proceduri și modele solide de evaluare pentru a adresa circumstanțele în care informațiile referitoare la preț nu sunt disponibile rapid sau nu sunt de încredere.

(4) Administratorul CPC adoptă modele și parametri pentru marjele inițiale care să fie bazate pe risc și care generează cerințe de marjă suficiente pentru a-și acoperi expunerile potențiale viitoare față de participanți, în intervalul dintre ultima colectare a marjelor și lichidarea pozițiilor ca urmare a intrării în incapacitate de plată a unui participant.

(5) Marja inițială îndeplinește un interval stabilit de încredere de cel puțin 99 la sută cu privire la distribuția estimată a expunerilor viitoare.

(6) Pentru administratorul unei CPC care calculează marja la nivelul portofoliului, această cerință se aplică pentru distribuțiile expunerilor viitoare ale fiecărui portofoliu.

(7) Pentru administratorul unei CPC care calculează marja la un nivel mai detaliat, precum un subportofoliu sau pe produs, cerința este îndeplinită pentru distribuțiile corespunzătoare ale expunerilor viitoare.

(8) Modelul utilizat pentru determinarea marjelor trebuie:

a) să utilizeze o estimare precaută a orizonturilor de timp necesare pentru hedging sau închiderea pozițiilor pe fiecare tip de produse compensate de către CPC (inclusiv în condiții de piață tensionate);

b) să dispună de o metodă adecvată de evaluare a expunerii la riscul de credit care să acopere factorii de risc relevanți pentru produse și efectele de portofoliu între produse; și

c) în măsura în care este posibil și prudent, să limiteze necesitatea unor modificări prociclice destabilizatoare.

Art. 31. - Administratorul unei CPC marchează la piață pozițiile participanților și colectează marja de variație cel puțin zilnic, pentru a limita acumularea de expuneri curente.

Art. 32. - Administratorul unei CPC deține autoritatea și capacitatea operațională de a face, în timpul zilei, apeluri în marjă și plăți către participanți, atât programate, cât și neprogramate.

Art. 33. - Pentru a calcula cerințele de marjă, administratorul CPC poate permite compensări sau reduceri ale marjei solicitate cu privire la produsele pe care le compensează sau cu privire la produsele compensate de către aceasta și o altă CPC, dacă riscul unui produs este corelat în mod semnificativ și sigur cu riscul celuilalt produs.

Art. 34. - Acolo unde două sau mai multe CPC sunt autorizate să ofere marje între CPC-uri, acestea trebuie să dețină măsuri de siguranță adecvate și sisteme armonizate de administrare a riscurilor.

Art. 35. - (1) Administratorul unei CPC analizează și monitorizează performanța modelului său și capacitatea de acoperire a marjelor, prin realizarea de teste zilnice riguroase de tip testare a posteriori și cel puțin lunar sau mai des atunci când este cazul de analize de sensibilitate.

(2) Administratorul unei CPC efectuează, cu regularitate, o evaluare a proprietăților teoretice și empirice ale modelului său de marjă pentru toate produsele pe care le compensează.

(3) Pentru realizarea analizelor de senzitivitate a puterii de acoperire a modelului, prevăzute la alin. (1), administratorul unei CPC ia în considerare o gamă largă de parametri și ipoteze, care să reflecte posibilele condiții de piață, inclusiv cele mai volatile perioade înregistrate de către piețele pe care le deservește, precum și schimbările extreme în corelațiile dintre prețuri.

Art. 36. - Administratorul CPC revizuieste și validează cu regularitate sistemul său de marje.

SECȚIUNEA a 7-a

Cerințe privind gestionarea riscului de lichiditate

Art. 37. - (1) Administratorul IPF stabilește un cadru cuprinzător de gestionare a riscurilor de lichiditate generate de participanții la IPF, băncile de decontare, agenții nostro, băncile custode, furnizorii de lichiditate și alte entități relevante.

(2) Cadrul de gestionare a riscurilor de lichiditate furnizează participanților instrumente adecvate pentru a-și administra eficient lichiditatea și asigură monitorizarea și facilitarea fluxului normal de lichiditate în sistem.

Art. 38. - Administratorul IPF stabilește instrumente operaționale și analitice care îi permit să identifice, să măsoare și să monitorizeze fluxurile de decontare și finanțare, inclusiv utilizarea de lichiditate pe parcursul zilei, în mod permanent și în timp util.

Art. 39. - Administratorul IPF, în cazul unui sistem de decontare pe bază netă amânată, se asigură că:

- a) obligațiile financiare sunt stabilite cel târziu în momentul în care un ordin de transfer este inclus în calcularea pozițiilor de decontare netă accesibile fiecărui participant; și
- b) sunt deținute suficiente resurse lichide în conformitate cu [art. 40](#) și [41](#) cel târziu în momentul menționat la lit. a).

Art. 40. - (1) Administratorul IPF deține sau se asigură că participanții dețin permanent suficiente resurse lichide din momentul stabilirii obligațiilor financiare, în toate monedele în care operează, pentru a efectua decontarea în aceeași zi a obligațiilor de plată într-o gamă largă de potențiale scenarii de criză, inclusiv decontarea pe parcursul zilei sau pe durata mai multor zile, dacă este cazul.

(2) Scenariile de criză includ:

- a) o neîndeplinire a obligațiilor, în condiții de piață extreme, dar plauzibile, de către participantul care, împreună cu societățile afiliate, are cea mai mare obligație de plată agregată; și
- b) alte scenarii în conformitate cu [art. 44](#).

Art. 41. - Administratorul IPF care decontează plăți deține sau se asigură că participanții dețin resurse lichide suficiente, în conformitate cu [art. 40](#), pentru efectuarea unei decontări în timp util a obligațiilor financiare în cazul unei neîndepliniri a obligațiilor participantului care, împreună cu societățile afiliate ale acestuia, are cea mai mare obligație financiară agregată, astfel cum se determină la art. 40 alin. (2) [lit. a](#)), în oricare dintre modalitățile următoare:

- a) în numerar la Banca Națională a României sau la o instituție de credit; sau

b) în garanții eligibile pentru operațiunile de piață efectuate de Banca Națională a României, cu condiția ca administratorul IPF să poată demonstra că o astfel de garanție este imediat disponibilă și convertibilă în numerar în aceeași zi, utilizând acorduri de finanțare prestabilite și foarte sigure, chiar în condițiile pieței în situație de criză.

Art. 42. - Administratorul IPF nu prezumă că va fi disponibil credit de urgență din partea băncii centrale.

Art. 43. - Administratorul IPF cu acces la conturile, serviciile de plăți sau serviciile aferente instrumentelor financiare ale Băncii Naționale a României utilizează aceste servicii, acolo unde este practicabil.

Art. 44. - (1) Administratorul IPF, prin simulări riguroase și testare în scenarii de criză, determină nivelul resurselor lichide și testează în mod periodic dacă dispune de resurse lichide suficiente pentru a îndeplini cerințele de la [art. 40](#) și [41](#).

(2) La efectuarea simulărilor de testare la stres, administratorul IPF ia în considerare o gamă largă de scenarii relevante, inclusiv una sau mai multe situații de neîndeplinire a obligațiilor de către participanți în aceeași zi și în două sau mai multe zile ulterioare.

(3) Atunci când sunt avute în vedere astfel de scenarii, sunt luate în considerare proiectarea și funcționarea IPF și sunt examinate toate entitățile care ar putea genera riscuri de lichiditate semnificative la adresa IPF, inclusiv bănci de decontare, agenți nostro, bănci custode, furnizori de lichiditate, precum și IPF conectate.

(4) Scenariile acoperă o perioadă de mai multe zile.

Art. 45. - (1) Administratorul IPF documentează motivele păstrării fondurilor și a altor active menținute de administratorul IPF sau de participanți și are mecanisme de guvernare corespunzătoare în acest sens.

(2) Administratorul IPF stabilește proceduri clare pentru raportarea către consiliu a rezultatelor testărilor obținute potrivit [art. 44](#).

(3) Administratorul IPF utilizează rezultatele testărilor, obținute potrivit [art. 44](#), pentru a evalua adecvarea cadrului său de gestionare a riscurilor de lichiditate și pentru a efectua ajustări ale acestuia.

Art. 46. - (1) Administratorul IPF stabilește reguli și proceduri clare care permit IPF să efectueze decontarea în aceeași zi și, dacă este cazul, decontarea în timp util pe parcursul aceleiași zile și pe durata mai multor zile a obligațiilor financiare în urma neîndeplinirii obligațiilor unuia sau mai multor participanți.

(2) Regulile și procedurile stabilite potrivit alin. (1):

a) vor aborda deficite de lichiditate neprevăzute și potențial neacoperite;

b) vor urmări să evite anularea, revocarea sau întârzierea decontării pe parcursul aceleiași zile a obligațiilor financiare;

c) vor indica modul de reconstituire a fondurilor și a altor active utilizate de IPF în cursul unui eveniment de criză, la nivelul prevăzut la [art. 40-41](#).

Art. 47. - (1) Administratorul unei CPC deține resurse lichide suficiente, în toate monedele relevante, pentru a deconta plăți legate de instrumentele financiare, pentru a face plăți referitoare la marjele de variație solicitate și pentru a îndeplini alte obligații de plată la timp, cu un grad ridicat de încredere,

pentru o gamă largă de scenarii potențiale de stres, care ar trebui să includă, fără a se limita la, intrarea în incapacitate de plată a celui participant și a societăților afiliate care ar genera cea mai mare obligație de plată agregată către CPC, în condiții de piață extreme, dar plauzibile.

(2) Administratorul unei CPC care este implicată în activități cu un profil de risc mai complex sau care este importantă din punct de vedere sistemic în mai multe jurisdicții trebuie să ia în considerare păstrarea unor resurse de lichiditate suplimentare, suficiente pentru a acoperi o gamă mai largă de scenarii potențiale de criză, care ar trebui să includă, fără a se limita la, intrarea în incapacitate de plată a celor doi participanți și a afiliaților acestora care ar genera cea mai mare obligație de plată agregată pentru CPC, în condiții de piață extreme, dar plauzibile.

SECȚIUNEA a 8-a

Cerințe privind decontarea finală

Art. 48. - (1) Decontarea finală se realizează de către administratorul IPF cel mai târziu la sfârșitul zilei stabilite pentru decontare și, de preferat, în timpul zilei sau în timp real, pentru a reduce riscul de decontare.

(2) Un sistem de plăți de mare valoare sau un sistem de decontare a operațiunilor cu instrumente financiare trebuie să ia în considerare adoptarea unui sistem de decontare pe bază brută în timp real sau procesarea în sesiuni multiple, în cadrul zilei de decontare.

(3) Administratorul IPF stabilește în mod clar momentul la care decontarea este finală.

(4) Administratorul IPF definește în mod clar momentul de la care plățile nedecontate, instrucțiunile de transfer sau alte obligații nu mai pot fi revocate de către un participant.

SECȚIUNEA a 9-a

Cerințe privind decontarea fondurilor

Art. 49. - (1) Administratorul IPF care decontează plăți unilaterale în lei se asigură că decontarea finală se efectuează în banii băncii centrale.

(2) Administratorul IPF care decontează plăți bilaterale sau plăți unilaterale în alte monede decât lei se asigură că decontarea finală se efectuează în banii băncii centrale, dacă acest lucru este practic și disponibil.

Art. 50. - Administratorul IPF care decontează plăți pentru alte IPF depune eforturi pentru a permite acestora să efectueze decontări chiar în situații de urgență.

Art. 51. - În cazul în care nu sunt utilizați banii băncii centrale, administratorul IPF se asigură că decontările de fonduri au loc utilizând un activ de decontare cu risc de credit și de lichiditate redus sau care nu presupune risc de credit sau de lichiditate.

Art. 52. - (1) În cazul în care o decontare se efectuează în banii băncii comerciale, administratorul IPF monitorizează, gestionează și limitează riscurile de credit și de lichiditate care provin de la băncile comerciale de decontare.

(2) Administratorul IPF stabilește criterii stricte pentru băncile sale de decontare și monitorizează respectarea lor, luând în considerare, dar fără a se limita la:

- a) reglementarea și supravegherea acestora;
- b) solvabilitatea;
- c) capitalizarea;
- d) accesul la lichiditate; și
- e) siguranța operațională.

(3) Administratorul IPF trebuie să monitorizeze și să gestioneze concentrarea expunerilor la riscul de credit și lichiditate față de băncile comerciale de decontare ale IPF.

Art. 53. - Acordurile juridice ale unui administrator IPF cu orice bănci comerciale de decontare precizează în mod clar:

- a) când se anticipează transferuri în conturile băncilor de decontare individuale;
- b) că transferurile sunt finale atunci când sunt efectuate;
- c) că fondurile primite sunt transferabile imediat ce este posibil, cel târziu până la sfârșitul zilei.

Art. 54. - În cazul în care un administrator IPF efectuează decontări în bani în propriile registre, acesta își minimizează și controlează strict riscurile de credit și de lichiditate.

SECȚIUNEA a 10-a

Cerințe privind livrarea fizică a instrumentelor financiare

Art. 55. - (1) Administratorul IPF stabilește, în mod clar, în regulile unei IPF obligațiile sale cu privire la livrarea fizică a instrumentelor financiare sau a mărfurilor.

(2) Administratorul IPF identifică, monitorizează și administrează riscurile și costurile asociate depozitării și livrării fizice a instrumentelor financiare sau a mărfurilor.

SECȚIUNEA a 11-a

Cerințe aplicabile administratorilor sistemelor de decontare a operațiunilor cu instrumente financiare din cadrul depozitarilor centrali de instrumente financiare (DC)

Art. 56. - Administratorul unui DC trebuie să stabilească reguli și proceduri pentru a asigura diminuarea și gestionarea riscurilor asociate transferului instrumentelor financiare.

Art. 57. - (1) Administratorul unui DC păstrează instrumentele financiare într-o formă imobilizată sau dematerializată, pentru transferul acestora prin înregistrări în conturi.

(2) Administratorul unui DC poate asigura stimulente pentru imobilizarea sau dematerializarea instrumentelor financiare, dacă este cazul.

Art. 58. - Administratorul unui DC identifică, măsoară, monitorizează și administrează riscurile asociate altor activități pe care le-ar putea desfășura, putând fi necesare instrumente suplimentare pentru a gestiona aceste riscuri.

Art. 59. - (1) Confirmarea tranzacțiilor între participanții direcți are loc cât mai curând posibil după încheierea tranzacției, dar nu mai târziu de data tranzacției.

(2) Atunci când este necesară confirmarea tranzacțiilor de către participanții indirecti aceasta are loc cât mai curând posibil după încheierea tranzacției, dar nu mai târziu de ziua lucrătoare imediat ulterioară datei tranzacției.

(3) Decontarea finală se realizează nu mai târziu de două zile lucrătoare după data tranzacției.

Art. 60. - În vederea facilitării decontării tranzacțiilor cu instrumente financiare, administratorul unui DC trebuie să analizeze oportunitatea implementării unui mecanism de împrumut de instrumente financiare, inclusiv aranjamente de tip repo.

SECȚIUNEA a 12-a

Cerințe aplicabile administratorilor sistemelor de decontare prin schimburi de valoare

Art. 61. - Administratorul unui sistem de decontare prin schimburi de valoare trebuie să elimine riscul de principal prin reguli care să asigure că decontarea finală a unei obligații are loc dacă și numai dacă are loc decontarea finală a obligației conexe, indiferent dacă acea IPF decontează pe bază brută sau netă și indiferent de momentul realizării finalității decontării.

SECȚIUNEA a 13-a

Reguli și proceduri privind neîndeplinirea obligațiilor de către un participant

Art. 62. - Administratorul IPF stabilește reguli și proceduri prin care definește cel puțin situația de neîndeplinire a obligațiilor unui participant, atunci când acestea devin scadente, ca urmare a unor cauze operaționale, a încălcării acordurilor la care este parte sau deschiderii procedurii de insolvență împotriva respectivului participant.

Art. 63. - (1) Administratorul IPF definește și distinge între situații automate și discreționare de neîndeplinire a obligațiilor.

(2) În cazul situației discreționare de neîndeplinire a obligațiilor, administratorul IPF precizează entitatea care exercită această putere discreționară.

(3) În situația prevăzută la alin. (2) administratorul IPF reexaminează respectiva definiție cel puțin anual.

Art. 64. - (1) Administratorul IPF stabilește reguli și proceduri pentru cazurile de neîndeplinire a obligațiilor de către participanți care îi permit să continue să își îndeplinească obligațiile.

(2) Regulile și procedurile prevăzute la alin. (1) vizează reconstituirea resurselor în urma unei neîndepliniri a obligațiilor de către unul sau mai mulți participanți.

(3) Regulile și procedurile definesc cel puțin următoarele aspecte:

a) măsurile pe care le poate lua administratorul IPF atunci când are loc o neîndeplinire a obligațiilor;

b) dacă aceste măsuri se iau automat sau în mod discreționar și mijlocul prin care este exercitată această putere discreționară;

- c) modificări potențiale ale practicilor normale de decontare ale unui administrator IPF, pentru asigurarea unei decontări în timp util;
- d) gestionarea plăților în diferite etape de prelucrare;
- e) secvențialitatea probabilă a acțiunilor;
- f) rolurile, obligațiile și responsabilitățile părților relevante, inclusiv ale participanților care nu sunt într-o situație de neîndeplinire a obligațiilor;
- g) alte mecanisme care trebuie activate pentru a limita impactul unei neîndepliniri a obligațiilor.

Art. 65. - Pentru punerea în aplicare a regulilor și procedurilor privind neîndeplinirea obligațiilor, inclusiv orice proceduri discreționare prevăzute în regulile sale, administratorul IPF se asigură că:

- a) are capacitatea operațională, inclusiv suficient personal bine pregătit, pentru a pune în aplicare în timp util procedurile descrise la [art. 64](#); și
- b) regulile și procedurile IPF abordează nevoile de documentare, informare și comunicare, precum și de coordonare, atunci când sunt implicate mai multe IPF sau autorități.

Art. 66. - Administratorul IPF face publice aspectele-cheie ale regulilor și procedurilor descrise la [art. 64](#), incluzând cel puțin următoarele aspecte:

- a) circumstanțele în care se iau măsuri;
- b) cine ia respectivele măsuri;
- c) sfera măsurilor care urmează a fi luate;
- d) mecanismele care vizează obligațiile unui administrator IPF față de participanții care nu sunt într-o situație de neîndeplinire a obligațiilor.

Art. 67. - Administratorul IPF testează și reexaminează regulile și procedurile IPF descrise la [art. 64](#) cel puțin anual sau după orice schimbări semnificative ale IPF care afectează aceste reguli și proceduri. Administratorul IPF implică participanții la IPF și părțile interesate relevante la aceste testări și reexaminări.

SECȚIUNEA a 14-a

Cerințe privind segregarea și portabilitatea pozițiilor și garanțiilor clienților

Art. 68. - (1) Administratorul unei CPC trebuie să dispună de reguli și proceduri de segregare și portabilitate care să protejeze, în mod eficace, pozițiile clienților unui participant și garanțiile corespunzătoare în cazul intrării în incapacitate de plată sau de insolvență a respectivului participant.

(2) Dacă administratorul unei CPC oferă protecție suplimentară pentru pozițiile și garanțiile clientului împotriva intrării simultane în incapacitate de plată a participantului și a unui alt client al acestuia, acel administrator al CPC ia măsuri pentru a se asigura că o astfel de protecție este eficace.

Art. 69. - Administratorul unei CPC utilizează o structură a conturilor care să îi permită să identifice cu promptitudine pozițiile clienților unui participant și să segreghe garanțiile corespunzătoare. Administratorul unei CPC menține pozițiile și garanțiile clientului în conturi de clienți individuale sau în conturi de clienți globale.

Art. 70. - Administratorul unei CPC trebuie să dețină aranjamente de portabilitate structurate, astfel încât să fie accesibilă transferarea pozițiilor și a garanțiilor corespunzătoare ale clienților unui participant intrat în incapacitate de plată, către unul sau mai mulți participanți.

Art. 71. - (1) Administratorul unei CPC are obligația de a face publice regulile, politicile și procedurile sale referitoare la segregarea și portabilitatea pozițiilor și a garanțiilor corespunzătoare ale clienților unui participant.

(2) Administratorul unei CPC face cunoscut dacă garanțiile clientului sunt protejate pe bază individuală sau pe bază globală.

(3) În plus, administratorul unei CPC face cunoscute orice constrângeri, precum constrângeri legale sau operaționale, care ar putea împiedica capacitatea acestuia de a segrega sau de a transfera pozițiile și garanțiile corespunzătoare ale clienților unui participant.

SECȚIUNEA a 15-a

Cerințe privind riscul general de afaceri

Art. 72. - În vederea evitării unor situații care să genereze riscul general de afaceri, administratorul IPF stabilește sisteme robuste de gestionare și control pentru a identifica, monitoriza și gestiona acest risc, inclusiv pierderile care rezultă din executarea defectuoasă a strategiei de afaceri, fluxuri negative de fonduri sau cheltuieli operaționale neașteptate sau excesiv de mari.

Art. 73. - În sensul respectării [art. 72](#) administratorul IPF trebuie să dispună de un plan viabil de redresare și lichidare ordonată, în acord cu [art. 16](#).

Art. 74. - (1) Administratorul IPF determină, pe baza profilului riscului general de afaceri al acestuia și a intervalului de timp necesar pentru a realiza o redresare și/sau o lichidare ordonată a operațiunilor și serviciilor sale critice, valoarea activelor necesare pentru punerea în aplicare a planului prevăzut la [art. 73](#).

(2) Valoarea activelor determinate potrivit alin. (1) nu este mai mică decât cea reprezentată de cheltuielile de exploatare curente pentru cel puțin șase luni.

Art. 75. - (1) Pentru a acoperi valoarea prevăzută la [art. 74](#), administratorul IPF trebuie să dețină active nete lichide finanțate prin capital propriu, precum acțiuni ordinare, rezerve publicate sau alte rezultate reportate, astfel încât să poată asigura continuitatea operațiunilor și a serviciilor.

(2) Aceste active se adaugă resurselor deținute pentru a acoperi neîndeplinirea obligațiilor participanților sau alte riscuri de credit și lichiditate.

(3) Capitalul propriu deținut în baza unor standarde internaționale de capital în funcție de gradul de risc poate fi inclus pentru a evita duplicarea cerințelor de capital.

Art. 76. - (1) Activele menționate la [art. 75](#) deținute pentru acoperirea riscului general de afaceri au o lichiditate și o calitate suficient de ridicate pentru a fi disponibile în timp util și sunt separate de activele administratorului IPF utilizate pentru operațiunile zilnice.

(2) Administratorul IPF este capabil să execute activele deținute pentru acoperirea riscului general de afaceri fără efecte adverse sau cu efecte adverse mici asupra prețurilor, astfel încât să poată asigura continuitatea operațiunilor și a serviciilor dacă înregistrează pierderi comerciale generale.

Art. 77. - Administratorul IPF stabilește un plan viabil privind atragerea de capital suplimentar, în cazul în care capitalul propriu al acestuia se apropie de valoarea prevăzută la [art. 74](#) sau scade sub nivelul acesteia.

SECȚIUNEA a 16-a

Cerințe privind riscul de custodie și de investiție

Art. 78. - (1) Pentru evitarea riscului de custodie, administratorul IPF păstrează activele proprii și ale participanților la entități supravegheate și reglementate, denumite în continuare custodi, care au practici contabile, proceduri de păstrare în siguranță și controale interne care protejează pe deplin aceste active împotriva riscului de pierdere în cazul insolvenței, neglijenței, fraudei, administrării defectuoase sau evidenței necorespunzătoare ale unui custode sau subcustode.

(2) În aplicarea alin. (1), administratorul IPF are acces în timp util la activele sale și la activele furnizate de către participanți.

Art. 79. - Administratorul IPF evaluează și înțelege expunerile proprii față de băncile custode ale acestuia, ținând seama de întreaga sferă a relațiilor sale cu fiecare dintre acestea.

Art. 80. - (1) Administratorul IPF stabilește o strategie de investiții care ia în calcul apariția unor factori care pot să genereze posibile riscuri de investiție și care este în conformitate cu strategia generală a acestuia de gestionare a riscului.

(2) Strategia prevăzută la alin. (1) este comunicată în întregime participanților și este revizuită cel puțin anual.

Art. 81. - Investițiile unui administrator IPF sunt garantate de debitori cu solvabilitate ridicată sau sunt creanțe asupra unor asemenea debitori. Administratorul IPF definește criteriile pentru debitorii de calitate înaltă. Investițiile trebuie să fie în instrumente cu riscuri minime de credit, de piață și de lichiditate.

SECȚIUNEA a 17-a

Cerințe privind gestionarea riscului operațional

Art. 82. - Administratorul IPF stabilește un cadru robust cu sisteme, politici, proceduri și controale adecvate pentru a identifica, monitoriza și gestiona riscul operațional, cu obligația de a le reexamina, audita și testa periodic și după schimbări semnificative.

Art. 83. - (1) Administratorul IPF stabilește obiectivele privind nivelurile serviciilor prestate participanților și fiabilitatea operațională, precum și politicile destinate să atingă aceste obiective, care vor fi reexamineate cel puțin anual.

(2) Administratorul IPF se asigură că IPF are permanent posibilitatea de a ajusta capacitatea de procesare pentru a face față creșterilor volumelor de operațiuni care apar din cauza evenimentelor de criză și că își poate atinge obiectivele privind nivelurile serviciilor.

Art. 84. - Administratorul IPF stabilește politici cuprinzătoare de securitate fizică și a informațiilor care identifică, evaluează și gestionează în mod adecvat toate vulnerabilitățile și amenințările potențiale, care vor fi reexamineate cel puțin anual.

Art. 85. - (1) Administratorul IPF stabilește un plan de continuitate a activității care abordează evenimente care determină un risc semnificativ de perturbare a operațiunilor, care va fi reexaminat și testat cel puțin anual.

(2) Planul stabilit conform alin. (1) include utilizarea unui sediu secundar pentru desfășurarea activității și este proiectat să asigure reluarea operațiunilor critice și funcționarea sistemelor informatice critice în termen de două ore de la producerea acestor evenimente.

(3) Planul de continuitate a activității este conceput astfel încât IPF este întotdeauna capabilă să deconteze toate tranzacțiile scadente până la sfârșitul zilei lucrătoare în care are loc perturbarea.

Art. 86. - Administratorul IPF identifică participanții critici în special pe baza volumelor, a valorilor plăților și a impactului potențial al acestora asupra altor participanți și asupra IPF în ansamblu, în cazul unei probleme operaționale semnificative cu care s-ar confrunța acești participanți.

Art. 87. - Administratorul IPF identifică, monitorizează și gestionează riscurile pe care participanții critici, alte IPF, precum și furnizorii de servicii și utilități le-ar putea genera pentru operațiunile IPF.

Art. 88. - Administratorii IPF trebuie să desemneze anual, până la data de 31 ianuarie, participanții critici, în baza activității acestora din anul anterior și să le comunice acestora calitatea de participanți critici pentru anul curent.

SECȚIUNEA a 18-a

Cerințe privind criteriile de acces și participare

Art. 89. - În vederea asigurării unor condiții echitabile de participare, administratorul IPF stabilește și face publice criteriile nediscriminatorii de acces și participare la serviciile IPF pentru participanții direcți și, dacă este cazul, pentru participanții indirecti, precum și pentru alte IPF, care vor fi reexamineate cel puțin anual.

Art. 90. - (1) Criteriile de acces și participare stabilite potrivit art. 89 sunt justificate în raport cu siguranța și eficiența IPF și a piețelor pe care acesta le deservește și sunt adaptate și proporționale cu riscurile specifice ale IPF.

(2) Pentru asigurarea conformității cu principiul proporționalității, administratorul IPF stabilește cerințele prevăzute la [art. 89](#) astfel încât să limiteze accesul în cea mai mică măsură posibilă.

(3) În cazul în care administratorul IPF refuză accesul unei entități solicitante, motivează în scris acest lucru, în baza unei analize cuprinzătoare a riscului.

Art. 91. - (1) Administratorul IPF monitorizează în mod permanent conformitatea participanților cu criteriile de acces și participare ale IPF.

(2) Administratorul IPF stabilește și face publice procedurile nediscriminatorii de facilitare a suspendării și încetării ordonate a dreptului de participare al unui participant atunci când participantul nu respectă criteriile de acces și participare și face publice aspectele-cheie relevante ale unor astfel de proceduri.

(3) Procedurile stabilite potrivit alin. (2) vor fi reexamineate cel puțin anual.

SECȚIUNEA a 19-a

Cerințe privind acordurile de participare pe niveluri

Art. 92. - (1) În scopul gestionării adecvate a riscurilor, administratorul IPF se asigură că regulile, procedurile și acordurile contractuale ale IPF îi permit colectarea de informații privind participarea indirectă, pentru a identifica, monitoriza și gestiona orice riscuri semnificative la adresa IPF care decurg din participare.

(2) Informațiile pe care le colectează includ cel puțin următoarele aspecte:

a) activitatea pe care participanții direcți o desfășoară în nume propriu și în numele participanților indirecti ca pondere în activitatea la nivelul sistemului;

b) numărul de participanți indirecti care decontează prin intermediul participanților direcți individuali;

c) volumele și valorile tranzacțiilor din IPF care provin de la fiecare participant indirect;

d) volumele și valorile tranzacțiilor menționate la litera c) ca pondere în cele ale participantului direct prin care participantul indirect accesează IPF.

Art. 93. - Administratorul IPF identifică dependențele semnificative dintre participanții direcți și indirecti care pot afecta IPF, luând în considerare informațiile prevăzute la [art. 92](#).

Art. 94. - Administratorul IPF identifică participanții indirecti care generează riscuri semnificative pentru IPF și participanții direcți prin care aceștia accesează IPF, în vederea gestionării acestor riscuri.

Art. 95. - Administratorul IPF reexaminează cel puțin anual riscurile care rezultă din acordurile de participare pe niveluri și ia măsuri de diminuare atunci când este necesar, pentru a se asigura că riscurile sunt gestionate în mod corespunzător.

SECȚIUNEA a 20-a

Cerințe aplicabile conexiunilor între IPF

Art. 96. - În scopul gestionării adecvate a riscurilor asociate conexiunilor între IPF, administratorul IPF identifică, monitorizează și gestionează aceste riscuri.

Art. 97. - Înainte de a stabili o conexiune și în mod permanent odată ce conexiunea a fost stabilită, administratorul IPF identifică, monitorizează și administrează toate sursele potențiale de risc care rezultă din aranjamentul de conexiune.

Art. 98. - Administratorul IPF se asigură că o conexiune dispune de o bază legală solidă, în toate jurisdicțiile relevante, care să sprijine arhitectura sistemului și să ofere o protecție adecvată a IPF implicate în conexiune.

Art. 99. - (1) Administratorii unor DC conectați măsoară, monitorizează și administrează riscurile de credit și de lichiditate generate de ambele părți.

(2) Orice acordare de credit între DC conectați este supusă unei anumite limite și este acoperită integral de garanții de înaltă calitate.

Art. 100. - Transferurile provizorii de instrumente financiare între DC conectați sunt interzise.

Art. 101. - Administratorul unui DC investitor stabilește o legătură cu un DC emitent doar dacă aranjamentul asigură un nivel ridicat de protecție a drepturilor participanților DC investitor.

Art. 102. - Administratorul unui DC investitor care utilizează un intermediar pentru a opera o legătură cu un DC emitent măsoară, monitorizează și administrează riscurile suplimentare, inclusiv riscurile de custodie, de credit, juridice și operaționale, care decurg din utilizarea intermediarului.

Art. 103. - (1) Înainte de a stabili o conexiune cu o altă CPC, administratorul CPC identifică și administrează efectele potențiale de contaminare care decurg din intrarea în incapacitate de plată a CPC conectate.

(2) Dacă o conexiune cuprinde trei sau mai multe CPC, administratorul fiecărei CPC identifică, evaluează și administrează riscurile aranjamentului de conexiune colectiv.

Art. 104. - Fiecare CPC dintr-un aranjament de conexiune între CPC este în măsură să acopere integral, cel puțin zilnic, expunerile sale curente și expunerile potențiale viitoare față de acele CPC cu care este conectată și față de participanții săi, dacă este cazul, cu un grad ridicat de încredere, fără a reduce capacitatea acelei CPC de a-și îndeplini obligațiile, în orice moment, față de propriii participanți.

Art. 105. - Aranjamentele de conexiune între sisteme de plăți sunt concepute astfel încât fiecare sistem de plăți să fie capabil să respecte cerințele prevăzute în anexa [nr. 2](#).

SECȚIUNEA a 21-a

Cerințe privind eficiența și eficacitatea

Art. 106. - Administratorul IPF trebuie să dispună de mecanisme de identificare și îndeplinire a nevoilor piețelor deservite de IPF, în special cu privire la:

- a) alegerea unui mecanism de compensare și decontare;
- b) structura de operare;
- c) sfera produselor compensate sau decontate;
- d) utilizarea tehnologiei și a procedurilor.

Art. 107. - Administratorul IPF trebuie să aibă scopuri și obiective clar definite care sunt măsurabile și realizabile, cum ar fi cele referitoare la nivelurile minime ale serviciilor, așteptările în privința gestionării riscurilor și prioritățile de afaceri.

Art. 108. - Administratorul IPF trebuie să dispună de mecanisme pentru reexaminarea periodică, cel puțin anuală, a cerințelor prevăzute la [art. 106](#) și [107](#).

SECȚIUNEA a 22-a

Proceduri și standarde de comunicare

Art. 109. - (1) În scopul de a facilita plăți, compensări, decontări și înregistrări eficiente, administratorul IPF utilizează proceduri și standarde de comunicare acceptate și relevante la nivel internațional.

(2) În situația în care administratorul IPF nu utilizează proceduri și standarde de comunicare acceptate și relevante la nivel internațional, acesta trebuie să asigure adaptarea propriilor proceduri și standarde

de comunicare astfel încât să fie posibilă conversia sau traducerea datelor din standardele internaționale în cele utilizate la nivel intern și viceversa.

SECȚIUNEA a 23-a

Comunicarea regulilor, procedurilor esențiale și a datelor de piață

Art. 110. - (1) Administratorul IPF adoptă reguli și proceduri clare și cuprinzătoare care sunt comunicate în întregime participanților.

(2) Administratorul IPF trebuie să facă disponibile public regulile și procedurile stabilite potrivit alin. (1), care sunt relevante și, respectiv, esențiale.

Art. 111. - Administratorul IPF comunică descrieri clare ale arhitecturii și operațiunilor sistemului, precum și ale drepturilor și obligațiilor administratorului IPF și ale participanților, astfel încât participanții să poată evalua riscurile pe care le-ar suporta prin participarea la IPF.

Art. 112. - Administratorul IPF oferă toată documentația și formarea necesare și corespunzătoare pentru a facilita înțelegerea de către participanți a regulilor și procedurilor IPF și a riscurilor cu care aceștia se confruntă prin participarea la IPF.

Art. 113. - (1) Administratorul IPF face publice comisioanele IPF la nivelul serviciilor individuale pe care le oferă, precum și politicile sale de reduceri.

(2) Administratorul IPF furnizează descrieri clare ale serviciilor tarificate, din rațiuni de comparabilitate.

Art. 114. - Administratorul IPF comunică public, anual, cel puțin date de bază privind volumele și valorile tranzacțiilor.

SECȚIUNEA a 24-a

Cerințe aplicabile administratorilor IPF pentru asigurarea rezilienței cibernetice

Art. 115. - Administratorul IPF stabilește un cadru eficace de reziliență cibernetică care cuprinde măsuri corespunzătoare de guvernare pentru gestionarea riscului cibernetic, conform anexei nr. 1.

Art. 116. - (1) Administratorul IPF își identifică operațiunile și activele conexe critice și ia măsurile corespunzătoare pentru a le proteja de atacuri cibernetice, precum și pentru a detecta astfel de atacuri, a le răspunde și a se redresa în urma acestora.

(2) Măsurile prevăzute la alin. (1) sunt testate în mod periodic.

Art. 117. - (1) Administratorul IPF se asigură că dispune de un nivel solid de conștientizare a situației în ceea ce privește amenințările cibernetice.

(2) Administratorul IPF asigură existența unui proces de învățare și evoluție continuă care să îi permită să își adapteze, în timp util, oricând este necesar, cadrul de reziliență cibernetică la natura dinamică a riscurilor cibernetice.

CAPITOLUL II

Cerințe aplicabile participanților la infrastructurile pieței financiare

Art. 118. - Participanții la infrastructurile pieței financiare trebuie, în orice moment, să respecte regulile și să îndeplinească cerințele tehnice de funcționare ale infrastructurii respective.

Art. 119. - (1) Participanții critici la IPF trebuie să ia măsurile necesare și să efectueze teste cel puțin anual, pentru a se asigura că au capacitatea operațională, chiar și în scenarii extreme, dar plauzibile, de a relua activitatea de plăți și/sau decontări în cel mult patru ore de la producerea unui eveniment perturbator.

(2) Participanții critici trebuie să dispună permanent de un sediu secundar operațional, suplimentar față de sediul principal, disponibil cel puțin din punctul de vedere al liniilor de comunicații ce permit conectarea la IPF, care să le permită reluarea activităților de plăți și/sau decontări cu respectarea cerințelor de la alin. (1).

Art. 120. - Participanții la IPF ce nu sunt desemnați drept critici trebuie să ia măsurile necesare și să efectueze teste cel puțin anual, pentru a se asigura că au capacitatea operațională, chiar și în scenarii extreme, dar plauzibile, de a relua activitatea de plăți și/sau decontări cel târziu a doua zi lucrătoare după producerea unui eveniment perturbator.

CAPITOLUL III

Cerințe aplicabile prestatorilor de servicii de plată

Art. 121. - Prestatorii de servicii de plată care pun în circulație sau acceptă instrumente de plată au următoarele obligații:

- a) să adopte proceduri care să asigure efectuarea, în mod eficient și conform unui program stabilit, a operațiunilor de plată care derivă din utilizarea instrumentelor de plată;
- b) să asigure, în orice moment, siguranța în funcționare și continuitatea serviciului în condiții de securitate, în scopul asigurării integrității, confidențialității, autenticității și a posibilității de urmărire a operațiunilor de plată și prevenirii utilizării neautorizate a instrumentelor de plată;
- c) să documenteze și să implementeze măsuri privind identificarea, clasificarea, evaluarea, prevenirea și limitarea riscurilor asociate operațiunilor de plată, punerii în circulație și utilizării instrumentelor de plată, inclusiv prin analizarea posibilităților de producere a unor acțiuni de natură frauduloasă, în scopul evitării și limitării pierderilor financiare ale utilizatorilor;
- d) în cazul nefuncționării unui serviciu de plată, prestatorii de servicii de plată vor informa, prin orice mijloace, în cel mult o oră, clienții utilizatori ai respectivului serviciu de plată cu privire la indisponibilitatea acestuia și termenul preconizat pentru remediere și vor relua activitatea de plăți în cel mult opt ore de la producerea unui eveniment perturbator.

TITLUL III

Autorizarea infrastructurilor pieței financiare și notificarea punerii în circulație a instrumentelor de plată

CAPITOLUL I

Autorizarea operării infrastructurilor pieței financiare

Art. 122. - (1) Persoana juridică care intenționează să opereze o IPF pe teritoriul României va înainta Băncii Naționale a României - Direcția monitorizare a infrastructurilor pieței financiare și a plăților o cerere de autorizare conform modelului prevăzut în anexa [nr. 3](#), însoțită de documentația și informațiile prevăzute în prezentul regulament.

(2) Cererea de autorizare va fi însoțită de o autoevaluare, inclusiv documentația justificativă aferentă, privind îndeplinirea permanentă a cerințelor aplicabile administratorilor IPF, stabilite la capitolul I al titlului I din prezentul regulament.

(3) În cazul în care persoana juridică solicitantă consideră că o cerință nu i se aplică, aceasta trebuie să precizeze, în mod clar, în autoevaluarea sa, cerința în cauză și motivele pentru care consideră că cerința nu i se aplică.

(4) Orice informații, date, documente și declarații transmise de către persoana juridică solicitantă în cursul procesului de autorizare a IPF trebuie să fie însoțite de o scrisoare semnată de un reprezentant legal, care să ateste că documentele transmise sunt exacte și informațiile sunt complete la data transmiterii lor către Banca Națională a României.

Art. 123. - (1) În termen de 30 de zile lucrătoare de la primirea cererii, Banca Națională a României analizează documentația prezentată conform [art. 122](#) și informează persoana juridică solicitantă dacă documentația prevăzută la [art. 122](#) este completă.

(2) În cazul în care documentația este incompletă, Banca Națională a României stabilește un termen maxim până la care persoana juridică solicitantă trebuie să completeze documentația, perioadă în care termenul prevăzut la alin. (4) se suspendă.

(3) Persoana juridică solicitantă trebuie să transmită, la solicitarea Băncii Naționale a României, orice alte informații, date, documente și declarații necesare în vederea evaluării respectării cerințelor prezentului regulament.

(4) În termen de 6 luni de la depunerea documentației complete aferente cererii de autorizare, respectiv după termenul prevăzut la alin. (2), Banca Națională a României va transmite persoanei juridice solicitante, în scris, o decizie motivată privind acordarea sau refuzul emiterii autorizației de funcționare a IPF.

Art. 124. - Emiterea autorizației de funcționare nu limitează posibilitatea Băncii Naționale a României de a formula recomandări sau dispune măsuri de remediere și termene de implementare a acestora.

Art. 125. - Prin derogare de la prevederile [art. 122](#), IPF operate pe teritoriul României de către Eurosistem, Banca Centrală Europeană și Banca Națională a României sunt autorizate prin hotărârea Consiliului de administrație al Băncii Naționale a României privind operaționalizarea acestora.

Art. 126. - În cazul unei IPF care operează transfrontalier și care procesează ordine de transfer denumite în lei, autorizarea se va realiza de către Banca Națională a României, în cooperare cu alte bănci centrale și autorități naționale competente din statele membre cu atribuții în autorizarea și monitorizarea IPF, după caz.

Art. 127. - (1) Orice intenție de modificare adusă informațiilor cuprinse în documentația în baza căreia s-a acordat autorizația de funcționare a unei IPF sau a documentelor depuse în acest scop trebuie notificată de către administratorul acesteia Băncii Naționale a României - Direcția monitorizare a infrastructurilor pieței financiare și a plăților în cel mult 5 zile lucrătoare de la luarea deciziei de modificare.

(2) În termen de 30 de zile de la depunerea notificării prevăzute la alin. (1), vizând modificări prevăzute la alin. (3), Banca Națională a României poate stabili un termen până la care administratorul IPF să furnizeze informații și documente suplimentare, urmând ca în termen de 90 de zile de la depunerea documentației complete sau de la data la care expiră termenul stabilit pentru completare, Banca Națională a României să transmită administratorului IPF, în scris, aprobarea sau refuzul modificării solicitate.

(3) Modificările regulilor de sistem sau externalizarea unor servicii și funcții critice vor intra în vigoare numai după primirea aprobării prevăzute la alin. (2).

CAPITOLUL II

Notificarea punerii în circulație a instrumentelor de plată electronică

Art. 128. - (1) Prestatorul de servicii de plată poate pune în circulație instrumente de plată electronică, în termen de 30 de zile lucrătoare de la notificarea Băncii Naționale a României - Direcția monitorizare a infrastructurilor pieței financiare și a plăților și transmiterea tuturor documentelor prevăzute la [art. 129](#).

(2) Banca Națională a României se poate opune, în termenul prevăzut la alin. (1), intenției de punere în circulație a instrumentelor de plată electronică, comunicând în scris prestatorului de servicii de plată opoziția și motivele corespunzătoare.

Art. 129. - (1) În vederea notificării emiterii instrumentelor de plată electronică, prestatorul de servicii de plată va transmite Băncii Naționale a României următoarele documente:

1. În cazul cardurilor:

a) formularul de notificare conform modelului prevăzut la anexa [nr. 4](#); o imagine a cardului, scala 1 la 1, avers și revers;

b) fișa de produs.

2. În cazul instrumentelor de plată electronică cu acces la distanță:

a) formularul de notificare conform modelului prevăzut la anexa [nr. 5](#);

b) fișa de produs;

c) avizul Ministerului Comunicațiilor și Societății Informaționale sau al altor entități indicate de acesta.

(2) Banca Națională a României poate solicita orice alte informații, date, documente și declarații necesare în vederea evaluării cu privire la punerea în circulație a instrumentului de plată electronică. Prestatorul de servicii de plată trebuie să transmită informațiile solicitate în termen de maximum 30 de zile lucrătoare de la data comunicării solicitării, perioadă în care termenul de evaluare prevăzut la art. 128 [alin. \(1\)](#) se suspendă.

Art. 130. - Fișa de produs a instrumentului de plată electronică, prevăzută la [art. 129](#), trebuie să conțină cel puțin informații referitoare la:

- a) descriere, caracteristicile funcționale și aria de utilizare;
- b) producere și distribuire;
- c) procesarea și decontarea operațiunilor de plată efectuate prin intermediul său, inclusiv orarul de funcționare;
- d) descrierea măsurilor de gestionare a riscurilor operaționale și de securitate referitoare la utilizarea și procesarea operațiunilor de plată.

Art. 131. - (1) Modificările intervenite cu privire la documentația prevăzută la [art. 129](#) se vor transmite Băncii Naționale a României - Direcția monitorizare a infrastructurilor pieței financiare și a plăților, în termen de 10 zile la luarea deciziei de modificare.

(2) În situația prevăzută la alin. (1), Banca Națională a României se poate opune, în termen de cel mult 30 de zile de la data primirii tuturor documentelor modificate de către Banca Națională a României, intenției de punere în circulație a instrumentelor de plată electronică, comunicând în scris prestatorului de servicii de plată opoziția și motivele corespunzătoare.

Art. 132. - Prestatorul de servicii de plată care a pus în circulație un instrument de plată electronică are obligația de a notifica Băncii Naționale a României - Direcția monitorizare a infrastructurilor pieței financiare și a plăților decizia de renunțare la punerea în circulație ori de retragere din circulație a instrumentului de plată electronică, în termen de cel mult 30 de zile de la această decizie. În cazul retragerii din circulație va fi precizată în notificare data estimată la care instrumentul nu va mai circula.

CAPITOLUL III

Notificarea punerii în circulație a cecurilor barate

Art. 133. - (1) Instituțiile de credit pot pune în circulație tiraje de cecuri barate, în termen de 30 de zile lucrătoare de la notificarea Băncii Naționale a României - Direcția monitorizare a infrastructurilor pieței financiare și a plăților și transmiterea tuturor documentelor prevăzute la [art. 134](#).

(2) Banca Națională a României se poate opune, în termenul prevăzut la alin. (1), intenției de punere în circulație a tirajului de cecuri barate, comunicând în scris instituției de credit opoziția și motivele corespunzătoare.

Art. 134. - În vederea notificării punerii în circulație a unui tiraj de cecuri barate, instituțiile de credit trebuie să prezinte Băncii Naționale a României următoarele:

- a) formularul de notificare conform modelului prevăzut la anexa [nr. 6](#);
- b) specificația tehnică semnată și ștampilată de către tipografia care a tipărit cecurile barate respective, care să ateste tipărirea tirajului de cecuri barate cu menționarea intervalului numerotat, în conformitate cu prevederile reglementărilor legale în vigoare.

TITLUL IV

Activitatea de monitorizare a infrastructurilor pieței financiare și a instrumentelor de plată

CAPITOLUL I

Obținerea de informații

Art. 135. - (1) Administratorii IPF și prestatorii de servicii de plată care pun în circulație și/sau acceptă instrumente de plată vor furniza Băncii Naționale a României, oricând la solicitarea acesteia, toate informațiile și documentele necesare pentru a evalua conformitatea cu cerințele stabilite de prezentul regulament.

(2) Banca Națională a României poate efectua inspecții la fața locului pentru obținerea și verificarea informațiilor, poate lua în considerare opinii formulate de experți, cum ar fi consultanți și auditori externi, poate utiliza informații furnizate de alte autorități de reglementare sau supraveghere și poate lua în considerare informații și sesizări primite de la utilizatori de instrumente de plată sau participanți.

(3) Informațiile obținute de Banca Națională a României în desfășurarea activității de monitorizare vor putea fi utilizate de Banca Națională a României în contextul participării la misiuni în cadrul Sistemului european al băncilor centrale.

Art. 136. - (1) Administratorii IPF și prestatorii de servicii de plată care pun în circulație și/sau acceptă instrumente de plată vor informa de îndată Banca Națională a României - Direcția monitorizare a infrastructurilor pieței financiare și a plăților, prin mijloace de comunicare stabilite de Banca Națională a României, cu privire la apariția oricăror incidente în funcționarea normală a IPF, a serviciilor de plată sau a instrumentelor de plată, conform formularului din anexa [nr. 7](#) - Raport incidente operaționale și/sau de securitate.

(2) Raportarea de către prestatorii de servicii de plată a incidentelor operaționale și/sau de securitate majore se va face potrivit reglementărilor Băncii Naționale a României.

(3) Administratorii IPF și prestatorii de servicii de plată care pun în circulație și/sau acceptă instrumente de plată vor transmite Băncii Naționale a României - Direcția monitorizare a infrastructurilor pieței financiare și a plăților un raport scris cu explicarea cauzelor incidentelor raportate conform [alin. \(1\)](#), precum și a măsurilor de remediere întreprinse sau avute în vedere, în termen de cel mult 30 de zile calendaristice de la data incidentului.

(4) Banca Națională a României poate solicita în orice moment administratorilor IPF și prestatorilor de servicii de plată care pun în circulație și/sau acceptă instrumente de plată, date, informații și rapoarte suplimentare referitoare la incidentele și fraudele apărute.

Art. 137. - Administratorii IPF trebuie să comunice Băncii Naționale a României, anual, până la data de 31 martie a anului curent, serviciile, funcțiile, participanții și tipurile de instrucțiuni procesate pe care acesta le-a identificat drept critice pentru funcționarea sigură și eficace a IPF.

Art. 138. - (1) Administratorii IPF și prestatorii de servicii de plată care pun în circulație și/sau acceptă instrumente de plată vor efectua cel puțin anual testări ale rezilienței, inclusiv la atacuri cibernetice, a infrastructurii informatice utilizate pentru procesarea plăților, decontărilor și a instrumentelor de plată.

(2) Entitățile prevăzute la alin. (1) vor remite anual, până la data de 31 martie, pentru anul anterior, prin mijloace de comunicare stabilite de Banca Națională a României următoarele informații:

a) scenariile de test avute în vedere și rezultatele testărilor prevăzute la [alin. \(1\)](#);

- b) extrase din rapoartele auditorilor și/sau experților, care să conțină concluziile acestora cu privire la reziliența infrastructurii informatice;
- c) modificările semnificative aduse infrastructurii informatice și locațiilor sediilor secundare ce asigură continuitatea activității de procesare a plăților, decontărilor și a instrumentelor de plată.

CAPITOLUL II

Evaluarea

Art. 139. - (1) Banca Națională a României evaluează complet, cel puțin o dată la 3 ani, IPF prin prisma cerințelor prezentului regulament.

(2) Banca Națională a României poate evalua parțial o IPF, ori de câte ori consideră oportun, în scopul gestionării și prevenirii manifestării riscurilor specifice.

TITLUL V

Măsuri de remediere și sancțiuni

Art. 140. - În situația în care Banca Națională a României constată că cerințele prezentului regulament nu sunt respectate, poate dispune măsuri de remediere și termene de implementare.

Art. 141. - În situația în care Banca Națională a României constată că nu sunt respectate cerințele prezentului regulament și/sau măsurile de remediere nu sunt implementate, în termenele dispuse de Banca Națională a României conform [art. 140](#), Banca Națională a României poate aplica sancțiuni, astfel:

a) administratorilor și participanților la IPF, în conformitate cu prevederile [art. 408](#) din Ordonanța de urgență a Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, aprobată cu modificări și completări prin Legea [nr. 227/2007](#), cu modificările și completările ulterioare;

b) prestatorilor de servicii de plată care pun în circulație și/sau acceptă instrumente de plată, în conformitate cu prevederile art. 57 [alin. \(1\)](#) din Legea nr. 312/2004 privind Statutul Băncii Naționale a României.

Art. 142. - (1) Sancțiunile stabilite de către Banca Națională a României conform art. 141 [lit. a](#)) pot fi contestate în conformitate cu prevederile [art. 275](#) din Ordonanța de urgență a Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, aprobată cu modificări și completări prin Legea [nr. 227/2007](#), cu modificările și completările ulterioare.

(2) Sancțiunile stabilite de către Banca Națională a României conform art. 141 [lit. b](#)) pot fi contestate în conformitate cu prevederile art. 57 [alin. \(2\) - \(4\)](#) din Legea nr. 312/2004 privind Statutul Băncii Naționale a României.

TITLUL VI

Dispoziții tranzitorii și finale

Art. 143. - IPF autorizate de către Banca Națională a României la data intrării în vigoare a prezentului regulament nu necesită o nouă autorizare conform prevederilor [art. 122](#). Acestea se vor conforma cerințelor stabilite la capitolul I al titlului II, în termen de 12 luni de la data intrării în vigoare a prezentului regulament.

Art. 144. - Instrumentele de plată electronică aflate în circulație și notificate Băncii Naționale a României în baza Regulamentului [nr. 6/2006](#) privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente, cu modificările ulterioare, vor face obiectul procedurii de notificare prevăzute la art. 128, în termen de 6 luni de la data intrării în vigoare a prezentului regulament.

Art. 145. - Prezentul regulament intră în vigoare la data publicării în Monitorul Oficial al României, Partea I.

Art. 146. - Anexele [nr. 1-7](#) fac parte integrantă din prezentul regulament.

Art. 147. - De la data intrării în vigoare a prezentului regulament se abrogă:

a) Regulamentul [nr. 9/2007](#) privind monitorizarea sistemelor de plăți, a sistemelor de decontare a operațiunilor cu instrumente financiare și a instrumentelor de plată, publicat în Monitorul Oficial al României, Partea I, nr. 803 din 26 noiembrie 2007;

b) Regulamentul [nr. 1/2005](#) privind sistemele de plăți care asigură compensarea fondurilor, republicat în Monitorul Oficial al României, Partea I, nr. 596 din 29 august 2007, cu modificările ulterioare;

c) Regulamentul [nr. 6/2006](#) privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente, publicat în Monitorul Oficial al României, Partea I, nr. 927 din 15 noiembrie 2006, cu modificările ulterioare;

d) Regulamentul [nr. 1/1995](#) privind principiile și organizarea avizării tehnice a sistemelor de plăți și decontări fără numerar, publicat în Monitorul Oficial al României, Partea I, nr. 75 din 26 aprilie 1995, cu modificările ulterioare.

Președintele Consiliului de administrație al Băncii Naționale a
României,
Mugur Constantin Isărescu

București, 1 august 2018.

Nr. 3.

ANEXA Nr. 1

Cerințe pentru asigurarea rezilienței cibernetice

1. Guvernanța

Administratorul IPF dispune de aranjamente pentru a defini, implementa și revizui periodic cadrul de gestionare a rezilienței cibernetice. Cadrul de gestionare a rezilienței cibernetice acordă o importanță ridicată siguranței și eficienței operațiunilor unei IPF, susținând stabilitatea financiară. Cadrul de gestionare a rezilienței cibernetice trebuie să fie aprobat de consiliu și include:

- a) o strategie privind reziliența cibernetică, care detaliază modul în care sunt determinate obiectivele de reziliență cibernetică, toleranța la riscurile cibernetice și modul în care sunt identificate și administrate riscurile cibernetice, în scopul atingerii obiectivelor stabilite;
- b) obiectivele de reziliență cibernetică, riscurile identificate și măsurile de gestionare a acestora;
- c) cerințele în ceea ce privește resursele umane, tehnologice și procesele necesare gestionării riscurilor cibernetice;
- d) procedurile de comunicare pentru a asigura colaborarea eficace cu toate părțile relevante (cum ar fi autoritățile, alte IPF, participanții și furnizorii de servicii informatice);
- e) definirea rolurilor și responsabilităților consiliului și a managementului în domeniul asigurării rezilienței cibernetice, inclusiv în cazuri de urgență;
- f) procesul de evaluare periodică a adecvării și eficacității cadrului de gestionare a rezilienței cibernetice;
- g) revizuirea periodică a cadrului de gestionare a rezilienței cibernetice, având în vedere noile amenințări, incidentele anterioare și scenarii noi potențiale.

2. Identificarea

Administratorul IPF identifică și clasifică din punctul de vedere al importanței: funcțiile și serviciile furnizate, precum și activele informaționale suport aferente, modalitățile de acces la sistem și dependențele interne și externe. Acestea trebuie protejate, în ordinea priorității, împotriva compromiterii prin atacuri cibernetice. Administratorul IPF identifică riscurile de natură cibernetică pe care le suportă de la sau pe care le induce altor entități.

3. Protecția

Administratorul IPF proiectează sistemele, procesele și serviciile, precum și definește și implementează controale eficiente și eficace, pentru a proteja confidențialitatea, integritatea și disponibilitatea funcțiilor, serviciilor și activelor- suport. Proiectarea și controalele vizează mai multe niveluri de protecție și detecție, în cazul în care măsurile de protecție inițiale eșuează. Criteriile de participare, contractele cu furnizorii externi și conexiunile stabilite sprijină obiectivele de reziliență cibernetică. Măsurile de protecție contra amenințărilor interne includ cel puțin următoarele: înregistrarea și analiza activităților suspecte ale personalului cu acces la sistem, prevenirea pierderii datelor, verificarea personalului la angajare și periodic, inclusiv în cazul modificării responsabilităților, permiterea accesului fizic și informatic la sistem exclusiv personalului autorizat, monitorizat și pregătit.

4. Detectarea

Administratorul IPF implementează proceduri și instrumente de monitorizare în timp real, care permit detectarea unor amenințări, a manifestării unor anomalii sau evenimente ce pot indica un potențial incident de natură cibernetică. Este necesar să fie detectate amenințările cunoscute, precum și cele încă necunoscute, în baza unor criterii de comportament suspect. Detectarea incidentelor se asigură în timp util, pentru a permite aplicarea măsurilor de protecție stabilite în vederea prevenirii și/sau limitării

consecințelor incidentului. Procedurile sprijină procesul de investigare ulterioară a incidentelor, prin păstrarea unor jurnale de operare detaliate o perioadă adecvată de timp.

5. Reluarea activităților

Administratorul IPF dispune de planuri de măsuri pentru a investiga în detaliu și a răspunde eficient și eficace la o gamă largă de incidente cibernetice, în vederea limitării impactului incidentului, reluării activității și recuperării activelor și informațiilor afectate. Administratorul IPF proiectează și testează sistemele și procesele pentru a realiza reluarea în siguranță, cu menținerea integrității datelor, a operațiunilor și serviciilor sale critice, în maximum două ore de la momentul apariției unei perturbări, și să asigure decontarea până la sfârșitul zilei în care s-a manifestat perturbarea, inclusiv în situații extreme, dar plauzibile. Planurile de măsuri au în vedere și situația în care obiectivul de reluare a activității nu este atins, prevăzând sisteme sau proceduri alternative, cum ar fi procesarea manuală, în scopul de a procesa cel puțin instrucțiunile critice. Planurile de măsuri includ păstrarea în siguranță a unor copii de rezervă a datelor și aplicațiilor, reconcilierea periodică și recuperarea datelor și aplicațiilor.

6. Testarea

6.1. Cadrul de administrare a rezilienței cibernetice este testat riguros, cel puțin anual, pentru a determina eficacitatea acestuia. Testele trebuie:

- a) să utilizeze informații actualizate privind amenințările cibernetice, luând în considerare scenarii extreme, dar plauzibile și capacități avansate ale atacatorilor;
- b) să identifice și să evalueze vulnerabilități care pot afecta atingerea obiectivelor de reziliență cibernetică;
- c) să ofere informații utile și credibile pentru gestionarea riscurilor cibernetice.

6.2. Tipurile de teste efectuate includ:

- a) exerciții de identificare și evaluare de vulnerabilități, inclusiv prin operarea periodică pe mediul de producție de la sediul secundar;
- b) testări pe bază de scenarii, inclusiv indisponibilitatea totală a sediului principal în cursul zilei de operare;
- c) teste de penetrare a sistemelor și rețelelor, în special a celor conectate la internet;
- d) teste efectuate de echipe independente față de funcția testată (red teams), care să simuleze atacuri reale și care să vizeze sistemele, rețelele, personalul și procesele.

6.3. Periodic, IPF trebuie să organizeze exerciții de testare a rezilienței cibernetice care să implice cel puțin toți participanții critici, furnizorii critici și IPF conectate. IPF trebuie să participe la exerciții de continuitate a activității organizate de autorități.

7. Conștientizarea amenințărilor

Administratorul IPF monitorizează proactiv amenințările cibernetice curente, pentru a obține și utiliza informații pertinente în vederea prevenirii incidentelor cibernetice și a tratării rapide și eficiente a acestora.

Administratorul IPF stabilește un proces de colectare, analiză și diseminare a informațiilor referitoare la amenințările cibernetice. Cadrul de administrare a rezilienței cibernetice este revizuit continuu în baza acestor informații.

8. Învățarea și dezvoltarea

Administratorul IPF evaluează incidentele cibernetice care au avut loc, mai ales atacurile reușite, monitorizează dezvoltările tehnologice și adoptă măsuri pentru detectarea și contracararea unor posibile amenințări viitoare, prin analiza deviațiilor de la nivelul normal al activităților din sistem și al comportamentelor personalului.

ANEXA Nr. 2

Cerințe aplicabile conexiunilor între sistemele de plăți

1. Generale

- a) Administratorul sistemului de plăți identifică și evaluează toate sursele potențiale de risc care rezultă din stabilirea unei conexiuni, atât înainte de a încheia acordul aferent conexiunii, cât și în mod permanent, după stabilirea acesteia.
- b) Administratorul sistemului de plăți implicat într-o conexiune îndeplinește, întocmai și la timp, toate obligațiile față de sistemele de plăți cu care este conectat și față de participanții săi.
- c) Administratorul sistemului de plăți, care stabilește conexiuni multiple, asigură că riscurile generate într-o conexiune nu se propagă și nu afectează siguranța altor conexiuni și a altor sisteme de plăți.
- d) O conexiune este concepută astfel încât fiecare administrator de sistem de plăți să fie capabil să continue să respecte alte cerințe de monitorizare aplicabile.

2. Siguranța juridică

- a) Cadrul legal aplicabil atât sistemelor de plăți implicate într-o conexiune, cât și cel aplicabil conexiunii în cauză oferă un grad ridicat de certitudine pentru fiecare aspect al funcționării conexiunii, în toate jurisdicțiile relevante.
- b) Regulile, procedurile și contractele care guvernează conexiunea sunt clare, ușor de înțeles și în conformitate cu legile și alte reglementări relevante. Acestea sunt ușor accesibile pentru fiecare parte care are un interes legitim.
- c) Regulile, procedurile și contractele care guvernează conexiunea sunt complete, valabile și aplicabile în toate jurisdicțiile relevante. Există un nivel ridicat de certitudine că măsurile dispuse în conformitate cu aceste reguli și proceduri nu pot fi suspendate, anulate sau reversibile.
- d) Administratorii sistemelor de plăți implicați într-o conexiune identifică și atenuează riscurile care decurg din orice potențial conflict de legi între jurisdicții.
- e) Administratorii sistemelor de plăți implicați într-o conexiune respectă cadrele de reglementare aplicabile.

3. Riscul operațional

- a) Obiectivele administratorului sistemului de plăți privind cerințele și politica de securitate a informației acoperă și aranjamentul aferent conexiunii.
- b) Nivelul de calitate a serviciilor furnizate prin intermediul conexiunii este aprobat de administratorii sistemelor de plăți implicate într-o conexiune și comunicat tuturor părților relevante.

c) Administratorii sistemelor de plăți asigură că aranjamentele de gestionare a riscurilor și capacitatea de procesare sunt dimensionate corespunzător și sunt sigure pentru a opera conexiunea pentru volumele maxime curente și viitoare proiectate ale activității desfășurate prin intermediul conexiunii.

d) Funcționarea conexiunii este testată și monitorizată, în mod corespunzător, și incidentele sunt înregistrate și urmărite. Administratorii sistemelor de plăți conectate și toate părțile implicate convin asupra aranjamentelor privind continuitatea activității desfășurate prin intermediul conexiunii.

4. Riscul financiar

a) Administratorii sistemelor de plăți au o înțelegere clară a impactului pe care conexiunea îl are asupra fiecărui risc la care acestea se expun.

b) Regulile și procedurile sistemului de plăți permit participanților să aibă o înțelegere clară a impactului pe care conexiunea îl are asupra fiecărui risc la care aceștia se expun.

c) Activele utilizate pentru decontare prin intermediul conexiunilor comportă riscuri de credit sau de lichiditate scăzute sau inexistente.

d) Plățile prin intermediul conexiunii sunt decontate prompt, de preferință în cadrul aceleiași zile de operare.

e) Acordul privind stabilirea conexiunii asigură măsuri adecvate pentru gestionarea și minimizarea riscurilor asociate incapacității unui participant de a-și îndeplini prompt obligațiile sale, în special în cazul în care are loc un proces de compensare.

5. Criteriile de acces

a) Criteriile de acces sunt clare, obiective și nediscriminatorii. Aceste criterii sunt publice.

b) Criteriile de acces sunt justificate din perspectiva siguranței și eficienței sistemului de plăți și a piețelor financiare pe care le deservește.

c) Criteriile de acces sunt adaptate în funcție de tipul conexiunii, ținând cont de riscurile la care sunt expuși administratorii sistemelor interconectate și participanții, în cazul fiecărui tip de conexiune.

d) Administratorul sistemului de plăți care refuză stabilirea unei conexiuni trebuie să motiveze solicitantului refuzul, în scris.

e) Administratorul sistemului de plăți implicat într-o conexiune se asigură că prețurile se stabilesc nediscriminatoriu și transparent.

f) Regulile și procedurile de încetare a accesului sunt definite.

6. Eficiența

a) Administratorul sistemului de plăți dispune de scopuri și obiective clar definite, măsurabile și realizabile în legătură cu funcționarea conexiunii, cum ar fi, dar fără a se limita la, nivelul minim de calitate a serviciilor prestate, gestionarea riscurilor și prioritățile de afaceri. Administratorul sistemului de plăți deține mecanisme de revizuire regulată a eficienței și eficacității fiecărei conexiuni.

b) O conexiune este concepută astfel încât să satisfacă nevoile actuale și viitoare ale participanților și ale piețelor pe care le deservește.

c) Stabilirea de conexiuni nu afectează echilibrul dintre eficiență și gestionarea riscului în cadrul sistemelor de plăți.

7. Guvernanța

- a) Conducerea administratorului sistemului de plăți implicat într-o conexiune dispune de o strategie clară privind stabilirea de conexiuni, care este adusă la cunoștința proprietarilor sistemului, autorităților relevante, utilizatorilor și, la un nivel mai general, altor sisteme de plăți.
 - b) Administratorul sistemului de plăți are obiective care evidențiază prioritatea siguranței și eficienței conexiunii și care sprijină, în mod explicit, interesul public.
 - c) Aranjamentele de guvernare asigură că o decizie de a stabili o conexiune reflectă corespunzător obiectivele și interesele părților implicate și modul cum se realizează această reflectare.
 - d) Administratorul sistemului de plăți implicat într-o conexiune trebuie să implementeze mecanisme formalizate pentru schimbul de informații relevante cu părțile implicate relevante și să le consulte atunci când este nevoie.
8. Conexiunile indirecte și conexiunile releu
- a) Înainte de stabilirea unei conexiuni indirecte sau releu, administratorul sistemului de plăți analizează toate riscurile aferente intermedierei schimbului de ordine de plată.
 - b) Administratorul sistemului de plăți care utilizează un intermediar pentru a opera o conexiune cu un alt sistem de plăți cuantifică, monitorizează și gestionează riscul juridic suplimentar, care decurge din utilizarea unui intermediar.
 - c) Administratorii sistemelor de plăți identifică și atenuează adecvat riscul operațional indus de către intermediar.
 - d) Administratorul sistemului de plăți implicat într-o conexiune indirectă sau releu monitorizează adecvat rolul și soliditatea financiară a oricărui intermediar.
 - e) Administratorii sistemelor de plăți implicate într-o conexiune indirectă sau releu se asigură că intermediarul nu restricționează în mod nejustificat utilizarea conexiunii de către orice participant.
 - f) Eficiența și eficacitatea conexiunilor indirecte și releu sunt periodic evaluate și comparate cu canalele alternative de transmitere a ordinelor de transfer, de exemplu, prin conexiuni directe.

ANEXA Nr. 3

Cerere de autorizare a infrastructurii pieței financiare (IPF)

Informații generale

| |
|--|
| Data cererii |
| Denumirea persoanei juridice solicitante |

| |
|--|
| Sediul social |
| Tipul infrastructurii pieței financiare |
| Numele persoanei care își asumă responsabilitatea pentru cerere |
| Datele de contact ale persoanei care își asumă responsabilitatea pentru cerere |
| Numele persoanei responsabile pentru conformitatea IPF |
| Datele de contact ale persoanei responsabile pentru conformitatea IPF |
| Datele de identificare ale societății-mamă (dacă este cazul) |

Referințele documentelor

| Cerința din titlul III capitolul I Autorizarea operării infrastructurilor pieței financiare | Numărul de referință unic al documentului | Titlul documentului | Capitolul, secțiunea ori pagina documentului unde sunt furnizate informațiile sau motivul pentru care nu sunt furnizate informațiile |
|--|---|------------------------|---|
| Art. xx | | | |
| Anexa x, pct. y | | | |

ANEXA Nr. 4

Formular de notificare carduri

..... (numele instituției emitente), înmatriculată la oficiul registrului comerțului cu nr., având cod unic de înregistrare nr., având sediul în țara/județul, localitatea , str. nr., cod poștal, prin, în calitate de reprezentant legal, notificăm emiterea și punerea în circulație a instrumentului de plată electronică de tip card -, în următoarele condiții:

- cont/conturi atașate (monedă națională, valute sau monedă electronică)
- funcționalitate card -
- circulație națională/internațională

- d) card cu bandă magnetică/chip/dual;
- e) executarea plasticului se va face de către societatea, înmatriculată la oficiul registrului comerțului cu nr., având cod unic de înregistrare, cu sediul în localitatea, str. nr., cod poștal;
- f) personalizarea cardurilor se va face de către societatea, înmatriculată la oficiul registrului comerțului cu nr. cu sediul în localitatea, str. nr., cod poștal;
- g) procesarea tranzacțiilor cu carduri se va face de către societatea, înmatriculată la oficiul registrului comerțului cu nr., având cod unic de înregistrare, cu sediul în localitatea, str. nr., cod poștal

Semnătura autorizată a
solicitantului,
S.S./L.S.

ANEXA Nr. 5

Formular de notificare instrumente de plată electronică cu acces la distanță

. (numele instituției emitente), înmatriculată la oficiul registrului comerțului sub nr. /
., având cod unic de înregistrare nr., având sediul în țara/județul,
localitatea, str. nr., cod poștal, prin, în calitate de
reprezentant legal, notificăm emiterea și punerea în circulație a instrumentului de plată electronică cu
acces la distanță de tip, în următoarele condiții:

a) denumire produs;

b) operațiuni efectuate prin intermediul instrumentului

.

.

.;

c) producătorul programului informatic este societatea, înmatriculată la oficiul registrului
comerțului sub nr., având cod unic de înregistrare, cu sediul în localitatea
, str. nr., cod poștal

Semnătura autorizată a

solicitantului,
S.S./L.S.

ANEXA Nr. 6

Formular de notificare tiraj de cecuri barate

..... (numele instituției de credit), înmatriculată la oficiul registrului comerțului cu nr., având cod unic de înregistrare nr., având sediul în țara/județul, localitatea , str. nr., cod poștal, prin, în calitate de reprezentant legal, notificăm punerea în circulație a tirajului de cecuri barate cu seria de la până la
Tipărirea tirajului de cecuri barate s-a realizat de către societatea, înmatriculată la oficiul registrului comerțului cu nr., având cod unic de înregistrare, cu sediul în localitatea, str. nr., cod poștal

Semnătura autorizată a
solicitantului,
S.S./L.S.

ANEXA Nr. 7

Model raport incident operațional sau de securitate

1. Administrator IPF/Prestator de servicii de plată
2. Numele, funcția și datele de contact ale persoanei care raportează incidentul
3. Data și momentul apariției incidentului
4. Data și momentul constatării incidentului
5. Data și momentul finalizării incidentului
6. Tip incident operațional/de securitate (echipament, soft, uman, social, procedură, cauză naturală, altele)
7. Cauza incidentului
8. Descrierea detaliată a incidentului
9. Măsurile luate pentru limitarea consecințelor incidentului
10. Măsurile luate pentru prevenirea unor incidente similare
11. Numele, funcția și datele de contact ale persoanei/persoanelor care pot furniza informații suplimentare legate de incidentul raportat

Parlamentul României

Legea nr. 296/2004 privind Codul consumului

În vigoare de la 01 ianuarie 2007

Formă aplicabilă de la 24 martie 2008

Consolidarea din data de **05 noiembrie 2019** are la bază [republicarea din Monitorul Oficial, Partea I](#) nr. 224 din 24 martie 2008

Include modificările aduse prin următoarele acte: L [161/2010](#).

Ultimul amendament în 22 iulie 2010.

CAPITOLUL I Dispoziții generale

Art. 1. - Prezenta lege, denumită în continuare Codul, are ca obiect reglementarea raporturilor juridice create între operatorii economici și consumatori, cu privire la achiziționarea de produse și servicii, inclusiv a serviciilor financiare, asigurând cadrul necesar accesului la produse și servicii, informării lor complete și corecte despre caracteristicile esențiale ale acestora, apărării și asigurării drepturilor și intereselor legitime ale consumatorilor împotriva unor practici abuzive, participării acestora la fundamentarea și luarea deciziilor ce îi interesează în calitate de consumatori.

Art. 2. - Prevederile prezentului Cod se aplică comercializării produselor noi, folosite sau recondiționate, și a serviciilor, inclusiv a serviciilor financiare, destinate consumatorilor, contractelor încheiate cu consumatorii, regulilor privind publicitatea produselor și serviciilor, cu excepția produselor și serviciilor care sunt reglementate prin legi speciale, a produselor care se comercializează ca antichități și a produselor necesar a fi reparate sau recondiționate pentru a fi utilizate, cu condiția ca operatorul economic să informeze consumatorul despre aceasta.

Art. 3. - Actele normative privind protecția consumatorilor nu trebuie să includă bariere în calea liberei circulații a mărfurilor și serviciilor.

Art. 4. - Principiile de bază ale protecției consumatorilor sunt:

- a) contradictorialitatea - presupune asigurarea posibilității persoanelor aflate pe poziții divergente de a se exprima cu privire la orice act sau fapt care are legătură cu posibila încălcare a dispozițiilor privind protecția consumatorilor;
- b) celeritatea procedurii de cercetare - presupune obligația autorității competente în domeniul protecției consumatorilor de a proceda, fără întârziere, la cercetarea sesizării consumatorilor, cu respectarea drepturilor persoanelor implicate și a regulilor prevăzute de lege;
- c) proporționalitatea - conform căreia trebuie respectat un raport corect între gravitatea sau consecințele faptei constatate, circumstanțele săvârșirii acesteia și măsura sancționatorie aplicată;
- d) legalitatea măsurilor propuse/dispuse - presupune că autoritățile competente nu pot propune/dispune decât măsurile prevăzute de lege;

e) confidențialitatea - obligația personalului din cadrul autorităților competente de a păstra confidențialitatea datelor, actelor, informațiilor de orice natură, prin a căror divulgare se pot aduce prejudicii persoanelor fizice sau juridice, care sunt sau pot fi menționate în aceste informații;

f) recunoașterea reciprocă - orice produs legal fabricat sau comercializat într-un stat membru al Uniunii Europene sau în Turcia ori fabricat în mod legal într-un alt stat aparținând Spațiului Economic European este admis pe teritoriul României, dacă oferă un grad echivalent de protecție cu cel impus de normele române.

Art. 5. - Statul, prin autoritatea centrală cu atribuții în domeniul protecției consumatorilor, are drept obiective:

a) protecția consumatorilor împotriva riscului de a achiziționa un produs sau de a li se presta un serviciu care ar putea să le prejudicieze viața, sănătatea sau securitatea ori să le afecteze drepturile și interesele legitime;

b) promovarea și protecția intereselor economice ale consumatorilor;

c) accesul consumatorilor la informații complete, corecte și precise asupra caracteristicilor esențiale ale produselor și serviciilor, astfel încât decizia pe care o adoptă în legătură cu acestea să corespundă cât mai bine nevoilor lor;

d) educarea consumatorilor;

e) despăgubirea efectivă a consumatorilor;

f) sprijinirea consumatorilor sau a altor grupuri sau organizații reprezentative de a se organiza, pentru a-și expune opiniile în procesele de luare a unei decizii care îi privește;

g) promovarea cooperării internaționale în domeniul protecției consumatorilor și participarea la schimburile rapide de informații;

h) prevenirea și combaterea, prin toate mijloacele, a practicilor comerciale abuzive și a prestării serviciilor, inclusiv a celor financiare care pot afecta interesele economice ale consumatorilor.

Art. 6. - Prevederile cuprinse în prezentul Cod sunt obligatorii pentru toți consumatorii și operatorii economici care efectuează acte și fapte de comerț, în condițiile legii.

Art. 7. - Termenii utilizați în legislația privind protecția consumatorilor sunt enumerați cu titlu exemplificativ în anexa care face parte integrantă din prezentul Cod.

CAPITOLUL II

Obligațiile operatorilor economici

Art. 8. - Operatorii economici sunt obligați să pună pe piață numai produse sau servicii sigure, care corespund caracteristicilor prescrise sau declarate, să se comporte în mod corect în relațiile cu consumatorii și să nu folosească practici comerciale abuzive.

Art. 9. - Sunt interzise importul, fabricația, distribuția, precum și comercializarea produselor falsificate ori contrafăcute, periculoase sau care au parametrii de securitate neconformi care pot afecta viața, sănătatea sau securitatea consumatorilor.

Art. 10. - Este interzisă condiționarea vânzării către consumator a unui produs, de cumpărarea unei cantități impuse sau de cumpărarea concomitentă a unui alt produs sau serviciu. De asemenea, este

interzisă prestarea unui serviciu către consumator, condiționată de prestarea altui serviciu sau de cumpărarea unui produs.

Art. 11. - Orice vânzare forțată este interzisă. Expedierea unui produs sau prestarea unui serviciu către o persoană se face numai în baza unei comenzi prealabile din partea acesteia.

Art. 12. - Cheltuielile legate de înlocuirea produselor defecte, de remedierea sau de restituirea contravalorii acestora vor fi suportate de vânzător și recuperate de acesta de la producător sau, după caz, de la importator sau de la furnizorul anterior aflat pe lanțul de distribuție, dacă prin contractul încheiat între aceștia nu s-a stabilit altfel.

Art. 13. - Orice persoană care are calitatea de producător, distribuitor sau vânzător de produse alimentare va comercializa numai alimente care prezintă siguranță pentru consumator, sunt salubre și apte pentru consum uman.

Art. 14. - Consumatorii trebuie să primească toate informațiile necesare pentru o utilizare corespunzătoare, potrivit destinației inițiale a bunurilor.

Art. 15. - În cazul în care operatorii economici iau cunoștință, la o dată ulterioară punerii pe piață a produselor comercializate, despre existența unor pericole care, la momentul punerii pe piață nu puteau fi cunoscute, trebuie să anunțe, fără întârziere, autoritățile competente și să facă aceste informații publice.

Art. 16. - În cazul produselor identificate sau identificabile cu defecte, producătorii și/sau distribuitorii au obligația de a le retrage de pe piață, de a le înlocui sau de a le repara, iar în situația în care aceste măsuri nu pot fi făcute într-o perioadă rezonabilă de timp, stabilită de comun acord între vânzător și consumator și fără niciun inconvenient semnificativ pentru consumator, consumatorul trebuie să fie compensat în mod corespunzător.

Art. 17. - În cazul lipsei conformității, astfel cum este prevăzut în actele normative în domeniul conformității produselor, constatate de consumator, acesta are dreptul de a solicita vânzătorului, ca măsură reparatorie, repararea sau înlocuirea produselor, în fiecare caz fără plată, cu excepția cazului în care această solicitare este imposibilă sau disproporționată.

Art. 18. - Orice reparare sau înlocuire a produselor va fi făcută în cadrul unei perioade rezonabile de timp, stabilită de comun acord între vânzător și consumator și fără niciun inconvenient semnificativ pentru consumator, luând în considerare natura produselor și scopul pentru care acesta a solicitat produsele, în condițiile legii.

Art. 19. - Guvernul elaborează prevederi privind reguli de securitate și reguli privind întocmirea documentelor de conformitate, care asigură că produsele comercializate pe piață sunt sigure.

Art. 20. - Ambalajele produselor trebuie să asigure integritatea și protecția calității acestora, fiind, totodată, conforme prevederilor legale referitoare la protecția muncii, mediului și a securității consumatorilor.

Art. 21. - Operatorii economici sunt obligați să comercializeze alimente care:

- a) sunt însoțite de documente care le atestă originea, proveniența și securitatea, după caz;
- b) sunt manipulate și comercializate în condiții corespunzătoare de igienă, care nu pun în pericol viața și sănătatea consumatorilor și care respectă normele sanitare în vigoare;
- c) nu afectează viața și sănătatea consumatorilor.

Art. 22. - Se interzice comercializarea produselor ce imită produsele alimentare, fără a fi astfel de produse și care prezintă riscul de a pune în pericol sănătatea sau securitatea consumatorilor, conform reglementărilor legale în vigoare.

Art. 23. - Obligațiile producătorului:

- a) să răspundă pentru prejudiciul actual și cel viitor cauzat de produsul cu defect, precum și pentru cel cauzat ca rezultat cumulativ al produsului cu defect cu o acțiune sau o omisiune a unei terțe persoane;
- b) să pună pe piață numai produse sigure și, dacă actele normative în vigoare prevăd, acestea să fie testate și/sau certificate;
- c) să pună pe piață numai produse care respectă condițiile prescrise sau declarate;
- d) să oprească livrările, respectiv să retragă de pe piață sau de la consumatori produsele la care organele abilitate sau specialiștii proprii au constatat neîndeplinirea caracteristicilor prescrise, declarate sau care ar putea afecta viața, sănătatea ori securitatea consumatorilor, dacă această măsură constituie singurul mijloc prin care se pot elimina neconformitățile respective;
- e) să asigure, în cursul procesului de producție, condiții igienico-sanitare conform normelor sanitare în vigoare.

Art. 24. - Obligațiile distribuitorilor:

- a) să se asigure că produsele oferite spre comercializare sunt sigure și respectă condițiile prescrise sau declarate;
- b) să nu comercializeze produse despre care dețin informații sau consideră că pot fi periculoase;
- c) să anunțe, imediat, autoritățile publice competente, precum și producătorul, despre existența pe piață a oricărui produs de care au cunoștință că este periculos;
- d) să retragă de la comercializare produsele la care organele abilitate de lege au constatat că nu îndeplinesc caracteristicile prescrise sau declarate, dacă acesta constituie singurul mijloc prin care se pot elimina neconformitățile respective;
- e) să asigure condițiile tehnice stabilite de producător, precum și condițiile igienico-sanitare pe timpul transportului, manipulării, depozitării și desfacerii, conform normelor în vigoare.

Art. 25. - Obligațiile prestatorilor de servicii:

- a) să folosească, în cadrul serviciilor prestate, numai produse și proceduri sigure și, după caz, dacă actele normative în vigoare prevăd, acestea să fie testate și/sau certificate și să anunțe imediat existența pe piață a oricărui produs despre care au cunoștință că este periculos;
- b) să presteze numai servicii care nu afectează viața, sănătatea sau securitatea consumatorilor ori interesele economice ale acestora;
- c) să respecte condițiile prescrise sau declarate, precum și clauzele prevăzute în contracte;
- d) să asigure, la prestarea serviciilor, condițiile tehnice stabilite de producător, precum și condițiile igienico-sanitare, conform normelor în vigoare;
- e) să răspundă pentru prejudiciul actual și cel viitor cauzat de serviciul defectuos prestat.

Art. 26. - (1) Alte obligații ale operatorilor economici sunt:

- a) de a comercializa sau oferi, cu titlu gratuit, numai produse sigure, aflate în cadrul termenului de valabilitate și care nu prezintă riscuri pentru viața, sănătatea și/sau securitatea consumatorilor;

- b) de a nu comercializa, în spații în care nu pot fi asigurate condițiile de păstrare cerute de producător pentru a se preveni perisabilitatea accelerată, produse alimentare preambalate sau ambalate;
 - c) de a nu comercializa, în alte condiții decât cele cerute de legislația în vigoare, produse nealimentare noi, folosite sau recondiționate, fără a putea fi, acolo unde este cazul, probate, verificate sau asigurate condițiile de păstrare cerute de producător, pentru a se asigura menținerea caracteristicilor inițiale ale produselor;
 - d) de a nu importa, în vederea distribuției cu titlu oneros sau gratuit, produse periculoase, expirate sau care pot afecta viața, sănătatea și/sau securitatea consumatorilor prin utilizarea acestora.
- (2) Dispozițiile alin. (1) se aplică și persoanelor fizice sau juridice care pot avea calitatea de operator economic.

CAPITOLUL III

Drepturile consumatorilor

Art. 27. - Consumatorii beneficiază de următoarele drepturi:

- a) de a fi protejați împotriva riscului de a achiziționa un produs sau de a li se presta un serviciu care ar putea să le prejudicieze viața, sănătatea sau securitatea ori să le aducă atingere drepturilor și intereselor legitime;
- b) de a fi informați complet, corect și precis, asupra caracteristicilor esențiale ale produselor și serviciilor, astfel încât decizia pe care o adoptă în legătură cu acestea să corespundă cât mai bine nevoilor lor, precum și de a fi educați în calitatea lor de consumatori;
- c) de a avea acces la piețe care le asigură o gamă variată de produse și servicii de calitate;
- d) de a fi despăgubiți în mod real și corespunzător pentru pagubele generate de calitatea necorespunzătoare a produselor și serviciilor, folosind în acest scop mijloace prevăzute de lege;
- e) de a se organiza în asociații ale consumatorilor, în scopul apărării drepturilor și intereselor lor;
- f) de a refuza încheierea contractelor care cuprind clauze abuzive, conform prevederilor legale în vigoare;
- g) de a nu li se interzice de către un operator economic să obțină un beneficiu prevăzut în mod expres de lege.

Art. 28. - Se interzice refuzul vânzării unui produs sau prestării unui serviciu către un consumator fără un motiv justificat conform prevederilor legale în vigoare.

CAPITOLUL IV

Cadrul organizatoric al organizațiilor neguvernamentale

Art. 29. - Organizațiile neguvernamentale ale consumatorilor pot fi parteneri sociali cu drept de reprezentare în organismele constituite la nivel central sau local, cu rol în domeniul protecției consumatorilor, în care organele administrației publice sunt reprezentate.

Art. 30. - Personalul de conducere și salariații organelor de specialitate ale administrației publice, precum și ale serviciilor publice deconcentrate ale ministerelor sau ale altor autorități, cu atribuții în

domeniul protecției consumatorilor, nu au dreptul de a deține funcții în organele de conducere ale organizațiilor neguvernamentale ale consumatorilor.

Art. 31. - Organizațiile neguvernamentale ale consumatorilor pot fi consultate de către autoritățile administrației publice cu atribuții în domeniul protecției consumatorilor, la elaborarea dispozițiilor și procedurilor cu caracter general și a altor lucrări care au ca scop protecția consumatorilor, cu privire la:

- a) cunoașterea cerințelor consumatorilor privind sortimentele și calitatea produselor și serviciilor;
- b) formarea unei atitudini corecte a operatorilor economici, angajați în producerea și comercializarea produselor și prestarea serviciilor, față de calitatea acestora;
- c) prevenirea practicilor comerciale abuzive și a publicității de natură a afecta drepturile și interesele legitime ale consumatorilor.

Art. 32. - Organizațiile neguvernamentale ale consumatorilor au următoarele drepturi:

- a) de a fi sprijinite logistic de către organismele administrației publice centrale și locale, în vederea atingerii obiectivelor lor;
- b) de a primi sume de la bugetul de stat și de la bugetele locale;
- c) de a fi consultate, cu ocazia elaborării proiectelor de acte normative, standardelor sau specificațiilor care definesc caracteristicile tehnice și calitative ale produselor și serviciilor destinate consumatorilor;
- d) de a introduce acțiuni în justiție pentru apărarea drepturilor și intereselor legitime ale consumatorilor;
- e) de a obține informații asupra prețului și caracteristicilor calitative ale produselor sau serviciilor, de natură să ajute consumatorul la luarea unei decizii asupra achiziționării acestora.

Art. 33. - Organizațiile neguvernamentale ale consumatorilor au următoarele obligații:

- a) de a solicita autorităților competente luarea de măsuri în vederea opririi producției sau retragerii de pe piață a produselor ori serviciilor care nu asigură nivelul calitativ prevăzut în documentele stabilite de lege sau care pun în pericol viața, sănătatea ori securitatea consumatorilor;
- b) de a propune operatorilor economici realizarea de produse și servicii în condiții speciale, în vederea satisfacerii nevoilor consumatorilor cu handicap sau de vârstă a treia;
- c) de a solicita informații asupra prețului și caracteristicilor calitative ale produselor sau serviciilor, de natură să ajute consumatorul la luarea unei decizii asupra achiziționării acestora;
- d) de a informa opinia publică, prin mass-media, asupra neconformității produselor și serviciilor existente pe piață, precum și asupra posibilelor consecințe vătămătoare dovedite ale acestora pentru consumatori.

Art. 34. - Reprezentanții organizațiilor neguvernamentale ale consumatorilor nu au drept de control al operatorilor economici.

CAPITOLUL V

Cadrul general al securității produselor

Art. 35. - Riscul se consideră acceptabil și compatibil cu un grad înalt de protecție pentru siguranța și sănătatea consumatorilor, evaluarea riscului făcându-se în funcție de următoarele aspecte:

- a) caracteristicile produsului, ale ambalării și ale instrucțiunilor de montaj și întreținere;

- b) efectul asupra altor produse, împreună cu care acesta poate fi folosit;
- c) modul de prezentare a produsului, etichetarea, instrucțiunile de folosire și orice alte indicații și informații furnizate de producător;
- d) categoria de consumatori expusă riscului prin folosirea produsului.

Art. 36. - (1) Orice operator economic este obligat să introducă pe piață numai produse sigure pentru viața, sănătatea și securitatea consumatorilor.

(2) Orice comerciant trebuie să se asigure că produsele oferite spre comercializare sunt sigure și să informeze consumatorii asupra factorilor de risc în utilizarea și/sau consumul acestora.

Art. 37. - Este interzisă comercializarea produselor care nu sunt sigure, cât și a produselor neînsoțite de documentația obligatorie prevăzută de lege, prin care să se ateste că ele au fost testate și/sau certificate, după caz.

CAPITOLUL VI

Cadrul general privind obligativitatea informării și educării consumatorilor

Art. 38. - Statul trebuie să realizeze și să încurajeze folosirea de programe menite să asigure consumatorilor o informare și o educare corespunzătoare, pentru a permite acestora să acționeze în mod distinct, în vederea unei alegeri corecte bazate pe o informare corespunzătoare asupra bunurilor și a serviciilor și să fie cunoscători ai drepturilor și responsabilităților ce le revin.

Art. 39. - Statul, prin mijloacele sale, are ca scop protejarea consumatorilor la achiziționarea de produse și servicii, precum și protejarea interesului public general împotriva publicității înșelătoare, a consecințelor negative ale publicității și stabilește condițiile în care este permisă publicitatea comparativă.

Art. 40. - Educarea consumatorilor este o parte din programul de învățământ și o componentă a obiectelor de studii. Formarea competențelor în domeniul protecției consumatorului și a mediului se realizează în cadrul programului de învățământ. Formarea competențelor practice se realizează inclusiv prin colaborarea instituțiilor de învățământ preuniversitar cu operatorii economici din domeniu.

Art. 41. - În programele de educare și informare a consumatorilor se includ ca aspecte importante ale protecției acestora:

- a) legislația referitoare la protecția consumatorilor, agenții și organizații ale consumatorilor;
- b) sănătatea, alimentația, prevenirea îmbolnăvirilor și prevenirea achiziționării de produse alimentare falsificate;
- c) riscurile produselor;
- d) interesele economice ale consumatorilor la achiziționarea de servicii, inclusiv a celor financiare;
- e) practicile comerciale ale producătorilor, prestatorilor sau distribuitorilor și prevenirea actelor de comerț incorecte;
- f) etichetarea produselor, cu precizarea informațiilor necesare consumatorilor;
- g) informații despre dificultăți și măsuri de rezolvare a acestora, prețuri, calitate, condiții de creditare;
- h) protecția mediului, după caz.

Art. 42. - Programele ce privesc educarea și informarea consumatorilor pot fi implementate și prin intermediul organizațiilor neguvernamentale ale consumatorilor.

Art. 43. - Operatorii economici pot contribui și colabora cu terțe părți la realizarea unor programe reale și eficiente de educare și informare a consumatorilor.

Art. 44. - Având în vedere necesitatea asigurării unei informări complete, concrete și inteligibile a consumatorilor pot fi inițiate programe privind informarea consumatorilor prin mass-media.

Art. 45. - Consumatorii au dreptul de a fi informați, în mod complet, corect și precis, asupra caracteristicilor esențiale ale produselor și serviciilor, inclusiv a serviciilor financiare oferite de către operatorii economici, astfel încât să aibă posibilitatea de a face o alegere rațională între produsele și serviciile oferite, în conformitate cu interesele lor economice și de altă natură și să fie în măsură să le utilizeze, potrivit destinației acestora, în deplină siguranță și securitate.

Art. 46. - Informațiile privind protejarea vieții, sănătății și securității consumatorilor trebuie să fie comunicate acestora, pe cât este posibil și prin simboluri grafice internaționale, ușor de înțeles.

Art. 47. - Informarea consumatorilor despre produsele și serviciile oferite se realizează, în mod obligatoriu, prin elemente de identificare și caracterizare ale acestora, înscrise la vedere, în mod vizibil, lizibil și ușor de înțeles, după caz, pe produs, etichetă, ambalaj de vânzare sau în cartea tehnică, instrucțiunile de folosire ori altele asemenea, ce însoțesc produsul sau serviciul, în funcție de natura acestuia.

Art. 48. - Consumatorii trebuie să fie informați despre riscurile la care sunt supuși prin folosirea normală sau previzibilă a bunurilor.

Art. 49. - Scopul etichetării este de a oferi consumatorilor informațiile necesare, suficiente, verificabile și ușor de comparat, astfel încât să permită acestora să aleagă acel produs care corespunde exigențelor lor din punct de vedere al nevoilor și posibilităților lor financiare, precum și de a cunoaște eventualele riscuri la care ar putea fi supuși.

Art. 50. - Informațiile de pe etichetele produselor trebuie să fie înscrise în limba română, indiferent de țara producătoare, fără a se exclude prezentarea lor și în alte limbi, să fie vizibile, lizibile și inscripționate într-un mod care să nu permită ștergerea lor.

Art. 51. - Etichetarea și metodele prin care aceasta se realizează nu trebuie să atribuie alimentelor proprietăți de prevenire, tratare sau vindecare a bolilor sau să facă referiri la astfel de proprietăți; sunt exceptate de la această interdicție apele minerale naturale, precum și orice alimente cu destinații nutriționale speciale, expres prevăzute prin acte normative.

Art. 52. - (1) Pentru produsele alimentare, producătorul, astfel cum este definit în anexă, are obligația de a informa despre denumirea produsului, denumirea și/sau marca producătorului, cantitatea și, după caz, termenul de valabilitate ori data durabilității minime, lista ingredientelor, despre eventualele riscuri previzibile, modul de utilizare, manipulare, depozitare sau păstrare, despre contraindicații, mențiuni suplimentare pe grupe de produse, precum și alte mențiuni prevăzute de lege.

(2) Producătorul are obligația să-și precizeze adresa pe etichetă până la data aderării României la Uniunea Europeană.

Art. 53. - Pentru produsele de folosință îndelungată, acestea trebuie să fie însoțite de certificatul de garanție și, dacă reglementările în vigoare prevăd, de declarația de conformitate, precum și de cartea

tehnică ori de instrucțiunile de folosire, instalare, exploatare, întreținere, eliberate de către producător, conform prevederilor legale.

Art. 54. - Vânzătorul trebuie să informeze consumatorii despre prețul final al produsului și să ofere acestora toate informațiile și documentele tehnice care trebuie să însoțească produsul.

Art. 55. - Toate informațiile privitoare la produsele și serviciile oferite consumatorilor, documentele însoțitoare, precum și contractele preformulate, trebuie să fie scrise în limba română, indiferent de țara de origine a acestora, fără a exclude prezentarea acestora și în alte limbi.

Art. 56. - Denumirea sub care este vândut alimentul consumatorului sau operatorilor economici care prepară ori furnizează hrana pentru populație este cea prevăzută de reglementările specifice alimentului respectiv.

Art. 57. - În cazul prestărilor de servicii, informațiile trebuie să cuprindă categoria calitativă a serviciului, după caz, timpul de realizare, termenul de garanție și postgaranție, prețurile și tarifele, riscurile previzibile și, după caz, alte documente prevăzute expres de lege. În cazul serviciilor financiare, operatorii economici sunt obligați să ofere consumatorilor informații complete, corecte și precise asupra drepturilor și obligațiilor ce le revin.

Art. 58. - La punerea pe piață a produselor de folosință îndelungată, operatorii economici pot efectua demonstrații de utilizare, în public sau prin intermediul mass-media, în scopul promovării produsului respectiv.

Art. 59. - Operatorii economici sunt obligați să demonstreze consumatorilor, la cererea acestora, cu ocazia cumpărării, modul de utilizare și funcționare a produselor ce urmează a fi vândute, după caz.

Art. 60. - Obligația informării consumatorului privind elementele esențiale referitoare la produsul achiziționat nu poate fi înlăturată, de către operatorul economic care l-a comercializat, prin invocarea secretului comercial sau profesional, cu excepția cazurilor prevăzute de lege.

Art. 61. - Se interzice prezentarea, prin orice mijloace, a afirmațiilor și indicațiilor care nu sunt conforme cu parametrii ce caracterizează produsele și serviciile și care nu pot fi probate.

Art. 62. - Comercializarea produselor și prestarea serviciilor se fac numai în locuri și în spații autorizate, conform reglementărilor legale în vigoare.

Art. 63. - Este obligatorie afișarea, în mod vizibil, a denumirii unității, a autorizației de funcționare, a avertismentelor obligatorii prevăzute de lege, precum și afișarea orarului de funcționare.

CAPITOLUL VII

Cadrul general privind prețurile și tarifele

Art. 64. - Operatorul economic care, în rețeaua de distribuție, oferă spre vânzare produse/servicii trebuie să indice prețul de vânzare/tarif practicat și prețul pe unitatea de măsură, conform reglementărilor legale în vigoare.

Art. 65. - Prețurile și tarifele trebuie indicate în mod vizibil și într-o formă neechivocă, ușor de citit, prin marcare, etichetare și/sau afișare.

Art. 66. - Informațiile furnizate de aparatele de măsură utilizate pentru determinarea cantității produselor vândute în vrac trebuie să fie clare și ușor vizibile pentru consumator.

Art. 67. - Când livrarea produsului sau prestarea serviciului se face ulterior plății unei sume de bani cu titlu de avans, operatorul economic este obligat să elibereze consumatorului, la plata acontului, un document fiscal conform legislației în vigoare sau, după caz, un contract scris și să respecte condițiile contractuale.

Art. 68. - Operatorii economici care, potrivit legislației în vigoare, sunt obligați să utilizeze aparate de marcat electronice fiscale vor elibera bonuri fiscale consumatorilor de produse/servicii, aceștia având obligația de a păstra aceste documente, cel puțin până la momentul părăsirii spațiului comercial respectiv.

CAPITOLUL VIII Publicitatea produselor și serviciilor

Art. 69. - Publicitatea trebuie să fie decentă, corectă și să fie elaborată în spiritul responsabilității sociale.

Art. 70. - Se interzice publicitatea care:

- a) este înșelătoare;
- b) este subliminală;
- c) prejudiază respectul pentru demnitatea umană și morala publică;
- d) include discriminări bazate pe rasă, sex, limbă, origine, origine socială, identitate etnică sau naționalitate;
- e) atentează la convingerile religioase sau politice;
- f) aduce prejudicii imaginii, onoarei, demnității și vieții particulare a persoanelor;
- g) exploatează superstițiile, credulitatea sau frica persoanelor;
- h) prejudiază securitatea persoanelor sau incită la violență;
- i) încurajează un comportament care prejudiază mediul înconjurător;
- j) favorizează comercializarea unor bunuri sau servicii, care sunt produse ori distribuite contrar prevederilor legale.

Art. 71. - Autorul, realizatorul de publicitate și reprezentantul legal al mijlocului de difuzare răspund solidar cu persoana care își face publicitate, în cazul încălcării prevederilor prezentului Cod, cu excepția cazurilor expres prevăzute prin lege și la care răspunderea este menționată în sarcina altei persoane.

Art. 72. - Dacă persoana care își face publicitate nu are sediul în România sau dacă nu poate fi identificată, răspunderea revine, după caz, reprezentantului său legal în România, autorului, realizatorului de publicitate sau reprezentantului legal al mijlocului de difuzare.

Art. 73. - Persoana care își face publicitate trebuie să fie în măsură să probeze exactitatea afirmațiilor, indicațiilor sau prezentărilor din anunțul publicitar și este obligată, la solicitarea instituțiilor și autorităților publice abilitate să aplice și să constate contravenții în domeniul publicității, să furnizeze documentele care să probeze exactitatea acestora. În cazul în care documentele nu sunt furnizate în termen de maximum 7 zile de la solicitare sau dacă sunt considerate insuficiente, afirmațiile din anunțul publicitar în cauză vor fi considerate inexacte.

Art. 74. - În scopul protejării vieții, sănătății, securității și informării corecte a consumatorilor, statul poate adopta măsuri de interzicere totală sau parțială a publicității anumitor produse.

CAPITOLUL

IX

Drepturile consumatorilor la încheierea contractelor

Art. 75. - Orice contract încheiat între comercianți și consumatori, pentru vânzarea de bunuri sau prestarea de servicii, va cuprinde clauze contractuale clare, fără echivoc, pentru înțelegerea cărora nu sunt necesare cunoștințe de specialitate.

Art. 76. - Orice informații privind pachetele de servicii turistice, prețurile acestora, contractele de credit pentru consum și toate celelalte condiții aplicabile contractului, comunicate de organizator sau de detailist consumatorului, trebuie să conțină indicații corecte și clare, care să nu permită interpretări echivoce ale acestora.

Art. 77. - În caz de dubiu asupra interpretării unor clauze contractuale, acestea vor fi interpretate în favoarea consumatorului.

Art. 78. - Se interzice comercianților stipularea de clauze abuzive în contractele încheiate cu consumatorii.

Art. 79. - O clauză contractuală care nu a fost negociată direct cu consumatorul va fi considerată abuzivă dacă, prin ea însăși sau împreună cu alte prevederi din contract, creează, în detrimentul consumatorului și contrar cerințelor bunei-credințe, un dezechilibru semnificativ între drepturile și obligațiile părților.

Art. 80. - O clauză contractuală va fi considerată ca nefiind negociată direct cu consumatorul, dacă aceasta a fost stabilită fără a da posibilitatea consumatorului să influențeze natura ei, cum ar fi contractele preformulate sau condițiile generale de vânzare practicate de comercianți pe piața produsului sau serviciului respectiv.

Art. 81. - Faptul că anumite aspecte ale clauzelor contractuale sau numai una dintre clauze a fost negociată direct cu consumatorul nu exclude aplicarea prevederilor legale pentru restul contractului, în cazul în care o evaluare globală a contractului evidențiază că acesta a fost prestabilit unilateral de comerciant. Dacă un comerciant pretinde că o clauză preformată a fost negociată direct cu consumatorul este de datoria lui să prezinte probe în acest sens.

Art. 82. - Contractul trebuie să stipuleze, cu caractere mari și în imediata vecinătate a locului rezervat pentru semnătura consumatorului, clauza expresă despre dreptul de denunțare unilaterală a contractului, după caz, precum și numele și adresa comerciantului față de care consumatorul poate să își exercite acest drept, conform dispozițiilor legale.

Art. 83. - Comerciantul este obligat să remită consumatorului un exemplar din contractul încheiat și să poată proba acest lucru în fața organelor de control.

Art. 84. - Dreptul consumatorului la denunțarea sau rezilierea contractului nu poate fi anulat sau restrâns de nicio clauză contractuală sau înțelegere între părți, în cazurile prevăzute de lege, aceasta

fiind considerată nulă de drept. Drepturile părților referitoare la o justă despăgubire nu vor fi afectate în cazul denunțării unilaterale.

CAPITOLUL X

Dispoziții finale și tranzitorii

Art. 85. - (1) Acțiunile de control și supraveghere a pieței sunt efectuate de personalul împuternicit al autorităților publice centrale și teritoriale cu atribuții în domeniul protecției consumatorilor, conform competențelor specifice.

(2) Personalul prevăzut la alin. (1) este autorizat să facă copii de pe materialele și documentele care au legătură cu obiectul controlului și care se află în posesia celor inspecțiați și să solicite referințe despre acestea, numai dacă s-a constatat o abatere de la lege.

(3) Personalul împuternicit este obligat să păstreze secretul profesional și să nu divulge unei terțe părți secretele comerciale sau alte informații confidențiale ori particulare obținute în timpul sau în legătură cu acțiunile de control, dacă nu li se cere să facă aceasta de către o autoritate judecătorească sau de către partea inspectată. În cazul în care personalul cu atribuții de control identifică sau suspectează neconformarea cu prevederile actelor normative din domeniul protecției consumatorilor în vigoare, acesta poate adopta și/sau dispune măsuri în conformitate cu prevederile acestora.

(4) Personalul prevăzut la alin. (1) poate solicita, pe timpul controlului, pentru aducerea la îndeplinire în bune condiții a atribuțiilor de serviciu, după caz, protecția personală și sprijinul organelor responsabile cu ordinea și liniștea publică care au obligația de a le sprijini în acest sens.

(5) Documentele care conțin date cu caracter personal, sesizările și reclamațiile petenților, precum și documentele de constatare și sancționare contravențională nu pot avea caracter public, cu excepția cazurilor expres prevăzute de lege sau a cazurilor în care părțile ale căror date sunt identificate sau identificabile consimt, în scris, acest fapt.

Art. 86. - (1) În vederea punerii la dispoziția operatorilor economici și a consumatorilor a unui instrument neutru de informare, ca rezultat al studiilor de piață și sondajelor de opinie, al strategiilor de distribuție, al practicilor comerciale, se va înființa Institutul Național al Consumului, în coordonarea Autorității Naționale pentru Protecția Consumatorilor.

(2) Organizarea și funcționarea Institutului Național al Consumului se stabilesc prin hotărâre a Guvernului.

(3) Institutul Național al Consumului este organizat ca instituție publică de interes național, cu personalitate juridică, sub forma unui centru de cercetare, informare și studii în domeniul consumului, ale cărui venituri sunt acordate din surse bugetare și extrabugetare, în condițiile legii.

(4) Activitățile Institutului Național al Consumului se realizează cu sprijinul reprezentanților administrației publice centrale, ai societății civile, ai personalităților în domeniu, ai organizațiilor patronale și ai organizațiilor neguvernamentale ale consumatorilor.

(5) Institutul Național al Consumului sprijină organizațiile neguvernamentale ale consumatorilor în activitatea de informare și educare a consumatorilor.

Art. 87. - Autoritatea cu atribuții de protecție a consumatorilor, în toate cazurile în care constată nerespectarea actelor normative în domeniul protecției consumatorilor, este împuternicită să aplice sancțiuni contravenționale principale, complementare, să dispună măsuri complementare și să sechestrze organele de cercetare penală în cazul în care faptele constatate pot constitui infracțiuni.

Art. 88. - (1) Reglementările legale în vigoare privind protecția consumatorului care nu sunt cuprinse în prezenta lege se vor prelua ca anexe ale acesteia.

(2) În termen de 18 luni de la data publicării prezentei legi în Monitorul Oficial al României, Partea I, Guvernul va prezenta Parlamentului, spre adoptare, proiectul de lege cu privire la anexele prevăzute la alin. (1).

Art. 89. - Prezenta lege intră în vigoare la data de 1 ianuarie 2007.

ANEXĂ

DEFINIȚII

În sensul legislației privind protecția consumatorilor, termenii și expresiile de mai jos se definesc astfel:

1. operator economic - persoana fizică sau juridică, autorizată, care în cadrul activității sale profesionale fabrică, importă, depozitează, transportă sau comercializează produse ori părți din acestea sau prestează servicii;
2. aliment nepreambalat - aliment vrac care nu este supus operațiunii de preambalare și care, pentru vânzare, este măsurat sau cântărit în prezența consumatorului;
3. autoritate cu atribuții de protecția consumatorilor - autoritatea administrației publice centrale și serviciile sale deconcentrate abilitate să constate și să aplice sancțiuni pentru nerespectarea dispozițiilor privind protecția consumatorilor;
4. calitate - ansamblul de proprietăți și caracteristici ale unui produs sau serviciu, care îi conferă aptitudinea de a satisface, conform destinației acestuia, necesitățile explicite sau implicite;
5. centru comercial - structura de vânzare cu suprafața medie sau mare în care se desfășoară activități de comercializare cu amănuntul de produse, servicii de piață și de alimentație publică, ce utilizează o infrastructură comună și utilități adecvate;
6. clauză abuzivă - clauza contractuală care nu a fost negociată direct cu consumatorul și care prin ea însăși sau împreună cu alte prevederi din contract creează, în detrimentul consumatorilor și contrar cerințelor bunei-credințe, un dezechilibru semnificativ între drepturile și obligațiile părților;
7. comerciant - persoana fizică sau juridică autorizată să desfășoare activitatea de comercializare a produselor și serviciilor de piață;
8. comerț ambulant - activitatea de comercializare cu amănuntul realizată prin trecere dintr-un loc în altul, în rulote mobile, standuri mobile, chioșcuri mobile sau în vehicule special amenajate;
9. comerț cu amănuntul/de detail - activitatea desfășurată de operatorii economici care vând produse, de regulă, direct consumatorilor pentru uzul personal al acestora;

10. comerț cu ridicata/de gros - activitatea desfășurată de operatorii economici care cumpără produse în cantități mari, în scopul revânzării acestora în cantități mai mici altor comercianți sau utilizatori profesionali și colectivi;
11. comerț de gros cash and carry/formă de comerț cu autoservire, pe bază de legitimație de acces - activitatea desfășurată de operatorii economici care vând mărfuri prin sistemul de autoservire către persoane juridice sau persoane fizice autorizate și asociații familiale autorizate conform legii, înregistrate în baza de date a vânzătorului, în scopul revânzării și/sau prelucrării, precum și al utilizării acestora ca produse consumabile;
12. comerț în zone publice - activitatea de comercializare a produselor și serviciilor, desfășurată permanent sau sezonier în piețe, târguri, oboare, pasaje publice, porturi, aeroporturi, gări, autogări, drumuri publice și străzi sau orice zonă de altă natură destinată folosinței publice;
13. consumator - orice persoană fizică sau grup de persoane fizice constituite în asociații, care acționează în scopuri din afara activității sale comerciale, industriale sau de producție, artizanale ori liberale;
14. contract încheiat cu consumatorii - contractele încheiate între comercianți și consumatori, inclusiv certificatele de garanție, bonurile de comandă, facturile, borderourile sau bonurile de livrare, biletele, tichetele care conțin stipulări sau referiri la condiții generale prestabilite;
15. data durabilității minimale - data stabilită de producător, până la care un produs alimentar își păstrează caracteristicile specifice în condiții de depozitare corespunzătoare; produsele pentru care se stabilește data durabilității minimale nu trebuie să fie periculoase nici după această dată;
16. declarație de conformitate - declarația făcută de către un producător sau un prestator, prin care acesta informează, pe propria răspundere, despre faptul că un produs sau un serviciu este conform cu un document tehnic normativ;
17. distribuitor - operatorul economic din lanțul de distribuție, a cărui activitate profesională nu afectează caracteristicile produsului;
18. durata medie de utilizare - intervalul de timp, stabilit în documentele tehnice normative sau declarat de către producător ori convenit între părți, în cadrul căruia produsele de folosință îndelungată trebuie să își mențină caracteristicile funcționale, dacă au fost respectate condițiile de transport, manipulare, depozitare și exploatare;
19. etichetă - orice material scris, imprimat, litografiat, gravat sau ilustrat, care conține elemente de identificare a produsului și care însoțește produsul sau este aderent la ambalajul acestuia;
20. exercițiu comercial - una sau mai multe activități de comercializare cu ridicata, cu amănuntul, de tip cash and carry, de alimentație publică, precum și a serviciilor desfășurate de un comerciant;
21. garanție - orice angajament asumat de vânzător sau producător față de consumator, fără solicitarea unor costuri suplimentare, de restituire a prețului plătit de consumator, de reparare sau de înlocuire a produsului cumpărat, în cazul în care acesta nu corespunde condițiilor enunțate în declarațiile referitoare la garanție sau în publicitatea aferentă;
22. ingredient alimentar - orice substanță, inclusiv aditivii, utilizată la producerea sau la prepararea unui aliment și care va fi conținută și de produsul finit ca atare sau într-o formă modificată;

23. lot - un ansamblu de unități de vânzare dintr-un aliment fabricat, prelucrat sau ambalat în condiții practic identice;

24. pachet de servicii turistice - combinația prestabilă a cel puțin două dintre următoarele trei grupe de servicii, cu condiția ca durata neîntreruptă a acestora să depășească 24 de ore sau să cuprindă o înnoptare, și anume, transport, cazare și alte servicii, fără legătură cu transportul sau cazarea sau care nu sunt accesorii ale acestora și care reprezintă o parte semnificativă a pachetului de servicii turistice, cum ar fi: alimentație, tratament balnear, agrement și altele asemenea;

25. pagubă - prejudiciul creat consumatorilor prin utilizarea unui produs periculos sau a unui produs cu defecte, precum și cel creat de servicii necorespunzătoare furnizate de prestator. Prejudiciul poate fi material, vătămarea integrității corporale sau a sănătății, precum și pierderea vieții;

26. practici comerciale abuzive - metode de vânzare restrictive sau condiționate care afectează interesele consumatorilor;

27. prestator - operatorul economic care furnizează servicii;

28. producător:

a) operatorul economic care fabrică un produs finit sau o componentă a unui produs;

b) operatorul economic care fabrică materie primă;

c) operatorul economic care își aplică denumirea, marca sau un alt semn distinctiv pe produs;

d) operatorul economic care recondiționează produsul;

e) operatorul economic sau distribuitorul care prin activitatea sa modifică caracteristicile produsului;

f) reprezentantul înregistrat în România al unui operator economic care nu are sediul în România sau, în cazul inexistenței acestuia, importatorul produsului;

g) operatorul economic care importă produse în vederea realizării ulterioare a unei operațiuni de vânzare, închiriere, leasing sau orice altă formă de distribuție specifică derulării afacerilor sale;

h) distribuitorul produsului importat, în cazul în care nu se cunoaște importatorul, chiar dacă producătorul este menționat;

i) distribuitorul produsului, în cazul în care importatorul nu poate fi identificat, dacă nu informează persoana prejudiciată în termen de 30 de zile de la cererea acesteia asupra identității importatorului;

29. produs - bun material a cărui destinație finală este consumul sau utilizarea individuală ori colectivă; sunt considerate produse energia electrică, energia termică, apa și gazele livrate pentru consumul individual;

30. produs cu defecte - produsul la care modul de prezentare, utilizarea previzibilă și data achiziționării nu oferă siguranță consumatorilor, producând pagube acestora;

31. produs de folosință îndelungată - produsul relativ complex, constituit din piese și subansambluri, proiectat și construit pentru a putea fi utilizat pe durata medie de utilizare și asupra căruia se pot efectua reparații sau activități de întreținere;

32. produs contrafăcut - orice bun, inclusiv ambalajul acestuia, la care se constată utilizarea fără autorizare a unei mărci care este identică cu o marcă legal înregistrată, sau produsul care nu poate fi diferențiat în aspectele sale esențiale de un produs de marcă, prin care se încalcă drepturile prevăzute de lege ale deținătorului legal al mărcii respective;

33. produs falsificat - produs la care se constată alterarea sub orice formă a elementelor de identificare a unei mărci, denumiri, sigle ori desen industrial legal înregistrate, de natură a induce în eroare asupra provenienței sale, la produse care nu au fost fabricate de deținătorul legal al mărcii ori împuternicit al acestuia, sau la care s-a constatat utilizarea mărcii legal înregistrate fără a exista acordul titularului;
34. produs folosit - produs folosit de un alt consumator, reparat și testat, corespunzător din punct de vedere tehnic și funcțional unui produs similar nou sau recondiționat, și care este un produs sigur;
35. produs periculos - produsul care nu poate fi definit ca produs sigur;
36. produs recondiționat - produs nou cu ambalaj deteriorat, aspect fizic exterior necorespunzător, mici defecte de fabricație, dar care este adus la parametrii tehnici de funcționare inițiali dați de producător prin remediere;
37. produs sigur - produsul care, folosit în condiții normale sau previzibile, nu prezintă riscuri sau care prezintă riscuri minime, ținând seama de întrebuințarea acestuia; riscul se consideră acceptabil și compatibil cu un grad înalt de protecție pentru siguranța și sănătatea consumatorilor, în funcție de următoarele aspecte:
- a) caracteristicile produsului, ale ambalării și ale instrucțiunilor de montaj și întreținere;
 - b) efectul asupra altor produse, împreună cu care acesta poate fi folosit;
 - c) modul de prezentare a produsului, etichetarea, instrucțiunile de folosire și orice alte indicații și informații furnizate de producător;
 - d) categoria de consumatori expusă riscului prin folosirea produsului;
38. punere pe piață - acțiunea de a face disponibil pentru prima dată, contra cost sau gratuit, un produs sau un serviciu în vederea distribuirii sau utilizării;
39. recondiționare - repararea unui produs nou anterior punerii pe piață, pentru a corespunde condițiilor enunțate în declarațiile de garanție sau în publicitatea aferentă, la specificațiile prevăzute în contractul de vânzare-cumpărare pentru un produs nou și nereparat;
40. reparare - aducerea produsului care nu corespunde condițiilor enunțate în declarațiile de garanție sau în publicitatea aferentă la specificațiile prevăzute în contractul de vânzare-cumpărare, alte documente, ori în alte dispoziții legale;
41. serviciu - activitatea, alta decât cea din care rezultă produse, efectuată în scopul satisfacerii unor necesități ale consumatorilor;
42. serviciu de alimentație publică - activitatea de pregătire, preparare, prezentare și servire a produselor și a băuturilor pentru consumul acestora în unități specializate sau la domiciliul/locul de muncă al consumatorilor;
43. serviciu financiar - unele servicii de natură bancară, credite, asigurări, pensii private, investiții sau plăți;
44. serviciu de piață - orice acțiune sau prestație care face obiectul vânzării-cumpărării pe piață și care nu are drept consecință transferul proprietății asupra unui bun corporal, efectuată în scopul satisfacerii unor necesități ale consumatorilor;
45. structura de vânzare - spațiul de desfășurare a unuia sau mai multor exerciții comerciale;
46. structura de vânzare cu suprafață mare - structura de vânzare având o suprafață de vânzare mai mare de 1.000 m²;

47. structura de vânzare cu suprafață medie - structura de vânzare având o suprafață de vânzare cuprinsă între 400-1.000 m² inclusiv;
48. structura de vânzare cu suprafață mică - structura de vânzare având o suprafață de vânzare de până la 400 m² inclusiv;
49. suprafața de vânzare - suprafața destinată accesului consumatorilor pentru achiziționarea produsului/serviciului, expunerii produselor oferite, plății acestora și circulației personalului angajat pentru derularea activității. Nu constituie suprafețe de vânzare cele destinate depozitării și păstrării mărfurilor;
50. suprafața de vânzare a unui centru comercial - suma suprafețelor de vânzare cu amănuntul de produse și servicii de piață și de alimentație publică cuprinse în aceasta;
51. termen de garanție - limita de timp, care curge de la data dobândirii produsului sau serviciului, până la care producătorul sau prestatorul își asumă responsabilitatea remedierii sau înlocuirii produsului ori serviciului achiziționat, pe cheltuiala sa, dacă deficiențele nu sunt imputabile consumatorilor;
52. termen de valabilitate - limita de timp, stabilită de producător, până la care un produs perisabil sau un produs care în scurt timp poate prezenta un pericol imediat pentru sănătatea consumatorilor își păstrează caracteristicile specifice, dacă au fost respectate condițiile de transport, manipulare, depozitare și păstrare; pentru produsele alimentare acesta reprezintă data limită de consum;
53. vânzător - distribuitorul care oferă produsul consumatorilor;
54. viciu ascuns - deficiența calitativă a unui produs livrat sau a unui serviciu prestat care nu a fost cunoscută și nici nu putea fi cunoscută de către consumator prin mijloacele obișnuite de verificare.

Parlamentul României

Legea nr. 365/2002 privind comerțul electronic

În vigoare de la 05 iulie 2002

Formă aplicabilă de la 29 noiembrie 2006

Consolidarea din data de **05 noiembrie 2019** are la bază [republicarea din Monitorul Oficial, Partea I](#) nr. 959 din 29 noiembrie 2006

Include modificările aduse prin următoarele acte: L [187/2012](#).

Ultimul amendament în 01 februarie 2014.

CAPITOLUL I Dispoziții generale

ARTICOLUL 1 Definiții În înțelesul prezentei legi, următorii termeni se definesc astfel:

1. serviciu al societății informaționale - orice serviciu care se efectuează utilizându-se mijloace electronice și prezintă următoarele caracteristici:
 - a) este efectuat în considerarea unui folos patrimonial, procurat ofertantului în mod obișnuit de către destinatar;
 - b) nu este necesar ca ofertantul și destinatarul să fie fizic prezenți simultan în același loc;
 - c) este efectuat prin transmiterea informației la cererea individuală a destinatarului;
2. mijloace electronice - echipamente electronice și rețele de cablu, fibră optică, radio, satelit și altele asemenea, utilizate pentru prelucrarea, stocarea sau transmiterea informației;
3. furnizor de servicii - orice persoană fizică sau juridică ce pune la dispoziție unui număr determinat sau nedeterminat de persoane un serviciu al societății informaționale;
4. furnizor de servicii stabilit într-un stat - un furnizor de servicii având un sediu stabil pe teritoriul unui stat și care desfășoară efectiv o activitate economică utilizând acel sediu stabil pe teritoriul unui stat, pentru o perioadă nedeterminată; stabilirea unui furnizor de servicii într-un stat nu este determinată în mod necesar de locul în care sunt amplasate mijloacele tehnice și tehnologice necesare furnizării serviciului;
5. domeniu - o zonă dintr-un sistem informatic, deținută ca atare de o persoană fizică sau juridică ori de un grup de persoane fizice sau juridice în scopul prelucrării, stocării ori transferului de date;
6. destinatar al serviciului sau destinatar - orice persoană fizică sau juridică ce utilizează, în scopuri comerciale, profesionale sau de altă natură, un serviciu al societății informaționale, în special în scopul căutării de informații sau al furnizării accesului la acestea;
7. consumator - orice persoană fizică ce acționează în alte scopuri decât cele ale activității sale comerciale sau profesionale;
8. comunicare comercială - orice formă de comunicare destinată să promoveze, direct sau indirect, produsele, serviciile, imaginea, numele ori denumirea, firma sau emblema unui comerciant ori membru

al unei profesii reglementate; nu constituie prin ele însele comunicări comerciale următoarele: informațiile permițând accesul direct la activitatea unei persoane fizice sau juridice, în special pe nume de domeniu sau o adresă de poștă electronică, comunicările legate de produsele, serviciile, imaginea, numele ori mărcile unei persoane fizice sau juridice, efectuate de un terț independent față de persoana în cauză, mai ales atunci când sunt realizate cu titlu gratuit;

9. legislație coordonată - prevederile în vigoare ale legilor naționale, aplicabile activităților ce fac obiectul serviciilor societății informaționale sau furnizorilor de servicii în privința:

a) condițiilor pe care trebuie să le îndeplinească furnizorii de servicii în vederea începerii acestor activități, precum sunt cele legate de eventualele calificări, autorizații sau notificări necesare;

b) condițiilor pe care trebuie să le îndeplinească furnizorii de servicii pentru desfășurarea acestor activități, precum sunt cele care privesc conduita acestora, calitatea sau conținutul serviciilor oferite, inclusiv în materie de publicitate și încheiere a contractelor, sau cele care privesc răspunderea furnizorilor;

10. nu constituie obiect al legislației coordonate:

a) cerințele aplicabile bunurilor ca atare și livrării acestora;

b) cerințele aplicabile serviciilor care nu sunt prestate prin mijloace electronice;

11. instrument de plată electronică - un instrument care permite titularului său să efectueze următoarele tipuri de operațiuni:

a) transferuri de fonduri, altele decât cele ordonate și executate de către instituții financiare;

b) retrageri de numerar, precum și încărcarea și descărcarea unui instrument de monedă electronică;

12. instrument de plată cu acces la distanță - instrument de plată electronică prin intermediul căruia titularul său poate să își acceseze fondurile deținute într-un cont la o instituție financiară și să autorizeze efectuarea unei plăți, utilizând un cod personal de identificare sau un alt mijloc de identificare similar;

13. instrument de monedă electronică - instrument de plată electronică reîncărcabil, altul decât instrumentul de plată cu acces la distanță, pe care unitățile de valoare sunt stocate electronic și care permite titularului său să efectueze tipurile de operațiuni menționate la pct. 11;

14. titular - persoană care deține un instrument de plată electronică pe baza unui contract încheiat cu un emitent, în condițiile prevăzute de lege;

15. date de identificare - orice informații care pot permite sau facilita efectuarea tipurilor de operațiuni menționate la pct. 11, precum un cod de identificare, numele sau denumirea, domiciliul ori sediul, numărul de telefon, fax, adresa de poștă electronică, numărul de înmatriculare sau alte mijloace similare de identificare, codul de înregistrare fiscală, codul numeric personal și altele asemenea;

16. activitate profesională reglementată - activitatea profesională pentru care accesul sau exercitarea în România este condiționată, direct sau indirect, în conformitate cu legislația română în vigoare, de deținerea unui document care să ateste nivelul de formare profesională.

ARTICOLUL 2 Scop și domeniu de aplicare (1) Prezenta lege are ca scop stabilirea condițiilor de furnizare a serviciilor societății informaționale, precum și prevederea ca infracțiuni a unor fapte săvârșite în legătură cu securitatea domeniilor utilizate în comerțul electronic, emiterea și utilizarea instrumentelor de plată electronică și cu utilizarea datelor de identificare în vederea efectuării de

operațiuni financiare, pentru asigurarea unui cadru favorabil liberei circulații și dezvoltării în condiții de securitate a acestor servicii.

(2) Nu constituie servicii ale societății informaționale, în sensul prezentei legi, activitățile care nu întrunesc elementele definiției prevăzute la art. 1 [pct. 1](#), în special următoarele:

- a) oferta de servicii care necesită prezența fizică a furnizorului și a destinatarului, chiar dacă prestarea serviciilor respective implică utilizarea de echipamente electronice;
- b) oferta de servicii care presupun manipularea unor bunuri corporale de către destinatar, chiar dacă prestarea serviciilor respective implică utilizarea de echipamente electronice;
- c) oferta de bunuri sau servicii care nu este prezentată destinatarului prin transmiterea informației la cererea individuală a acestuia și care este destinată recepției simultane de către un număr nelimitat de persoane (punct-multipunct);
- d) activități care se efectuează prin intermediul serviciilor de telefonie vocală, telefax, telex, servicii de radiodifuziune și televiziune, inclusiv serviciile de teletext;
- e) serviciile de telefonie vocală, telefax sau telex;
- f) schimbul de informații prin poșta electronică sau prin alte mijloace de comunicare individuală echivalente, între persoane care acționează în scopuri străine activității lor comerciale sau profesionale;
- g) relația contractuală dintre un angajat și angajatorul său.

(3) Prezenta lege nu se aplică următoarelor activități:

- a) activitatea notarilor publici, în măsura în care aceasta presupune o participare directă și specifică la exercitarea prerogativelor autorității publice;
- b) activitățile de reprezentare juridică în fața organelor de jurisdicție și de urmărire penală;
- c) jocurile de noroc cu câștiguri în bani, loteriile și pariurile.

(4) Dispozițiile prezentei legi se completează cu:

- a) dispozițiile legale în materie fiscală;
- b) dispozițiile legale care reglementează protecția persoanelor în privința prelucrării datelor cu caracter personal și libera circulație a acestor date, precum și cele care reglementează prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor;
- c) prevederile Legii concurenței [nr. 21/1996](#), republicată.

(5) În măsura în care nu conține dispoziții derogatorii, prezenta lege se completează cu dispozițiile legale privind încheierea, validitatea și efectele actelor juridice, cu celelalte prevederi legale care au ca scop protecția consumatorilor și a sănătății publice.

ARTICOLUL 3 Aplicarea legii române în cazul serviciilor societății informaționale (1) Prezenta lege se aplică furnizorilor de servicii stabiliți în România și serviciilor oferite de aceștia.

(2) De la data intrării în vigoare a prezentei legi serviciile societății informaționale sunt supuse:

- a) exclusiv prevederilor în vigoare ale legilor române care fac parte din legislația coordonată, în cazul în care sunt oferite de furnizori de servicii stabiliți în România;
- b) exclusiv prevederilor în vigoare ale legilor statului în cauză care fac parte din legislația coordonată, în cazul în care sunt oferite de furnizori de servicii stabiliți într-un stat membru al Uniunii Europene.

(3) Libera circulație a serviciilor societății informaționale oferite de un furnizor stabilit într-un stat membru al Uniunii Europene nu poate fi restrânsă în România prin aplicarea unor prevederi legale care fac parte din legislația coordonată.

(4) Alin. (2) și (3) nu se aplică în următoarele domenii:

- a) dreptul de proprietate intelectuală și dreptul de proprietate industrială;
- b) emisiunea de monedă electronică, în condițiile prevăzute în normele metodologice de aplicare a prezentei legi;
- c) publicitatea pentru organisme de investiții colective în valori mobiliare;
- d) activitățile de asigurare, în condițiile prevăzute în normele metodologice de aplicare a prezentei legi;
- e) libertatea părților de a alege legea aplicabilă contractului, când părțile au acest drept;
- f) obligații rezultate din contractele încheiate cu consumatorii;
- g) cerințele de formă prevăzute pentru validitatea actelor juridice prin care se creează, se modifică, se sting sau se transmit drepturi reale asupra unor bunuri imobile situate pe teritoriul României.

(5) Autoritățile publice pot lua măsuri derogatorii de la prevederile alin. (3) numai în următoarele condiții:

- a) măsura este necesară pentru motive de ordine publică, desfășurarea instrucției penale, protecția minorilor, lupta împotriva oricărei forme de incitare la ură din rațiune de rasă, sex, religie sau naționalitate, atingeri aduse demnității umane, protecția sănătății publice, apărarea și siguranța națională, protecția consumatorilor, inclusiv a investitorilor;
- b) măsura vizează un serviciu al societății informaționale care aduce atingere uneia dintre valorile enumerate la lit. a) sau prezintă un risc serios și grav la adresa acestor valori;
- c) măsura este proporțională cu scopul urmărit;
- d) sunt respectate procedurile de colaborare, consultare sau informare prevăzute în normele metodologice de aplicare a prezentei legi.

CAPITOLUL II

Furnizarea serviciilor societății informaționale

ARTICOLUL 4 Principiile furnizării serviciilor societății informaționale (1) Furnizarea de servicii ale societății informaționale de către persoanele fizice sau juridice nu este supusă niciunei autorizări prealabile și se desfășoară în concordanță cu principiile concurenței libere și loiale, cu respectarea dispozițiilor legale în vigoare.

(2) Prevederile alin. (1) nu aduc atingere dispozițiilor legale care impun autorizarea prealabilă în vederea desfășurării unor activități de către persoanele fizice sau juridice, dacă dispozițiile în cauză nu vizează în mod expres și exclusiv serviciile societății informaționale sau furnizorii de servicii, în înțelesul prezentei legi.

(3) Furnizarea de servicii ale societății informaționale de către furnizorii de servicii stabiliți în statele membre ale Uniunii Europene se face, până la momentul aderării României la Uniunea Europeană, în condițiile prevăzute în Acordul european instituind o asociere între România, pe de o parte, și Comunitățile Europene și statele membre ale acestora, pe de altă parte.

(4) Furnizarea de servicii ale societății informaționale de către furnizorii de servicii stabiliți în alte state se face în condițiile acordurilor bilaterale încheiate cu statele respective, la care România este parte.

ARTICOLUL 5 Informații generale (1) Furnizorul de servicii are obligația de a pune la dispoziție destinatarilor și autorităților publice mijloace care să permită accesul facil, direct, permanent și gratuit cel puțin la următoarele informații:

- a) numele sau denumirea furnizorului de servicii;
- b) domiciliul sau sediul furnizorului de servicii;
- c) numerele de telefon, fax, adresa de poștă electronică și orice alte date necesare contactării furnizorului de servicii în mod direct și efectiv;
- d) numărul de înmatriculare sau alte mijloace similare de identificare, în cazul în care furnizorul de servicii este înscris în registrul comerțului sau în alt registru public similar;
- e) codul de înregistrare fiscală;
- f) datele de identificare ale autorității competente, în cazul în care activitatea furnizorului de servicii este supusă unui regim de autorizare;
- g) titlul profesional și statul în care a fost acordat, corpul profesional sau orice alt organism similar din care face parte, indicarea reglementărilor aplicabile profesiei respective în statul în care furnizorul de servicii este stabilit, precum și a mijloacelor de acces la acestea, în cazul în care furnizorul de servicii desfășoară o activitate profesională reglementată;
- h) tarifele aferente serviciilor oferite, care trebuie indicate cu respectarea normelor privind comercializarea produselor și serviciilor de piață, cu precizarea scutirii, includerii sau neincluserii taxei pe valoarea adăugată, precum și a cuantumului acesteia;
- i) includerea sau neincluderea în preț a cheltuielilor de livrare, precum și valoarea acestora, dacă este cazul;
- j) orice alte informații pe care furnizorul de servicii este obligat să le pună la dispoziție destinatarilor, în conformitate cu prevederile legale în vigoare.

(2) Obligația prevăzută la alin. (1) se consideră îndeplinită în cazul în care furnizorul unui serviciu afișează aceste informații într-o formă clară, vizibil și permanent, în interiorul paginii de web prin intermediul căreia este oferit serviciul respectiv, în condițiile menționate la alin. (1).

ARTICOLUL 6 Comunicările comerciale (1) Efectuarea de comunicări comerciale prin poșta electronică este interzisă, cu excepția cazului în care destinatarul și-a exprimat în prealabil consimțământul expres pentru a primi asemenea comunicări.

(2) Comunicările comerciale care constituie un serviciu al societății informaționale sau o parte a acestuia, în măsura în care sunt permise, trebuie să respecte cel puțin următoarele condiții:

- a) să fie clar identificabile ca atare;
- b) persoana fizică sau juridică în numele căreia sunt făcute să fie clar identificată;
- c) ofertele promoționale, precum reducerile, premiile și cadourile, să fie clar identificabile, iar condițiile care trebuie îndeplinite pentru obținerea lor să fie ușor accesibile și clar prezentate;
- d) competițiile și jocurile promoționale să fie clar identificabile ca atare, iar condițiile de participare să fie ușor accesibile și clar prezentate;
- e) orice alte condiții impuse prin dispozițiile legale în vigoare.

(3) Comunicările comerciale care constituie un serviciu al societății informaționale sau o parte a acestuia, atunci când acest serviciu este furnizat de un membru al unei profesii reglementate, sunt permise sub condiția respectării dispozițiilor legale și a reglementărilor aplicabile profesiei respective, care privesc, în special, independența, demnitatea și onoarea profesiei, secretul profesional și corectitudinea față de clienți și față de ceilalți membri ai profesiei.

(4) Furnizorii de servicii ale societății informaționale care efectuează comunicări comerciale au obligația de a respecta prevederile alin. (1)-(3).

CAPITOLUL III

Contractele încheiate prin mijloace electronice

ARTICOLUL 7 Validitatea, efectele juridice și proba contractelor încheiate prin mijloace electronice

(1) Contractele încheiate prin mijloace electronice produc toate efectele pe care legea le recunoaște contractelor, atunci când sunt întrunite condițiile cerute de lege pentru validitatea acestora.

(2) Pentru validitatea contractelor încheiate prin mijloace electronice nu este necesar consimțământul prealabil al părților asupra utilizării mijloacelor electronice.

(3) Proba încheierii contractelor prin mijloace electronice și a obligațiilor care rezultă din aceste contracte este supusă dispozițiilor dreptului comun în materie de probă și prevederilor Legii [nr. 455/2001](#) privind semnătura electronică.

ARTICOLUL 8 Informarea destinatarilor (1) Furnizorul de servicii este obligat să pună la dispoziție destinatarului, înainte ca destinatarul să trimită oferta de a contracta sau acceptarea ofertei ferme de a contracta făcute de furnizorul de servicii, cel puțin următoarele informații, care trebuie să fie exprimate în mod clar, neechivoc și într-un limbaj accesibil:

a) etapele tehnice care trebuie urmate pentru a încheia contractul;

b) dacă contractul, odată încheiat, este stocat sau nu de către furnizorul de servicii și dacă este accesibil sau nu;

c) mijloacele tehnice pe care furnizorul de servicii le pune la dispoziție destinatarului pentru identificarea și corectarea erorilor survenite cu ocazia introducerii datelor;

d) limba în care se poate încheia contractul;

e) codurile de conduită relevante la care furnizorul de servicii subscrie, precum și informații despre modul în care aceste coduri pot fi consultate prin mijloace electronice;

f) orice alte condiții impuse prin dispozițiile legale în vigoare.

(2) Furnizorul de servicii are obligația să ofere destinatarului posibilitatea de a utiliza un procedeu tehnic adecvat, eficace și accesibil, care să permită identificarea și corectarea erorilor survenite cu ocazia introducerii datelor, anterior trimiterii ofertei sau acceptării acesteia.

(3) Furnizorul de servicii poate deroga de la dispozițiile alin. (1) și (2) numai în situația în care a convenit altfel cu destinatarul, cu condiția că niciuna dintre părți să nu aibă calitatea de consumator.

(4) Clauzele și condițiile generale ale contractului propus trebuie puse la dispoziție destinatarului într-un mod care să îi permită acestuia să le stocheze și să le reproducă.

(5) Prevederile alin. (1)-(3) nu se aplică în privința contractelor încheiate exclusiv prin poștă electronică sau prin alte mijloace de comunicare individuală echivalente.

ARTICOLUL 9 Încheierea contractului prin mijloace electronice (1) Dacă părțile nu au convenit altfel, contractul se consideră încheiat în momentul în care acceptarea ofertei de a contracta a ajuns la cunoștința ofertantului.

(2) Contractul care, prin natura sa ori la cererea beneficiarului, impune o executare imediată a prestației caracteristice se consideră încheiat în momentul în care debitorul acesteia a început executarea, în afară de cazul în care ofertantul a cerut ca în prealabil să i se comunice acceptarea. În acest ultim caz se aplică prevederile alin. (1).

(3) În cazul în care destinatarul trimite prin mijloace electronice oferta de a contracta sau acceptarea ofertei ferme de a contracta făcute de furnizorul de servicii, furnizorul de servicii are obligația de a confirma primirea ofertei sau, după caz, a acceptării acesteia, în unul dintre următoarele moduri:

a) trimiterea unei dovezi de primire prin poștă electronică sau printr-un alt mijloc de comunicare individuală echivalent, la adresa indicată de către destinatar, fără întârziere;

b) confirmarea primirii ofertei sau a acceptării ofertei, printr-un mijloc echivalent celui utilizat pentru trimiterea ofertei sau a acceptării ofertei, de îndată ce oferta sau acceptarea a fost primită de furnizorul de servicii, cu condiția ca această confirmare să poată fi stocată și reprodusă de către destinatar.

(4) Oferta sau acceptarea ofertei, precum și confirmarea primirii ofertei sau a acceptării ofertei, efectuate în unul dintre modurile prevăzute la alin. (3), se consideră primite atunci când părțile cărora le sunt adresate pot să le acceseze.

(5) Prevederile alin. (3) nu se aplică în privința contractelor încheiate exclusiv prin poștă electronică sau prin alte mijloace de comunicare individuală echivalente.

ARTICOLUL 10 Condiții privind păstrarea sau prezentarea informației (1) Acolo unde legea impune ca informația să fie prezentată sau păstrată în forma sa originală, această cerință este îndeplinită dacă sunt întrunite în mod cumulativ următoarele condiții:

a) există garanția integrității informației, asigurată prin respectarea standardelor naționale în domeniu, din momentul în care a fost generată;

b) mesajul este semnat utilizându-se semnătura electronică extinsă a emitentului;

c) informația poate fi imediat furnizată și prezentată la cerere.

(2) Destinatarul comerciant acționează pe riscul propriu, dacă a știut sau ar fi trebuit să știe, în concordanță cu practicile comerciale curente sau ca urmare a folosirii procedurilor convenite expres cu emitentul, că informația conținută într-un mesaj electronic a fost alterată în timpul transmiterii sau prelucrării sale.

CAPITOLUL IV

Răspunderea furnizorilor de servicii

ARTICOLUL 11 Principii generale (1) Furnizorii de servicii sunt supuși dispozițiilor legale referitoare la răspunderea civilă, penală și contravențională, în măsura în care prin prezenta lege nu se dispune altfel.

(2) Furnizorii de servicii răspund pentru informația furnizată de ei înșiși sau pe seama lor.

(3) Furnizorii de servicii nu răspund pentru informația transmisă, stocată sau la care facilitează accesul, în condițiile prevăzute la [art. 12-15](#).

ARTICOLUL 12 Intermedierea prin simpla transmitere (1) Dacă un serviciu al societății informaționale constă în transmiterea într-o rețea de comunicații a informației furnizate de un destinatar al serviciului respectiv sau în asigurarea accesului la o rețea de comunicații, furnizorul aceluși serviciu nu răspunde pentru informația transmisă dacă sunt îndeplinite cumulativ următoarele condiții:

- a) transmiterea nu a fost inițiată de furnizorul de servicii;
- b) alegerea persoanei care recepționează informația transmisă nu aparține furnizorului de servicii;
- c) conținutul informației transmise nu a fost influențat în niciun fel de către furnizorul de servicii, în sensul că nu i se poate atribui nici selecția și nicio eventuală modificare a acestei informații.

(2) Transmiterea informației și asigurarea accesului, menționate la alin. (1), includ și stocarea automată, intermediară și temporară a informației transmise, în măsura în care această operație are loc exclusiv în scopul ca informația respectivă să tranziteze rețeaua de comunicații și cu condiția ca informația să nu fie stocată pentru o perioadă care depășește în mod nejustificat durata necesară transmiterii ei.

ARTICOLUL 13 Stocarea temporară a informației, stocarea-caching Dacă un serviciu al societății informaționale constă în transmiterea într-o rețea de comunicații a informației furnizate de un destinatar al serviciului respectiv, furnizorul aceluși serviciu nu răspunde pentru stocarea automată, intermediară și temporară a informației transmise, în măsura în care această operație are loc exclusiv în scopul de a face mai eficientă transmiterea informației către alți destinatari, la cererea acestora, dacă sunt îndeplinite cumulativ următoarele condiții:

- a) furnizorul de servicii nu aduce modificări informației transmise;
- b) furnizorul de servicii îndeplinește condițiile legale privind accesul la informația respectivă;
- c) furnizorul de servicii respectă regulile sau uzanțele referitoare la actualizarea informației, astfel cum acestea sunt larg recunoscute și aplicate în industrie;
- d) furnizorul de servicii nu împiedică utilizarea legală de către orice persoană a tehnologiilor larg recunoscute și aplicate în industrie, în vederea obținerii de date despre natura sau utilizarea informației;
- e) furnizorul de servicii acționează rapid în vederea eliminării informației pe care a stocat-o sau în vederea blocării accesului la aceasta, din momentul în care a cunoscut efectiv faptul că informația transmisă inițial a fost eliminată din rețeaua de comunicații ori că accesul la ea a fost blocat sau faptul că eliminarea ori blocarea accesului a avut loc prin efectul deciziei unei autorități publice.

ARTICOLUL 14 Stocarea permanentă a informației, stocarea-hosting (1) Dacă un serviciu al societății informaționale constă în stocarea informației furnizate de un destinatar al serviciului respectiv, furnizorul aceluși serviciu nu răspunde pentru informația stocată la cererea unui destinatar, dacă este îndeplinită oricare dintre următoarele condiții:

- a) furnizorul de servicii nu are cunoștință despre faptul că activitatea sau informația stocată este nelegală și, în ceea ce privește acțiunile în daune, nu are cunoștință despre fapte sau circumstanțe din care să rezulte că activitatea sau informația în cauză ar putea vătăma drepturile unui terț;
- b) având cunoștință despre faptul că activitatea sau informația respectivă este nelegală ori despre fapte sau circumstanțe din care să rezulte că activitatea ori informația în cauză ar putea vătăma

drepturile unui terț, furnizorul de servicii acționează rapid în vederea eliminării sau a blocării accesului la aceasta.

(2) Prevederile alin. (1) nu se aplică în situația în care destinatarul acționează sub autoritatea sau controlul furnizorului de servicii.

(3) Prevederile acestui articol nu vor afecta posibilitatea autorității judiciare sau administrative de a cere furnizorului de servicii să înceteze ori să prevină violarea datelor și, de asemenea, nu pot să afecteze posibilitatea stabilirii unor proceduri guvernamentale de limitare sau întrerupere a accesului la informații.

ARTICOLUL 15 Instrumente de căutare a informațiilor și legături cu alte pagini de web (1) Furnizorul unui serviciu al societății informaționale care facilitează accesul la informația furnizată de alți furnizori de servicii sau de destinatarii serviciilor oferite de alți furnizori, prin punerea la dispoziție destinatarilor serviciului său a unor instrumente de căutare a informațiilor sau a unor legături cu alte pagini de web, nu răspunde pentru informația în cauză, dacă este îndeplinită oricare dintre următoarele condiții:

a) furnizorul nu are cunoștință despre faptul că activitatea sau informația la care facilitează accesul este nelegală și, în ceea ce privește acțiunile în daune, nu are cunoștință despre fapte sau circumstanțe din care să rezulte că activitatea ori informația în cauză ar putea prejudicia drepturile unui terț;

b) având cunoștință despre faptul că activitatea sau informația respectivă este nelegală ori despre fapte sau circumstanțe din care să rezulte că activitatea sau informația în cauză ar putea vătăma drepturile unui terț, furnizorul acționează rapid în vederea eliminării posibilității de acces oferite sau a blocării utilizării acesteia.

(2) Furnizorul de servicii răspunde pentru informația în cauză atunci când caracterul nelegal al acesteia a fost constatat printr-o decizie a unei autorități publice.

(3) Prevederile alin. (1) nu se aplică în situația în care destinatarul acționează din ordinul sau sub comanda furnizorului de servicii.

CAPITOLUL V

Supraveghere și control

ARTICOLUL 16 Obligațiile furnizorilor de servicii (1) Furnizorii de servicii sunt obligați să informeze de îndată autoritățile publice competente despre activitățile cu aparență nelegală desfășurate de destinatarii serviciilor lor sau despre informațiile cu aparență nelegală furnizate de aceștia.

(2) Furnizorii de servicii sunt obligați să comunice de îndată autorităților prevăzute la alin. (1), la cererea acestora, informații care să permită identificarea destinatarilor serviciilor lor, cu care acești furnizori au încheiat contracte privind stocarea permanentă a informației.

(3) Furnizorii de servicii sunt obligați să întrerupă, temporar sau permanent, transmiterea într-o rețea de comunicații ori stocarea informației furnizate de un destinatar al serviciului respectiv, în special prin eliminarea informației sau blocarea accesului la aceasta, accesul la o rețea de comunicații ori prestarea oricărui alt serviciu al societății informaționale, dacă aceste măsuri au fost dispuse de autoritatea publică definită la art. 17 [alin. \(2\)](#); această autoritate publică poate acționa din oficiu sau ca urmare a plângerii ori sesizării unei persoane interesate.

(4) Plângerea prevăzută la alin. (3) poate fi făcută de către orice persoană care se consideră prejudiciată prin conținutul informației în cauză. Plângerea sau sesizarea se întocmește în formă scrisă, cu arătarea motivelor pe care se întemeiază, și va fi în mod obligatoriu datată și semnată. Plângerea nu poate fi înaintată dacă o cerere în justiție, având același obiect și aceleași părți, a fost anterior introdusă.

(5) Decizia autorității trebuie motivată și se comunică părților interesate în termen de 30 de zile de la data primirii plângerii sau a sesizării ori, dacă autoritatea a acționat din oficiu, în termen de 15 zile de la data la care a fost emisă.

(6) Împotriva unei decizii luate potrivit prevederilor alin. (3) persoana interesată poate formula contestație în termen de 15 zile de la comunicare, sub sancțiunea decăderii, la instanța de contencios administrativ competentă. Cererea se judecă de urgență, cu citarea părților. Sentința este definitivă.

ARTICOLUL 17 Autorități competente (1) Autoritatea de reglementare în comunicații și tehnologia informației, denumită în continuare Autoritatea, este competentă să supravegheze și să controleze respectarea de către furnizorii de servicii a prevederilor prezentei legi și a normelor metodologice de aplicare a acesteia, să constate contravențiile și să aplice sancțiunile prevăzute la [art. 22](#).

(2) Fără a aduce atingere prevederilor alin. (1), prin autorități publice, în sensul art. 3 [alin. \(5\)](#), [art. 5](#), [13](#), art. 15 [alin. \(2\)](#), art. 16 [alin. \(1\)](#) și [\(3\)](#) și art. 23 [alin. \(2\)](#), se înțelege acele autorități ale administrației publice sau, acolo unde este cazul, instanțe de judecată a căror competență în materia respectivă este stabilită prin dispozițiile legale în vigoare, aplicabile în fiecare caz.

(3) Autoritatea poate solicita furnizorilor de servicii orice informații necesare în vederea exercitării atribuțiilor sale, menționând baza legală și scopul solicitării, și poate stabili termene până la care aceste informații să îi fie furnizate, sub sancțiunea prevăzută de prezenta lege.

(4) În vederea descoperirii și investigării încălcărilor prevederilor prezentei legi și ale normelor sale de aplicare, Autoritatea acționează prin personalul de control împuternicit în acest scop.

(5) În exercitarea atribuțiilor de investigare personalul de control împuternicit în acest scop al Autorității sau al persoanei juridice prevăzute la alin. (12) poate solicita furnizorilor de servicii informațiile care îi sunt necesare, menționând baza legală și scopul solicitării, și poate stabili termene până la care aceste informații să îi fie furnizate, sub sancțiunea prevăzută de prezenta lege.

(6) Autoritatea dispune efectuarea de investigații, în condițiile prezentei legi, din oficiu sau la primirea unei plângeri ori sesizări din partea oricărei persoane.

(7) Personalul de control împuternicit în acest scop al Autorității sau al persoanei juridice prevăzute la alin. (12) poate să solicite declarații sau orice documente necesare pentru îndeplinirea misiunii, să sigileze, să ridice orice registre, acte financiar-contabile și comerciale sau alte evidențe, eliberând persoanei supuse investigației copii de pe originale, ori să obțină copii, lăsându-i acesteia originalele; de asemenea, este autorizat să facă inspecții inopinate, al căror rezultat va fi consemnat într-un proces-verbal de constatare, și să primească, la convocare sau la fața locului, informații și justificări.

(8) Organele administrației publice centrale și locale, precum și oricare alte instituții și autorități publice sunt obligate să permită personalului de control împuternicit în acest scop al Autorității sau, după caz, al persoanei juridice prevăzute la alin. (12) accesul la documentele, datele și informațiile deținute de acestea, în măsura în care sunt necesare îndeplinirii misiunii legale a Autorității, fără a se putea opune caracterul de secret de stat sau secret de serviciu al unor asemenea documente, date și informații.

(9) Personalul de control împuternicit în acest scop, primind acces la documentele, datele și informațiile menționate la alin. (8), este ținut la observarea strictă a caracterului de secret de stat sau secret de serviciu, atribuit legal respectivelor documente, date și informații.

(10) Autoritatea sesizează organele de urmărire penală ori de câte ori constată încălcări ale legii penale.

(11) Autoritatea informează furnizorii de servicii, destinatarii, statele membre ale Uniunii Europene și Comisia Europeană cu privire la toate aspectele legate de aplicarea prevederilor prezentei legi și cooperează cu autoritățile competente din alte state în vederea exercitării eficiente a supravegherii și controlului asupra activității furnizorilor de servicii.

(12) Autoritatea poate delega exercitarea atribuțiilor prevăzute în prezentul articol unei alte persoane juridice de drept public, cu atribuții de supraveghere și control în domeniul telecomunicațiilor.

(13) Pentru scopurile aplicării prezentei legi, până la înființarea Autorității atribuțiile acesteia sunt îndeplinite de Ministerul Comunicațiilor și Tehnologiei Informației.

ARTICOLUL 18 Coduri de conduită (1) Asociațiile și organizațiile neguvernamentale cu caracter profesional ori comercial sau cele constituite în scopul protecției consumatorilor, a minorilor ori a persoanelor cu handicap își pot elabora propriile coduri de conduită sau coduri comune cu Autoritatea și Ministerul Justiției, în vederea aplicării corespunzătoare a prevederilor prezentei legi.

(2) Autoritatea și Ministerul Justiției vor urmări includerea în codurile de conduită prevăzute la alin. (1) în special a unor prevederi referitoare la:

a) soluționarea litigiilor pe cale extrajudiciară;

b) întreruperea, temporară sau permanentă, a transmiterii într-o rețea de comunicații sau a stocării informației furnizate de un destinatar al serviciului, în special prin eliminarea informației ori blocarea accesului la aceasta, a accesului la o rețea de comunicații sau a prestării oricărui alt serviciu al societății informaționale;

c) protecția destinatarilor cu privire la efectuarea comunicărilor comerciale;

d) protecția minorilor și a demnității umane.

(3) Autoritatea și Ministerul Justiției susțin:

a) traducerea codurilor de conduită în limbi de circulație internațională;

b) facilitarea accesului la codurile de conduită prin mijloace electronice;

c) popularizarea codurilor de conduită la nivel național și transmiterea acestora, precum și a evaluărilor privind aplicarea și impactul lor practic către statele membre ale Uniunii Europene și către Comisia Europeană.

CAPITOLUL VI

Soluționarea litigiilor

ARTICOLUL 19 Acțiuni în justiție (1) Persoanele care au calitate procesuală activă, potrivit prevederilor alin. (2), pot solicita instanței obligarea pârâtului la încetarea oricărei acțiuni sau abțineri contrare prevederilor prezentei legi, interzicerea reluării ei în viitor și obligarea pârâtului la despăgubiri pentru prejudiciul suferit.

(2) Au calitate procesuală activă pentru introducerea acțiunii prevăzute la alin. (1):

- a) persoanele fizice și juridice ce se pretind titulare ale unui drept subiectiv prevăzut de prezenta lege sau ale unui interes care nu se poate realiza decât pe calea justiției;
- b) asociațiile și organizațiile neguvernamentale prevăzute la art. 18 [alin. \(1\)](#);
- c) Autoritatea Națională pentru Protecția Consumatorilor, oficiile pentru protecția consumatorilor județene și Oficiul pentru protecția consumatorilor al municipiului București;
- d) entitățile constituite în scopul protecției consumatorilor în statele membre ale Uniunii Europene, în condițiile prevăzute de normele metodologice de aplicare a prezentei legi.

(3) Acțiunea prevăzută la alin. (1) se prescrie în termen de un an de la data acțiunii sau a abținerii care a justificat introducerea ei.

(4) Persoanele care au calitate procesuală activă, potrivit prevederilor alin. (2), pot solicita instanței, pe cale de ordonanță președințială, încetarea oricărei acțiuni sau abțineri contrare prevederilor prezentei legi, în condițiile prevăzute de Codul de procedură civilă.

ARTICOLUL 20 Soluționarea litigiilor pe cale extrajudiciară (1) Furnizorii de servicii și destinatarii pot supune litigiile născute între ei arbitrajului, în condițiile prevăzute de lege, precum și celorlalte căi extrajudiciare de soluționare a litigiilor, prevăzute de codurile de conduită elaborate potrivit [art. 18](#).

(2) Utilizarea mijloacelor electronice în cadrul soluționării litigiilor pe cale extrajudiciară este posibilă în condițiile prevăzute de lege.

CAPITOLUL VII

Sanțiuni civile și contravenționale

ARTICOLUL 21 Nulitatea relativă a contractelor privind servicii ale societății informaționale Orice contract privind furnizarea de servicii ale societății informaționale este anulabil la cererea destinatarului, dacă a fost încheiat cu un furnizor de servicii care:

- a) nu a pus la dispoziție destinatarului, în condițiile prevăzute de lege, informațiile prevăzute la art. 5 [lit. a\) -i](#)), ori nu a furnizat toate aceste informații, sau a furnizat informații inexacte;
- b) nu a pus la dispoziție destinatarului, în condițiile prevăzute de lege, informațiile menționate la art. 8 alin. (1) [lit. a\) -e](#)), ori nu a furnizat toate aceste informații, sau a furnizat informații inexacte, dacă nu sunt aplicabile prevederile art. 8 [alin. \(3\)](#) sau [\(5\)](#);
- c) a încălcat obligația prevăzută la art. 8 [alin. \(2\)](#), dacă nu sunt aplicabile prevederile art. 8 [alin. \(3\)](#) sau [\(5\)](#);
- d) a încălcat obligația prevăzută la art. 8 [alin. \(4\)](#).

ARTICOLUL 22 Contravenții Constituie contravenție, dacă nu este săvârșită în astfel de condiții încât, potrivit legii penale, să constituie infracțiune, și se sancționează cu amendă de la 1.000 lei la 50.000 lei fapta furnizorului de servicii care:

- a) efectuează comunicări comerciale încălcând condițiile stabilite la art. 6 [alin. \(1\)](#) și alin. (2) [lit. a\) -d](#));
- b) nu pune la dispoziție destinatarii și autorităților publice, în condițiile prevăzute de lege, informațiile prevăzute la art. 5 [lit. a\) -i](#)), ori nu furnizează toate aceste informații, sau furnizează informații inexacte;

c) nu pune la dispoziție destinatarului, în condițiile prevăzute de lege, informațiile prevăzute la art. 8 alin. (1) [lit. a](#) -e), ori nu furnizează toate aceste informații, sau furnizează informații inexacte, dacă nu sunt aplicabile prevederile art. 8 [alin. \(3\)](#) sau [\(5\)](#);

d) încalcă obligația prevăzută la art. 8 [alin. \(2\)](#), dacă nu sunt aplicabile prevederile art. 8 [alin. \(3\)](#) sau [\(5\)](#);

e) încalcă obligația prevăzută la art. 8 [alin. \(4\)](#);

f) încalcă obligația prevăzută la art. 9 [alin. \(3\)](#);

g) încalcă obligațiile prevăzute la art. 16 [alin. \(1\) - \(3\)](#);

h) nu furnizează informațiile solicitate potrivit art. 17 [alin. \(3\)](#) sau [\(5\)](#), ori nu furnizează toate aceste informații, sau furnizează informații inexacte.

ARTICOLUL 23 Constatarea contravențiilor și aplicarea sancțiunilor (1) Constatarea contravenției prevăzute la art. 22 [lit. a](#)) și aplicarea sancțiunii corespunzătoare se fac, la sesizarea oricărei persoane sau din oficiu, de către reprezentanții împuterniciți ai Autorității de reglementare în comunicații și tehnologia informației sau ai autorității de supraveghere prevăzute de Legea [nr. 677/2001](#) pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare.

(2) Constatarea contravențiilor și aplicarea sancțiunilor prevăzute la art. 22 [lit. b\) -h\)](#) se fac de către reprezentanții împuterniciți ai Autorității sau ai celorlalte autorități publice competente, la sesizarea oricărei persoane sau din oficiu.

(3) Constatarea contravențiilor se poate face, în toate cazurile, și de către ofițerii sau subofițerii*) de poliție.

*) Gradul militar "subofițer de poliție" a fost înlocuit cu gradul profesional "agent de poliție" prin Legea [nr. 360/2002](#) privind Statutul polițistului, publicată în Monitorul Oficial al României, Partea I, nr. 440 din 24 iunie 2002.

(4) Contravențiilor prevăzute la [art. 22](#) le sunt aplicabile prevederile Ordonanței Guvernului [nr. 2/2001](#) privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea [nr. 180/2002](#), cu modificările și completările ulterioare.

CAPITOLUL VIII

Infrațiuni săvârșite în legătură cu emiterea și utilizarea instrumentelor de plată electronică și cu utilizarea datelor de identificare în vederea efectuării de operațiuni financiare

~~ARTICOLUL 24 Falsificarea instrumentelor de plată electronică~~ (1) [Abrogat\(ă\)](#)

(2) [Abrogat\(ă\)](#)

(3) [Abrogat\(ă\)](#)

(4) [Abrogat\(ă\)](#)

~~ARTICOLUL 25 Deținerea de echipamente în vederea falsificării instrumentelor de plată electronică~~ [Abrogat\(ă\)](#)

~~ARTICOLUL 26 Falsul în declarații în vederea emiterii sau utilizării instrumentelor de plată electronică~~ [Abrogat\(ă\)](#)

ARTICOLUL 27 Efectuarea de operațiuni financiare în mod fraudulos (1) [Abrogat\(ă\)](#)

(2) [Abrogat\(ă\)](#)

(3) [Abrogat\(ă\)](#)

(4) [Abrogat\(ă\)](#)

(5) [Abrogat\(ă\)](#)

ARTICOLUL 28 Acceptarea operațiunilor financiare efectuate în mod fraudulos (1) [Abrogat\(ă\)](#)

(2) [Abrogat\(ă\)](#)

(3) [Abrogat\(ă\)](#)

ARTICOLUL 29 Constatarea și judecarea infracțiunilor (1) [Abrogat\(ă\)](#)

(2) [Abrogat\(ă\)](#)

(3) [Abrogat\(ă\)](#)

CAPITOLUL IX Dispoziții finale

ARTICOLUL 30 Sarcina probei în cazul litigiilor privind furnizarea de servicii ale societății informaționale În cazul oricărui litigiu privind furnizarea unui serviciu al societății informaționale, declanșat între furnizorul serviciului respectiv și un destinatar al acestui serviciu, sarcina probei îndeplinirii obligațiilor prevăzute la [art. 5, 6, 8 și 9](#) revine furnizorului de servicii dacă destinatarul are calitatea de consumator.

ARTICOLUL 31 Abrogarea unor dispoziții contrare Litera f) a articolului 6 din Ordonanța Guvernului [nr. 130/2000](#) privind regimul juridic al contractelor la distanță, aprobată cu modificări și completări prin Legea [nr. 51/2003](#), se abrogă.

ARTICOLUL 32 Intrarea în vigoare și aplicarea legii (1) În termen de 3 luni de la data publicării prezentei legi în Monitorul Oficial al României, Partea I, Ministerul Comunicațiilor și Tehnologiei Informației va elabora normele metodologice de aplicare a acesteia, care se aprobă prin hotărâre a Guvernului.

(2) Prezenta lege intră în vigoare la data publicării ei în Monitorul Oficial al României, Partea I, și se pune în aplicare la 3 luni de la data intrării în vigoare.

*

Prezenta lege transpune Directiva [2000/31/CE](#) referitoare la anumite aspecte juridice privind serviciile societății informaționale, în special comerțul electronic în piața internă, publicată în Jurnalul Oficial al Comunităților Europene nr. L 178/2000.

Parlamentul României

Legea nr. 193/2000 privind clauzele abuzive din contractele încheiate între profesioniști și consumatori

În vigoare de la 10 decembrie 2000

Formă aplicabilă de la 03 august 2012

Consolidarea din data de **05 noiembrie 2019** are la bază [republicarea din Monitorul Oficial, Partea I](#) nr. 543 din 03 august 2012

Include modificările aduse prin următoarele acte: L [76/2012](#); OUG [34/2014](#).
Ultimul amendament în 13 iunie 2014.

CAPITOLUL I Dispoziții generale

Art. 1. - (1) Orice contract încheiat între profesioniști și consumatori pentru vânzarea de bunuri sau prestarea de servicii va cuprinde clauze contractuale clare, fără echivoc, pentru înțelegerea cărora nu sunt necesare cunoștințe de specialitate.

(2) În caz de dubiu asupra interpretării unor clauze contractuale, acestea vor fi interpretate în favoarea consumatorului.

(3) Se interzice profesioniștilor stipularea de clauze abuzive în contractele încheiate cu consumatorii.

Art. 2. - (1) Prin consumator se înțelege orice persoană fizică sau grup de persoane fizice constituite în asociații, care, în temeiul unui contract care intră sub incidența prezentei legi, acționează în scopuri din afara activității sale comerciale, industriale sau de producție, artizanale ori liberale.

(2) Prin profesionist se înțelege orice persoană fizică sau juridică autorizată, care, în temeiul unui contract care intră sub incidența prezentei legi, acționează în cadrul activității sale comerciale, industriale sau de producție, artizanale ori liberale, precum și orice persoană care acționează în același scop în numele sau pe seama acesteia.

Art. 3. - (1) Prevederile prezentei legi se aplică și bonurilor de comandă sau bonurilor de livrare, biletelor, tichetelor și altora asemenea care conțin stipulări sau referiri la condiții generale prestabilite.

(2) Clauzele contractuale prevăzute în temeiul altor acte normative în vigoare nu sunt supuse dispozițiilor prezentei legi.

CAPITOLUL II Drepturile și obligațiile părților contractante

Art. 4. - (1) O clauză contractuală care nu a fost negociată direct cu consumatorul va fi considerată abuzivă dacă, prin ea însăși sau împreună cu alte prevederi din contract, creează, în detrimentul

consumatorului și contrar cerințelor buneii-credințe, un dezechilibru semnificativ între drepturile și obligațiile părților.

(2) O clauză contractuală va fi considerată ca nefiind negociată direct cu consumatorul dacă aceasta a fost stabilită fără a da posibilitate consumatorului să influențeze natura ei, cum ar fi contractele standard preformulate sau condițiile generale de vânzare practicate de comercianți pe piața produsului sau serviciului respectiv.

(3) Faptul că anumite aspecte ale clauzelor contractuale sau numai una dintre clauze a fost negociată direct cu consumatorul nu exclude aplicarea prevederilor prezentei legi pentru restul contractului, în cazul în care o evaluare globală a contractului evidențiază că acesta a fost prestabilit unilateral de profesionist. Dacă un profesionist pretinde că o clauză standard preformată a fost negociată direct cu consumatorul, este de datoria lui să prezinte probe în acest sens.

(4) Lista cuprinsă în anexa care face parte integrantă din prezenta lege redă, cu titlu de exemplu, clauzele considerate ca fiind abuzive.

(5) Fără a încălca prevederile prezentei legi, natura abuzivă a unei clauze contractuale se evaluează în funcție de:

a) natura produselor sau a serviciilor care fac obiectul contractului la momentul încheierii acestuia;

b) toți factorii care au determinat încheierea contractului;

c) alte clauze ale contractului sau ale altor contracte de care acesta depinde.

(6) Evaluarea naturii abuzive a clauzelor nu se asociază nici cu definirea obiectului principal al contractului, nici cu calitatea de a satisface cerințele de preț și de plată, pe de o parte, nici cu produsele și serviciile oferite în schimb, pe de altă parte, în măsura în care aceste clauze sunt exprimate într-un limbaj ușor inteligibil.

Art. 5. - În cazul contractelor standard preformulate, profesionistul are obligația să remită, la cerere, oricărei persoane interesate un exemplar din contractul pe care îl propune.

Art. 6. - Clauzele abuzive cuprinse în contract și constatate fie personal, fie prin intermediul organelor abilitate prin lege nu vor produce efecte asupra consumatorului, iar contractul se va derula în continuare, cu acordul consumatorului, numai dacă după eliminarea acestora mai poate continua.

Art. 7. - În măsura în care contractul nu își mai poate produce efectele după înlăturarea clauzelor considerate abuzive, consumatorul este îndreptățit să ceară rezilierea contractului, putând solicita, după caz, și daune-interese.

CAPITOLUL III

Organele abilitate pentru constatarea contravențiilor și soluționarea litigiilor

Art. 8. - Controlul respectării dispozițiilor prezentei legi se face de reprezentanții împuterniciți ai Autorității Naționale pentru Protecția Consumatorilor, precum și de specialiști autorizați ai altor organe ale administrației publice, potrivit competențelor.

Art. 9. - Organele de control efectuează verificări la sesizarea persoanelor prejudiciate prevăzute la art. 2 [alin. \(1\)](#) sau din oficiu.

Art. 10. - Profesioniștii au obligația de a prezenta organelor de control, în original, contractele încheiate cu consumatorii.

Art. 11. - Organele de control abilitate încheie procese verbale prin care se consemnează faptele constatate cu ocazia verificărilor făcute, precum și articolele din lege încălcate de profesionist.

Art. 12. - (1) În cazul în care constată utilizarea unor contracte de adeziune care conțin clauze abuzive, organele de control prevăzute la [art. 8](#) vor sesiza tribunalul de la domiciliul sau, după caz, sediul profesionistului, solicitând obligarea acestuia să modifice contractele aflate în curs de executare, prin eliminarea clauzelor abuzive.

(2) La cererea de chemare în judecată va fi anexat procesul-verbal întocmit potrivit [art. 11](#).

(3) Asociațiile pentru protecția consumatorului care îndeplinesc condițiile prevăzute la [art. 30](#) și [32](#) din Ordonanța Guvernului [nr. 21/1992](#) privind protecția consumatorilor, republicată, cu modificările și completările ulterioare, îl pot chema în judecată pe profesionistul care utilizează contracte de adeziune care conțin clauze abuzive, la instanța prevăzută la alin. (1), pentru ca aceasta să dispună încetarea folosirii acestora, precum și modificarea contractelor aflate în curs de executare, prin eliminarea clauzelor abuzive. Dispozițiile art. 13 [alin. \(1\)](#) și [\(4\)](#) sunt aplicabile.

(4) Dispozițiile alin. (1)-(3) nu aduc atingere dreptului consumatorului căruia i se opune un contract de adeziune ce conține clauze abuzive de a invoca nulitatea clauzei pe cale de acțiune ori pe cale de excepție, în condițiile legii.

Art. 13. - (1) Instanța, în cazul în care constată existența clauzelor abuzive în contract, obligă profesionistul să modifice toate contractele de adeziune în curs de executare, precum și să elimine clauzele abuzive din contractele preformulate, destinate a fi utilizate în cadrul activității profesionale.

(2) În cazul prevăzut la alin. (1), instanța va aplica și amenda contravențională prevăzută la [art. 16](#).

(3) Dacă instanța constată că nu sunt clauze abuzive în contract, va anula procesul-verbal întocmit.

(4) Hotărârea este supusă numai apelului.

Art. 14. - Consumatorii prejudiciați prin contracte încheiate cu încălcarea prevederilor prezentei legi au dreptul de a se adresa organelor judecătorești în conformitate cu prevederile [Codului civil](#) și ale [Codului de procedură civilă](#).

Art. 15. - În cazul în care părțile contractante aleg ca lege aplicabilă contractului legea unui stat care nu face parte din Uniunea Europeană, iar contractul are o strânsă legătură cu teritoriul României sau cu al altor state membre ale Uniunii Europene și în cazul în care prezenta lege are prevederi mai favorabile pentru consumator, se vor aplica acestea din urmă.

CAPITOLUL IV

Sanctiuni

Art. 16. - (1) Constituie contravenție, în măsura în care fapta nu este săvârșită în astfel de condiții încât, potrivit legii penale, să fie considerată infracțiune, încălcarea interdicției stipulate la art. 1 [alin. \(3\)](#) și se sancționează cu amendă de la 200 lei la 1.000 lei.

(2) Prevederile prezentei legi se completează cu dispozițiile Ordonanței Guvernului [nr. 2/2001](#) privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea [nr. 180/2002](#), cu modificările și completările ulterioare, cu excepția [art. 27-29](#).

CAPITOLUL V

Dispoziții finale

Art. 17. - Prezenta lege intră în vigoare la 30 de zile de la publicarea în Monitorul Oficial al României, Partea I. La aceeași dată, orice dispoziții contrare se abrogă.

Art. 17¹. - Autoritatea Națională pentru Protecția Consumatorilor informează Comisia Europeană cu privire la adoptarea sau menținerea unor prevederi mai stricte în prezenta ordonanță de urgență decât prevederile Directivei [93/13/CEE](#) a Consiliului din 5 aprilie 1993 privind clauzele abuzive în contractele încheiate cu consumatorii, precum și în legătură cu orice modificare ulterioară a prezentei ordonanțe de urgență, în special în cazul în care respectivele prevederi fie extind testarea caracterului abuziv la clauzele contractuale negociate individual sau la caracterul adecvat al prețului sau remunerației, fie conțin liste de termeni contractuali care vor fi considerați abuzivi.

*

Prezenta lege transpune prevederile Directivei Consiliului [93/13/CEE](#) din 5 aprilie 1993 privind clauzele abuzive în contractele încheiate cu consumatorii, publicată în Jurnalul Oficial al Uniunii Europene (JOCE) nr. L 95 din 21 aprilie 1993.

ANEXĂ

LISTA

cuprinzând clauzele considerate ca fiind abuzive

(1) Sunt considerate clauze abuzive acele prevederi contractuale care:

a) dau dreptul profesionistului de a modifica unilateral clauzele contractului, fără a avea un motiv întemeiat care să fie precizat în contract.

Prevederile acestei litere nu se opun clauzelor în temeiul cărora un furnizor de servicii financiare își rezervă dreptul de a modifica rata dobânzii plătită de către consumator ori datorată acestuia din urmă sau valoarea altor taxe pentru servicii financiare, fără o notificare prealabilă, dacă există o motivație întemeiată, în condițiile în care profesionistul este obligat să informeze cât mai curând posibil despre aceasta celelalte părți contractante și acestea din urmă au libertatea de a rezilia imediat contractul.

Prevederile acestei litere nu se opun, de asemenea, clauzelor prin care profesionistul își rezervă dreptul de a modifica unilateral clauzele unui contract cu durată nedeterminată, în condițiile în care

profesionistul are obligația de a-l informa pe consumator, printr-o notificare prealabilă transmisă în termen rezonabil, pentru ca acesta din urmă să aibă libertatea de a rezilia contractul;

b) obligă consumatorul să se supună unor condiții contractuale despre care nu a avut posibilitatea reală să ia cunoștință la data semnării contractului;

c) obligă consumatorul să își îndeplinească obligațiile contractuale, chiar și în situațiile în care profesionistul nu și le-a îndeplinit pe ale sale;

d) dau dreptul profesionistului să prelungească automat un contract încheiat pentru o perioadă determinată, prin acordul tacit al consumatorului, dacă perioada-limită la care acesta putea să își exprime opțiunea a fost insuficientă;

e) dau dreptul profesionistului să modifice unilateral, fără acordul consumatorului, clauzele privind caracteristicile produselor și serviciilor care urmează să fie furnizate sau termenul de livrare a unui produs ori termenul de executare a unui serviciu;

f) dau dreptul profesionistului să constate unilateral conformitatea produselor și serviciilor furnizate cu prevederile contractuale;

g) dau dreptul exclusiv profesionistului să interpreteze clauzele contractuale;

h) restrâng sau anulează dreptul consumatorului să pretindă despăgubiri în cazurile în care profesionistul nu își îndeplinește obligațiile contractuale;

i) obligă consumatorul la plata unor sume disproporționat de mari în cazul neîndeplinirii obligațiilor contractuale de către acesta, comparativ cu pagubele suferite de profesionist;

j) restrâng sau anulează dreptul consumatorului de a denunța sau de a rezilia unilateral contractul, în cazurile în care:

- profesionistul a modificat unilateral clauzele prevăzute la lit. e);

- profesionistul nu și-a îndeplinit obligațiile contractuale;

- profesionistul a impus consumatorului, prin contract, clauze referitoare la plata unei sume fixe în cazul denunțării unilaterale;

k) exclud sau limitează răspunderea legală a profesionistului în cazul vătămării sau decesului consumatorului, ca rezultat al unei acțiuni sau omisiuni a profesionistului privind utilizarea produselor și serviciilor;

l) exclud dreptul consumatorului de a întreprinde o acțiune legală sau de a exercita un alt remediu legal, solicitându-i în același timp rezolvarea disputelor în special prin arbitraj;

m) permit în mod nejustificat impunerea unor restricții în administrarea probelor evidente de care dispune consumatorul sau solicitarea unor probe care, potrivit legii, fac obiectul unei alte părți din contract;

n) dau dreptul profesionistului să transfere obligațiile contractuale unei terțe persoane - agent, mandatar etc. -, fără acordul consumatorului, dacă acest transfer servește la reducerea garanțiilor sau a altor răspunderi față de consumator;

o) interzic consumatorului să compenseze o datorie către profesionist cu o creanță pe care el ar avea-o asupra profesionistului;

p) prevăd că prețul produselor este determinat la momentul livrării sau permit vânzătorilor de produse ori furnizorilor de servicii dreptul de a crește prețurile, fără ca, în ambele cazuri, să acorde

consumatorului dreptul de a anula contractul în cazul în care prețul final este prea mare în raport cu prețul convenit la momentul încheierii contractului.

Prevederile acestei litere nu se opun clauzelor de indexare a prețurilor, atâ timp cât sunt legale, cu condiția ca metoda prin care prețurile variază să fie descrisă în mod explicit;

r) permit profesionistului obținerea unor sume de bani de la consumator, în cazul neexecutării sau finalizării contractului de către acesta din urmă, fără a prevedea existența compensațiilor în sumă echivalentă și pentru consumator, în cazul neexecutării contractului de către profesionist;

s) dau dreptul profesionistului să anuleze contractul în mod unilateral, fără să prevadă același drept și pentru consumator;

t) dau dreptul profesionistului să înceteze contractul încheiat pentru o durată nedeterminată fără o notificare prealabilă rezonabilă, cu excepția unor motive întemeiate.

Prevederile acestei litere nu se opun clauzelor prin care furnizorul de servicii financiare își rezervă dreptul de a dispune în mod unilateral încetarea unui contract încheiat pe o perioadă nedeterminată și fără o notificare prealabilă în cazul unui motiv întemeiat, cu condiția ca furnizorul să fie obligat să informeze imediat celelalte părți contractante.

(2) Dispozițiile alin. (1) lit. a), p) și t) nu sunt aplicabile în cazul:

a) tranzacțiilor cu valori mobiliare, instrumentelor financiare și altor produse sau servicii, în cazul în care prețul este legat de fluctuațiile cotației bursiere sau ale indicelui bursier ori ale unei rate de schimb pe piața financiară, pe care vânzătorul sau furnizorul nu le poate controla;

b) contractelor pentru cumpărarea sau vânzarea de devize, cecuri de călătorie, ordine de plată internaționale emise în devize sau alte instrumente de plată internaționale.

Parlamentul României

Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)

În vigoare de la 31 iulie 2018

Publicat în Monitorul Oficial, Partea I nr. 651 din 26 iulie 2018. Formă aplicabilă la [05 noiembrie 2019](#).

Parlamentul României adoptă prezenta lege.

CAPITOLUL I Dispoziții generale

Art. 1. - Obiectul legii Prezenta lege stabilește măsurile necesare punerii în aplicare la nivel național, în principal, a prevederilor art. 6 [alin. \(2\)](#), art. 9 [alin. \(4\)](#), [art. 37-39](#), [42](#), [43](#), art. 83 [alin. \(7\)](#), [art. 85](#) și ale [art. 87-89](#) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei [95/46/CE](#), publicat în Jurnalul Oficial al Uniunii Europene, seria L, nr. 119 din 4 mai 2016, denumit în continuare Regulamentul general privind protecția datelor.

Art. 2. - Definiții (1) În aplicarea Regulamentului general privind protecția datelor și a prezentei legi, termenii și expresiile de mai jos se definesc după cum urmează:

a) autorități și organisme publice - Camera Deputaților și Senatul, Administrația Prezidențială, Guvernul, ministerele, celelalte organe de specialitate ale administrației publice centrale, autoritățile și instituțiile publice autonome, autoritățile administrației publice locale și de la nivel județean, alte autorități publice, precum și instituțiile din subordinea/coordonarea acestora. În sensul prezentei legi, sunt asimilate autorităților/organismelor publice și unitățile de cult și asociațiile și fundațiile de utilitate publică;

b) număr de identificare național - numărul prin care se identifică o persoană fizică în anumite sisteme de evidență și care are aplicabilitate generală, cum ar fi: codul numeric personal, seria și numărul actului de identitate, numărul pașaportului, al permisului de conducere, numărul de asigurare socială de sănătate;

c) plan de remediere - anexă la procesul-verbal de constatare și sancționare a contravenției, întocmit în condițiile prevăzute la [art. 11](#), prin care Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, denumită în continuare Autoritatea națională de supraveghere, stabilește măsuri și un termen de remediere;

d) măsură de remediere - soluție dispusă de Autoritatea națională de supraveghere în planul de remediere în vederea îndeplinirii de către autoritatea/organismul public a obligațiilor prevăzute de lege;

e) termen de remediere - perioada de timp de cel mult 90 de zile de la data comunicării procesului-verbal de constatare și sancționare a contravenției, în care autoritatea/organismul public are posibilitatea remedierii neregulilor constatate și îndeplinirii obligațiilor legale;

f) îndeplinirea unei sarcini care servește unui interes public - include acele activități ale partidelor politice sau ale organizațiilor cetățenilor aparținând minorităților naționale, ale organizațiilor neguvernamentale, care servesc realizării obiectivelor prevăzute de dreptul constituțional sau de dreptul internațional public ori funcționării sistemului democratic, incluzând încurajarea participării cetățenilor în procesul de luare a deciziilor și a pregătirii politicilor publice, respectiv promovarea principiilor și valorilor democrației.

(2) În cuprinsul prezentei legi sunt, de asemenea, aplicabile definițiile prevăzute la [art. 4](#) din Regulamentul general privind protecția datelor.

CAPITOLUL II

Reguli speciale privind prelucrarea unor categorii de date cu caracter personal

Art. 3. - Prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea (1) Prelucrarea datelor genetice, biometrice sau a datelor privind sănătatea, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri, este permisă cu consimțământul explicit al persoanei vizate sau dacă prelucrarea este efectuată în temeiul unor dispoziții legale exprese, cu instituirea unor măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate.

(2) Prelucrarea datelor privind sănătatea realizată în scopul asigurării sănătății publice, astfel cum este definită în Regulamentul (CE) [nr. 1.338/2008](#) al Parlamentului European și al Consiliului din 16 decembrie 2008 privind statisticile comunitare referitoare la sănătatea publică, precum și la sănătatea și siguranța la locul de muncă, publicat în Jurnalul Oficial al Uniunii Europene, seria L, nr. 354/70 din 31 decembrie 2008, nu se poate efectua ulterior, în alte scopuri, de către terțe entități.

Art. 4. - Prelucrarea unui număr de identificare național (1) Prelucrarea unui număr de identificare național, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conțin, se poate efectua în situațiile prevăzute de art. 6 [alin. \(1\)](#) din Regulamentul general privind protecția datelor.

(2) Prelucrarea unui număr de identificare național, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conțin, în scopul prevăzut la art. 6 alin. (1) [lit. f](#)) din Regulamentul general privind protecția datelor, respectiv al realizării intereselor legitime urmărite de operator sau de o parte terță, se efectuează cu instituirea de către operator a următoarelor garanții:

- a) punerea în aplicare de măsuri tehnice și organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minimum a datelor, precum și pentru asigurarea securității și confidențialității prelucrărilor de date cu caracter personal, conform dispozițiilor [art. 32](#) din Regulamentul general privind protecția datelor;
- b) numirea unui responsabil pentru protecția datelor, în conformitate cu prevederile [art. 10](#) din prezenta lege;
- c) stabilirea de termene de stocare în funcție de natura datelor și scopul prelucrării, precum și de termene specifice în care datele cu caracter personal trebuie șterse sau revizuite în vederea ștergerii;
- d) instruirea periodică cu privire la obligațiile ce le revin a persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, prelucrează date cu caracter personal.

Art. 5. - Prelucrarea datelor cu caracter personal în contextul relațiilor de muncă În cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaților, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă:

- a) interesele legitime urmărite de angajator sunt temeinic justificate și prevalează asupra intereselor sau drepturilor și libertăților persoanelor vizate;
- b) angajatorul a realizat informarea prealabilă obligatorie, completă și în mod explicit a angajaților;
- c) angajatorul a consultat sindicatul sau, după caz, reprezentanții angajaților înainte de introducerea sistemelor de monitorizare;
- d) alte forme și modalități mai puțin intruzive pentru atingerea scopului urmărit de angajator nu și-au dovedit anterior eficiența; și
- e) durata de stocare a datelor cu caracter personal este proporțională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate.

Art. 6. - Prelucrarea datelor cu caracter personal și de categorii speciale de date cu caracter personal, în contextul îndeplinirii unei sarcini care servește unui interes public În cazul în care prelucrarea datelor personale și speciale este necesară pentru îndeplinirea unei sarcini care servește unui interes public conform art. 6 alin. (1) [lit. e](#)) și art. 9 [lit. g](#)) din Regulamentul general privind protecția datelor se efectuează cu instituirea de către operator sau de către partea terță a următoarelor garanții:

- a) punerea în aplicare a măsurilor tehnice și organizatorice adecvate pentru respectarea principiilor enumerate la [art. 5](#) din Regulamentul general privind protecția datelor, în special a reducerii la minimum a datelor, respectiv a principiului integrității și confidențialității;
- b) numirea unui responsabil pentru protecția datelor, dacă aceasta este necesară în conformitate cu [art. 10](#) din prezenta lege;
- c) stabilirea de termene de stocare în funcție de natura datelor și scopul prelucrării, precum și de termene specifice în care datele cu caracter personal trebuie șterse sau revizuite în vederea ștergerii.

CAPITOLUL III Derogări

Art. 7. - Prelucrarea datelor cu caracter personal în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare În vederea asigurării unui echilibru între dreptul la protecția datelor cu caracter personal, libertatea de exprimare și dreptul la informație, prelucrarea în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare poate fi efectuată, dacă aceasta privește date cu caracter personal care au fost făcute publice în mod manifest de către persoana vizată sau care sunt strâns legate de calitatea de persoană publică a persoanei vizate ori de caracterul public al faptelor în care este implicată, prin derogare de la următoarele capitole din Regulamentul general privind protecția datelor:

- a) capitolul II - Principii;
- b) capitolul III - Drepturile persoanei vizate;
- c) capitolul IV - Operatorul și persoana împuternicită de operator;
- d) capitolul V - Transferurile de date cu caracter personal către țări terțe sau organizații internaționale;
- e) capitolul VI - Autorități de supraveghere independente;
- f) capitolul VII - Cooperare și coerență;
- g) capitolul IX - Dispoziții referitoare la situații specifice de prelucrare.

Art. 8. - Prelucrarea datelor cu caracter personal în scopuri de cercetare științifică sau istorică, în scopuri statistice ori în scopuri de arhivare în interes public (1) Prevederile [art. 15](#), [16](#), [18](#) și [21](#) din Regulamentul general privind protecția datelor nu se aplică în cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică, în măsura în care drepturile menționate la aceste articole sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri.

(2) Prevederile [art. 15](#), [16](#), [18](#), [19](#), [20](#) și [21](#) din Regulamentul general privind protecția datelor nu se aplică în cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare în interes public, în măsura în care drepturile menționate la aceste articole sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar aceste derogări sunt necesare pentru îndeplinirea acestor scopuri.

(3) Derogările prevăzute la [alin. \(1\)](#) și [\(2\)](#) sunt aplicabile numai sub rezerva existenței garanțiilor corespunzătoare pentru drepturile și libertățile persoanelor vizate, prevăzute la art. 89 [alin. \(1\)](#) din Regulamentul general privind protecția datelor.

(4) În cazul în care prelucrarea menționată la [alin. \(1\)](#) și [\(2\)](#) servește în același timp și altui scop, derogările se aplică numai prelucrării în scopurile menționate la alineatele respective.

Art. 9. - (1) În vederea asigurării proporționalității și a unui echilibru între dreptul la protecția datelor cu caracter personal și a datelor speciale și prelucrarea unor astfel de date de către partidele politice și organizațiile cetățenilor aparținând minorităților naționale, organizațiilor neguvernamentale, se vor realiza următoarele garanții:

- a) informarea persoanei vizate despre prelucrarea datelor cu caracter personal;
- b) garantarea transparenței informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate;
- c) garantarea dreptului de rectificare și ștergere.

(2) Prelucrarea datelor cu caracter personal și special este permisă partidelor politice și organizațiilor cetățenilor aparținând minorităților naționale, organizațiilor neguvernamentale, în vederea realizării obiectivelor acestora, fără consimțământul expres al persoanei vizate, dar cu condiția să se prevadă garanțiile corespunzătoare, menționate la alineatul precedent.

CAPITOLUL IV

Responsabilul cu protecția datelor

Art. 10. - Desemnarea și sarcinile responsabilului cu protecția datelor (1) Operatorii și persoanele împuternicite de operator desemnează un responsabil cu protecția datelor în situațiile și condițiile prevăzute la [art. 37-39](#) din Regulamentul general privind protecția datelor.

(2) În cazul în care operatorul sau persoana împuternicită de operator este o autoritate publică sau un organism public, astfel cum este definit la art. 2 alin. (1) [lit. a](#)), poate fi desemnat un responsabil cu protecția datelor, unic pentru mai multe dintre aceste autorități sau organisme, luând în considerare structura organizatorică și dimensiunea acestora.

(3) Activitatea și sarcinile responsabilului cu protecția datelor se realizează cu respectarea prevederilor [art. 38](#) și [39](#) din Regulamentul general privind protecția datelor și a reglementărilor legale naționale aplicabile.

CAPITOLUL V

Organisme de certificare

Art. 11. - Acreditarea organismelor de certificare (1) Acreditarea organismelor de certificare prevăzute la [art. 43](#) din Regulamentul general privind protecția datelor se realizează de Asociația de Acreditare din România - RENAR, în calitate de organism național de acreditare, în conformitate cu Regulamentul (CE) [nr. 765/2008](#) al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) [nr. 339/93](#), publicat în Jurnalul Oficial al Uniunii Europene, seria L, nr. 218 din 13 august 2008, precum și în conformitate cu Ordonanța Guvernului [nr. 23/2009](#) privind activitatea de acreditare a organismelor de evaluare a conformității, aprobată cu modificări prin Legea [nr. 256/2011](#).

(2) Organismele de certificare vor fi acreditate potrivit reglementărilor legale aplicabile, în conformitate cu standardul EN-ISO/IEC 17065 și cu cerințele suplimentare stabilite de Autoritatea națională de supraveghere, precum și cu respectarea prevederilor [art. 43](#) din Regulamentul general privind protecția datelor.

CAPITOLUL VI

Măsuri corective și sancțiuni

Art. 12. - Dispoziții generale privind măsuri corective și sancțiuni (1) Încălcarea dispozițiilor enumerate la art. 83 [alin. \(4\)](#) - [\(6\)](#) din Regulamentul general privind protecția datelor constituie contravenție.

(2) Sancțiunile contravenționale principale sunt avertismentul și amenda contravențională.

(3) Încălcarea prevederilor [art. 3-9](#) din prezenta lege constituie contravenție și se sancționează în condițiile prevăzute la art. 83 [alin. \(5\)](#) din Regulamentul general privind protecția datelor.

(4) Constatarea contravențiilor prevăzute de prezenta lege și aplicarea sancțiunilor contravenționale, precum și a celorlalte măsuri corective prevăzute de [art. 58](#) din Regulamentul general privind protecția datelor se fac de Autoritatea națională de supraveghere, în conformitate cu dispozițiile Regulamentului general privind protecția datelor, ale Legii [nr. 102/2005](#) privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare, și ale prezentei legi.

Art. 13. - Aplicarea măsurilor corective autorităților și organismelor publice (1) În cazul constatării încălcării prevederilor Regulamentului general privind protecția datelor și ale prezentei legi de către autoritățile/organismele publice, Autoritatea națională de supraveghere încheie un proces-verbal de constatare și sancționare a contravenției prin care se aplică sancțiunea avertismentului și la care anexează un plan de remediere.

(2) Termenul de remediere se stabilește în funcție de riscurile asociate prelucrării, precum și demersurile necesar a fi îndeplinite pentru asigurarea conformității prelucrării.

(3) În termen de 10 zile de la data expirării termenului de remediere, Autoritatea națională de supraveghere poate să reia controlul.

(4) Responsabilitatea îndeplinirii măsurilor de remediere revine autorității/organismului public care, potrivit legii, poartă răspunderea contravențională pentru faptele constatate.

(5) Modelul planului de remediere care se anexează la procesul-verbal de constatare și sancționare a contravenției este prevăzut în anexa Plan de remediere, care face parte integrantă din prezenta lege.

Art. 14. - Constatarea contravențiilor și aplicarea de sancțiuni autorităților și organismelor publice (1) Dacă în urma controlului prevăzut la art. 13 [alin. \(3\)](#) se constată faptul că autoritățile/organismele publice nu au adus la îndeplinire în totalitate măsurile prevăzute în planul de remediere, Autoritatea națională de supraveghere, în funcție de circumstanțele fiecărui caz în parte, poate aplica sancțiunea contravențională a amenzii, cu luarea în considerare a criteriilor prevăzute la art. 83 [alin. \(2\)](#) din Regulamentul general privind protecția datelor.

(2) Constituie contravenție încălcarea de către autoritățile/organismele publice a următoarelor dispoziții din Regulamentul general privind protecția datelor, referitoare la:

a) obligațiile operatorului și ale persoanei împuternicite de operator în conformitate cu prevederile [art. 8](#), [art. 11](#), [art. 25-39](#), [art. 42](#) și [43](#);

b) obligațiile organismului de certificare în conformitate cu [art. 42](#) și [43](#);

c) obligațiile organismului de monitorizare în conformitate cu art. 41 [alin. \(4\)](#).

(3) Constituie contravenție încălcarea de către autoritățile/organismele publice a dispozițiilor [art. 3-9](#) din prezenta lege.

(4) Contravențiile prevăzute la [alin. \(2\)](#) și [\(3\)](#) se sancționează cu amendă de la 10.000 lei până la 100.000 lei.

(5) Constituie contravenție încălcarea de către autoritățile/organismele publice a următoarelor dispoziții din Regulamentul general privind protecția datelor, referitoare la:

a) principiile de bază pentru prelucrare, inclusiv condițiile privind consimțământul, în conformitate cu [art. 5-7](#) și [art. 9](#);

b) drepturile persoanelor vizate în conformitate cu [art. 12-22](#);

c) transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu [art. 44-49](#);

d) orice obligații în temeiul legislației naționale adoptate în temeiul [capitolului IX](#);

e) nerespectarea unei decizii sau a unei limitări temporare sau definitive asupra prelucrării sau a suspendării fluxurilor de date, emisă de către Autoritatea națională de supraveghere în temeiul art. 58 [alin. \(2\)](#), sau neacordarea accesului, prin încălcarea dispozițiilor art. 58 [alin. \(1\)](#).

(6) Prin derogare de la prevederile art. 8 alin. (2) [lit. a](#)) din Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea [nr. 180/2002](#), cu modificările și completările ulterioare, contravențiile prevăzute la [alin. \(5\)](#) se sancționează cu amendă de la 10.000 lei până la 200.000 lei.

(7) Constituie contravenție încălcarea de către autoritățile/organismele publice a unei decizii emise de Autoritatea națională de supraveghere în conformitate cu art. 58 [alin. \(2\)](#) coroborat cu art. 83 [alin. \(2\)](#) din Regulamentul general privind protecția datelor.

(8) Prin derogare de la prevederile art. 8 alin. (2) [lit. a](#)) din Ordonanța Guvernului nr. 2/2001, cu modificările și completările ulterioare, contravențiile prevăzute la alin. (7) se sancționează cu amendă de la 10.000 lei până la 200.000 lei.

Art. 15. - În aplicarea prevederilor art. 58 alin. (2) [lit. b](#)) din Regulamentul general privind protecția datelor, art. 14² [alin. \(1\)](#) din Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, publicată în Monitorul Oficial al României, Partea I, nr. 391 din 9 mai 2005, cu modificările și completările ulterioare, se modifică și va avea următorul cuprins:

"

Art. 14². - (1) Sancțiunile contravenționale principale pe care le aplică Autoritatea națională de supraveghere, potrivit art. 58 alin. (2) [lit. b](#)) și [i](#)) din Regulamentul general privind protecția datelor, sunt avertismentul și amenda. Aplicarea amenzii se face în condițiile art. 83 din Regulamentul general privind protecția datelor."

Art. 16. - Prezenta lege intră în vigoare la 5 zile de la data publicării în Monitorul Oficial al României, Partea I.

Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor [art. 75](#) și ale art. 76 [alin. \(1\)](#) din Constituția României, republicată.

p. PREȘEDINTELE CAMEREI
DEPUTAȚILOR,
PETRU-GABRIEL VLASE

p. PREȘEDINTELE
SENATULUI,
IULIAN-CLAUDIU MANDA

București, 18 iulie 2018.

Nr. 190.

ANEXĂ

Plan de remediere
ziua luna anul
Modul de îndeplinire a măsurilor de remediere

| Nr. | Fapta săvârșită | Măsuri de remediere | Termen de remediere | Mod de îndeplinire |
|-----|-----------------|---------------------|---------------------|--------------------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Alte mențiuni

.....
.....
.....

| | |
|---|--|
| Agent constator/ Persoană competentă, (numele, prenumele, semnătura) | Contravenient (numele, prenumele, semnătura) Ștampila |
|---|--|

Parlamentul European și Consiliul Uniunii Europene

Regulamentul nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE) - (General Data Protection Regulation - GDPR)

Număr celex: 32016R0679

În vigoare de la 25 mai 2018

Consolidarea din data de **05 noiembrie 2019** are la bază [publicarea din Jurnalul Oficial al Uniunii Europene](#) nr. 119 din 04 mai 2016

Include modificările aduse prin următoarele acte: Rectificare [2018](#).

Ultimul amendament în 25 mai 2018.

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere [Tratatul](#) privind funcționarea Uniunii Europene, în special [articolul 16](#),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European ⁽¹⁾,

⁽¹⁾ JO C 229, 31.7.2012.

având în vedere avizul Comitetului Regiunilor ⁽²⁾,

⁽²⁾ JO C 391, 18.12.2012.

hotărând în conformitate cu procedura legislativă ordinară ⁽³⁾,

⁽³⁾ Poziția Parlamentului European din 12 martie 2014 (nepublicată încă în Jurnalul Oficial) și Poziția în primă lectură a Consiliului din 8 aprilie 2016 (nepublicată încă în Jurnalul Oficial). Poziția Parlamentului European din 14 aprilie 2016.

întrucât:

(1) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 [alineatul \(1\)](#) din Carta drepturilor fundamentale a Uniunii Europene ("carta") și articolul 16 [alineatul \(1\)](#) din Tratatul privind funcționarea Uniunii Europene (TFUE) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc.

(2) Principiile și normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal ar trebui, indiferent de cetățenia sau de locul de reședință al persoanelor fizice, să respecte drepturile și libertățile fundamentale ale acestora, în special dreptul la protecția datelor cu caracter personal. Prezentul regulament urmărește să contribuie la realizarea unui

spațiu de libertate, securitate și justiție și a unei uniuni economice, la progresul economic și social, la consolidarea și convergența economiilor în cadrul pieței interne și la bunăstarea persoanelor fizice.

(3) Directiva [95/46/CE](#) a Parlamentului European și a Consiliului⁽⁴⁾ vizează armonizarea nivelului de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește activitățile de prelucrare și asigurarea liberei circulații a datelor cu caracter personal între statele membre.

⁽⁴⁾ Directiva [95/46/CE](#) a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date.

(4) Prelucrarea datelor cu caracter personal ar trebui să fie în serviciul cetățenilor. Dreptul la protecția datelor cu caracter personal nu este un drept absolut; acesta trebuie luat în considerare în raport cu funcția pe care o îndeplinește în societate și echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității. Prezentul regulament respectă toate drepturile fundamentale și libertățile și principiile recunoscute în [cartă](#) astfel cum sunt consacrate în tratate, în special respectarea vieții private și de familie, a reședinței și a comunicațiilor, a protecției datelor cu caracter personal, a libertății de gândire, de conștiință și de religie, a libertății de exprimare și de informare, a libertății de a desfășura o activitate comercială, dreptul la o cale de atac eficientă și la un proces echitabil, precum și diversitatea culturală, religioasă și lingvistică.

(5) Integrarea economică și socială care rezultă din funcționarea pieței interne a condus la o creștere substanțială a fluxurilor transfrontaliere de date cu caracter personal. Schimbul de date cu caracter personal între actori publici și privați, inclusiv persoane fizice, asociații și întreprinderi, s-a intensificat în întreaga Uniune. Conform dreptului Uniunii, autoritățile naționale din statele membre sunt chemate să coopereze și să facă schimb de date cu caracter personal pentru a putea să își îndeplinească atribuțiile sau să execute sarcini în numele unei autorități dintr-un alt stat membru.

(6) Evoluțiile tehnologice rapide și globalizarea au generat noi provocări pentru protecția datelor cu caracter personal. Amploarea colectării și a schimbului de date cu caracter personal a crescut în mod semnificativ. Tehnologia permite atât societăților private, cât și autorităților publice să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităților lor. Din ce în ce mai mult, persoanele fizice fac publice la nivel mondial informații cu caracter personal. Tehnologia a transformat deopotrivă economia și viața socială și ar trebui să faciliteze în continuare libera circulație a datelor cu caracter personal în cadrul Uniunii și transferul către țări terțe și organizații internaționale, asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal.

(7) Aceste evoluții impun un cadru solid și mai coerent în materie de protecție a datelor în Uniune, însoțit de o aplicare riguroasă a normelor, luând în considerare importanța creării unui climat de încredere care va permite economiei digitale să se dezvolte pe piața internă. Persoanele fizice ar trebui să aibă control asupra propriilor date cu caracter personal, iar securitatea juridică și practică pentru persoane fizice, operatori economici și autorități publice ar trebui să fie consolidată.

(8) În cazul în care prezentul regulament prevede specificări sau restricționări ale normelor sale de către dreptul intern, statele membre pot, în măsura în care acest lucru este necesar pentru coerență și pentru a asigura înțelegerea dispozițiilor naționale de către persoanele cărora li se aplică acestea, să încorporeze elemente din prezentul regulament în dreptul lor intern.

(9) Obiectivele și principiile Directivei [95/46/CE](#) rămân solide, dar aceasta nu a prevenit fragmentarea modului în care protecția datelor este pusă în aplicare în Uniune, insecuritatea juridică sau percepția publică larg răspândită conform căreia există riscuri semnificative pentru protecția persoanelor fizice, în special în legătură cu activitatea online. Diferențele dintre nivelurile de protecție a drepturilor și libertăților persoanelor fizice, în special a dreptului la protecția datelor cu caracter personal, în ceea ce privește prelucrarea datelor cu caracter personal din statele membre pot împiedica libera circulație a datelor cu caracter personal în întreaga Uniune. Aceste diferențe pot constitui, prin urmare, un obstacol în desfășurarea de activități economice la nivelul Uniunii, pot denatura concurența și pot împiedica autoritățile să îndeplinească responsabilitățile care le revin în temeiul dreptului Uniunii. Această diferență între nivelurile de protecție este cauzată de existența unor deosebiri în ceea ce privește transpunerea și aplicarea Directivei [95/46/CE](#).

(10) Pentru a se asigura un nivel consecvent și ridicat de protecție a persoanelor fizice și pentru a se îndepărta obstacolele din calea circulației datelor cu caracter personal în cadrul Uniunii, nivelul protecției drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea unor astfel de date ar trebui să fie echivalent în toate statele membre. Aplicarea consecventă și omogenă a normelor în materie de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ar trebui să fie asigurată în întreaga Uniune. În ceea ce privește prelucrarea datelor cu caracter personal în vederea respectării unei obligații legale, a îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul, statelor membre ar trebui să li se permită să mențină sau să introducă dispoziții de drept intern care să clarifice într-o mai mare măsură aplicarea normelor prezentului regulament. În coroborare cu legislația generală și orizontală privind protecția datelor, prin care este pusă în aplicare Directiva [95/46/CE](#), statele membre au mai multe legi sectoriale specifice în domenii care necesită dispoziții mai precise. Prezentul regulament oferă, de asemenea, statelor membre o marjă de manevră în specificarea normelor sale, inclusiv în ceea ce privește prelucrarea categoriilor speciale de date cu caracter personal ("date sensibile"). În acest sens, prezentul regulament nu exclude dreptul statelor membre care stabilește circumstanțele aferente unor situații de prelucrare specifice, inclusiv stabilirea cu o mai mare precizie a condițiilor în care prelucrarea datelor cu caracter personal este legală.

(11) Protecția efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea și stabilirea în detaliu a drepturilor persoanelor vizate și a obligațiilor celor care prelucrează și decid prelucrarea datelor cu caracter personal, ci și competențe echivalente pentru monitorizarea și asigurarea conformității cu normele de protecție a datelor cu caracter personal și sancțiuni echivalente pentru infracțiuni în statele membre.

(12) Articolul 16 [alineatul \(2\)](#) din TFUE mandatează Parlamentul European și Consiliul să stabilească normele privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal, precum și normele privind libera circulație a acestor date.

(13) În vederea asigurării unui nivel uniform de protecție pentru persoanele fizice în întreaga Uniune și a preîntâmpinării discrepanțelor care împiedică libera circulație a datelor în cadrul pieței interne, este necesar un regulament în scopul de a furniza securitate juridică și transparență pentru operatorii economici, inclusiv microîntreprinderi și întreprinderi mici și mijlocii, precum și de a oferi persoanelor

fizice în toate statele membre același nivel de drepturi, obligații și responsabilități opozabile din punct de vedere juridic pentru operatori și persoanele împuternicite de aceștia, pentru a se asigura o monitorizare coerentă a prelucrării datelor cu caracter personal, sancțiuni echivalente în toate statele membre, precum și cooperarea eficace a autorităților de supraveghere ale diferitelor state membre. Pentru buna funcționare a pieței interne este necesar ca libera circulație a datelor cu caracter personal în cadrul Uniunii să nu fie restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal. Pentru a se lua în considerare situația specifică a microîntreprinderilor și a întreprinderilor mici și mijlocii, prezentul regulament include o derogare pentru organizațiile cu mai puțin de 250 de angajați în ceea ce privește păstrarea evidențelor. În plus, instituțiile și organele Uniunii și statele membre și autoritățile lor de supraveghere sunt încurajate să ia în considerare necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii în aplicarea prezentului regulament. Noțiunea de microîntreprinderi și de întreprinderi mici și mijlocii ar trebui să se bazeze pe [articolul 2](#) din anexa la Recomandarea 2003/361/CE a Comisiei⁽¹⁾.

⁽¹⁾ Recomandarea [2003/361/CE](#) a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii [C (2003) 1422] (JO L 124, 20.5.2003, p. 36).

(14) Protecția conferită de prezentul regulament ar trebui să vizeze persoanele fizice, indiferent de cetățenia sau de locul de reședință al acestora, în ceea ce privește prelucrarea datelor cu caracter personal ale acestora. Prezentul regulament nu se aplică prelucrării datelor cu caracter personal care privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și datele de contact ale persoanei juridice.

(15) Pentru a preveni apariția unui risc major de eludare, protecția persoanelor fizice ar trebui să fie neutră din punct de vedere tehnologic și să nu depindă de tehnologiile utilizate. Protecția persoanelor fizice ar trebui să se aplice prelucrării datelor cu caracter personal prin mijloace automatizate, precum și prelucrării manuale, în cazul în care datele cu caracter personal sunt cuprinse sau destinate să fie cuprinse într-un sistem de evidență. Dosarele sau seturile de dosare, precum și copertele acestora, care nu sunt structurate în conformitate cu criteriile specifice ar trebui să intre în domeniul de aplicare al prezentului regulament.

(16) Prezentul regulament nu se aplică chestiunilor de protecție a drepturilor și libertăților fundamentale sau la libera circulație a datelor cu caracter personal referitoare la activități care nu intră în domeniul de aplicare al dreptului Uniunii, de exemplu activitățile privind securitatea națională. Prezentul regulament nu se aplică prelucrării datelor cu caracter personal de către statele membre atunci când acestea desfășoară activități legate de politica externă și de securitatea comună a Uniunii.

(17) Regulamentul (CE) [nr. 45/2001](#) al Parlamentului European și al Consiliului se aplică prelucrării de date cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii. Regulamentul (CE) nr. 45/2001 și alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal ar trebui adaptate la principiile și normele stabilite în prezentul regulament și aplicate în conformitate cu prezentul regulament. În vederea asigurării unui cadru solid și coerent în materie de protecție a datelor în Uniune, ar trebui ca după adoptarea prezentului regulament să se aducă Regulamentului (CE) [nr. 45/2001](#) adaptările necesare, astfel încât acestea să poată fi aplicate odată cu prezentul regulament.

(18) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice și care, prin urmare, nu are legătură cu o activitate profesională sau comercială. Activitățile personale sau domestice ar putea include corespondența și repertoriul de adrese sau activitățile din cadrul rețelelor sociale și activitățile online desfășurate în contextul respectivelor activități. Cu toate acestea, prezentul regulament se aplică operatorilor sau persoanelor împuternicite de operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activități personale sau domestice.

(19) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, precum și libera circulație a acestor date, face obiectul unui act juridic specific al Uniunii. Prin urmare, prezentul regulament nu ar trebui să se aplice activităților de prelucrare în aceste scopuri. Cu toate acestea, datele cu caracter personal prelucrate de către autoritățile publice în temeiul prezentului regulament, atunci când sunt utilizate în aceste scopuri, ar trebui să fie reglementate printr-un act juridic mai specific al Uniunii, și anume Directiva (UE) [2016/680](#) a Parlamentului European și a Consiliului. Statele membre pot încredința autorităților competente în sensul Directivei (UE) 2016/680 sarcini care nu sunt neapărat îndeplinite în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, astfel încât prelucrarea datelor cu caracter personal pentru alte scopuri, în măsura în care se încadrează în domeniul de aplicare al dreptului Uniunii, să intre în domeniul de aplicare al prezentului regulament.

În ceea ce privește prelucrarea datelor cu caracter personal de către aceste autorități competente în scopuri care intră în domeniul de aplicare al prezentului regulament, statele membre ar trebui să poată menține sau introduce dispoziții mai detaliate pentru a adapta aplicarea normelor din prezentul regulament. Aceste dispoziții pot stabili mai precis cerințe specifice pentru prelucrarea datelor cu caracter personal de către respectivele autorități competente în aceste alte scopuri, ținând seama de structura constituțională, organizatorică și administrativă a statului membru în cauză. Atunci când prelucrarea de date cu caracter personal de către organisme private face obiectul prezentului regulament, prezentul regulament ar trebui să prevadă posibilitatea ca statele membre, în anumite condiții, să impună prin lege restricții asupra anumitor obligații și drepturi, în cazul în care asemenea restricții constituie o măsură necesară și proporțională într-o societate democratică în scopul garantării unor interese specifice importante, printre care se numără siguranța publică și prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor sau executarea pedepselor, inclusiv protejarea împotriva amenințărilor la adresa siguranței publice și prevenirea acestora. Acest lucru este relevant, de exemplu, în cadrul combaterii spălării de bani sau al activităților laboratoarelor criminalistice.

(20) Deși prezentul regulament se aplică, inter alia, activităților instanțelor și ale altor autorități judiciare, dreptul Uniunii sau al statelor membre ar putea să precizeze operațiunile și procedurile de prelucrare în ceea ce privește prelucrarea datelor cu caracter personal de către instanțe și alte autorități judiciare. Prelucrarea datelor cu caracter personal nu ar trebui să fie de competența autorităților de supraveghere în cazul în care instanțele își exercită atribuțiile judiciare, în scopul garantării

independenței sistemului judiciar în îndeplinirea sarcinilor sale judiciare, inclusiv în luarea deciziilor. Supravegherea unor astfel de operațiuni de prelucrare a datelor ar trebui să poată fi încredințată unor organisme specifice din cadrul sistemului judiciar al statului membru, care ar trebui să asigure în special respectarea normelor prevăzute de prezentul regulament, să sensibilizeze membrii sistemului judiciar cu privire la obligațiile care le revin în temeiul prezentului regulament și să trateze plângerile în legătură cu astfel de operațiuni de prelucrare a datelor.

(21) Prezentul regulament nu aduce atingere aplicării Directivei [2000/31/CE](#) a Parlamentului European și a Consiliului, în special normelor privind răspunderea furnizorilor intermediari de servicii prevăzute la [articolele 12-15](#) din directiva menționată. Respectiva directivă își propune să contribuie la buna funcționare a pieței interne, prin asigurarea liberei circulații a serviciilor societății informaționale între statele membre.

(22) Orice prelucrare a datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune ar trebui efectuată în conformitate cu prezentul regulament, indiferent dacă procesul de prelucrare în sine are loc sau nu în cadrul Uniunii. Sediul implică exercitarea efectivă și reală a unei activități în cadrul unor înțelegeri stabile. Forma juridică a unor astfel de înțelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință.

(23) Pentru a se asigura că persoanele fizice nu sunt lipsite de protecția la care au dreptul în temeiul prezentului regulament, prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Uniunii de către un operator sau o persoană împuternicită de acesta care nu își are sediul în Uniune ar trebui să facă obiectul prezentului regulament în cazul în care activitățile de prelucrare au legătură cu oferirea de bunuri sau servicii unor astfel de persoane vizate, indiferent dacă acestea sunt sau nu legate de o plată. Pentru a determina dacă un astfel de operator sau o astfel de persoană împuternicită de operator oferă bunuri sau servicii unor persoane vizate care se află pe teritoriul Uniunii, ar trebui să se stabilească dacă reiese că operatorul sau persoana împuternicită de operator intenționează să furnizeze servicii persoanelor vizate din unul sau mai multe state membre din Uniune. Întrucât simplul fapt că există acces la un site al operatorului, al persoanei împuternicite de operator sau al unui intermediar în Uniune, că este disponibilă o adresă de e-mail și alte date de contact sau că este utilizată o limbă folosită în general în țara terță în care operatorul își are sediul este insuficient pentru a confirma o astfel de intenție, factori precum utilizarea unei limbi sau a unei monede utilizate în general în unul sau mai multe state membre cu posibilitatea de a comanda bunuri și servicii în respectiva limbă sau menționarea unor clienți sau utilizatori care se află pe teritoriul Uniunii pot conduce la concluzia că operatorul intenționează să ofere bunuri sau servicii unor persoane vizate în Uniune.

(24) Prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Uniunii de către un operator sau o persoană împuternicită de acesta care nu își are sediul în Uniune ar trebui, de asemenea, să facă obiectul prezentului regulament în cazul în care este legată de monitorizarea comportamentului unor astfel de persoane vizate, în măsura în care acest comportament se manifestă pe teritoriul Uniunii. Pentru a se determina dacă o activitate de prelucrare poate fi considerată ca "monitorizare a comportamentului" persoanelor vizate, ar trebui să se stabilească dacă persoanele

fizice sunt urmărite pe internet, inclusiv posibila utilizare ulterioară a unor tehnici de prelucrare a datelor cu caracter personal care constau în crearea unui profil al unei persoane fizice, în special în scopul de a lua decizii cu privire la aceasta sau de a analiza sau de a face previziuni referitoare la preferințele personale, comportamentele și atitudinile acesteia.

(25) În cazul în care dreptul unui stat membru se aplică în temeiul dreptului internațional public, prezentul regulament ar trebui să se aplice, de asemenea, unui operator care nu este stabilit în Uniune, ci, de exemplu, într-o misiune diplomatică sau într-un oficiu consular al unui stat membru.

(26) Principiile protecției datelor ar trebui să se aplice oricărei informații referitoare la o persoană fizică identificată sau identificabilă. Datele cu caracter personal care au fost supuse pseudonimizării, care ar putea fi atribuite unei persoane fizice prin utilizarea de informații suplimentare, ar trebui considerate informații referitoare la o persoană fizică identificabilă. Pentru a se determina dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană, în scopul identificării, în mod direct sau indirect, a persoanei fizice respective. Pentru a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace pentru identificarea persoanei fizice, ar trebui luați în considerare toți factorii obiectivi, precum costurile și intervalul de timp necesare pentru identificare, ținându-se seama atât de tehnologia disponibilă la momentul prelucrării, cât și de dezvoltarea tehnologică. Principiile protecției datelor ar trebui, prin urmare, să nu se aplice informațiilor anonime, adică informațiilor care nu sunt legate de o persoană fizică identificată sau identificabilă sau datelor cu caracter personal care sunt anonimizate astfel încât persoana vizată nu este sau nu mai este identificabilă. Prin urmare, prezentul regulament nu se aplică prelucrării unor astfel de informații anonime, inclusiv în cazul în care acestea sunt utilizate în scopuri statistice sau de cercetare.

(27) Prezentul regulament nu se aplică datelor cu caracter personal referitoare la persoane decedate. Statele membre pot să prevadă norme privind prelucrarea datelor cu caracter personal referitoare la persoane decedate.

(28) Aplicarea pseudonimizării datelor cu caracter personal poate reduce riscurile pentru persoanele vizate și poate ajuta operatorii și persoanele împuternicite de aceștia să își îndeplinească obligațiile de protecție a datelor. Introducerea explicită a conceptului de "pseudonimizare" în prezentul regulament nu este destinată să împiedice alte eventuale măsuri de protecție a datelor.

(29) Pentru a crea stimulente pentru aplicarea pseudonimizării atunci când sunt prelucrate date cu caracter personal, ar trebui să fie posibile măsuri de pseudonimizare, permițând în același timp analiza generală, în cadrul aceluiași operator atunci când operatorul a luat măsurile tehnice și organizatorice necesare pentru a se asigura că prezentul regulament este pus în aplicare în ceea ce privește respectiva prelucrare a datelor și că informațiile suplimentare pentru atribuirea datelor cu caracter personal unei anumite persoane vizate sunt păstrate separat. Operatorul care prelucrează datele cu caracter personal ar trebui să indice persoanele autorizate din cadrul aceluiași operator.

(30) Persoanele fizice pot fi asociate cu identificatorii online furnizați de dispozitivele, aplicațiile, instrumentele și protocoalele lor, cum ar fi adresele IP, identificatorii cookie sau alți identificatori precum etichetele de identificare prin frecvențe radio. Aceștia pot lăsa urme care, în special atunci

când sunt combinate cu identificatori unici și alte informații primite de servere, pot fi utilizate pentru crearea de profiluri ale persoanelor fizice și pentru identificarea lor.

(31) Autoritățile publice cărora le sunt divulgate date cu caracter personal în conformitate cu o obligație legală în vederea exercitării funcției lor oficiale, cum ar fi autoritățile fiscale și vamale, unitățile de investigare financiară, autoritățile administrative independente sau autoritățile piețelor financiare responsabile de reglementarea și supravegherea piețelor titlurilor de valoare, nu ar trebui să fie considerate destinatari în cazul în care primesc date cu caracter personal care sunt necesare pentru efectuarea unei anumite anchete de interes general, în conformitate cu dreptul Uniunii sau cel al statelor membre. Cererile de divulgare trimise de autoritățile publice ar trebui să fie întotdeauna prezentate în scris, motivate și ocazionale și nu ar trebui să se refere la un sistem de evidență în totalitate sau să conducă la interconectarea sistemelor de evidență. Prelucrarea datelor cu caracter personal de către autoritățile publice respective ar trebui să respecte normele aplicabile în materie de protecție a datelor în conformitate cu scopurile prelucrării.

(32) Consimțământul ar trebui acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declarație făcută în scris, inclusiv în format electronic, sau verbal. Acesta ar putea include bifarea unei căsuțe atunci când persoana vizitează un site, alegerea parametrilor tehnici pentru serviciile societății informaționale sau orice altă declarație sau acțiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu ar trebui să constituie un consimțământ. Consimțământul ar trebui să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul ar trebui dat pentru toate scopurile prelucrării. În cazul în care consimțământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară și concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimțământul.

(33) Adesea nu este posibil, în momentul colectării datelor cu caracter personal, să se identifice pe deplin scopul prelucrării datelor în scopuri de cercetare științifică. Din acest motiv, persoanelor vizate ar trebui să li se permită să își exprime consimțământul pentru anumite domenii ale cercetării științifice atunci când sunt respectate standardele etice recunoscute pentru cercetarea științifică. Persoanele vizate ar trebui să aibă posibilitatea de a-și exprima consimțământul doar pentru anumite domenii de cercetare sau părți ale proiectelor de cercetare în măsura permisă de scopul preconizat.

(34) Datele genetice ar trebui definite drept date cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care rezultă în urma unei analize a unei mostre de material biologic al persoanei fizice în cauză, în special a unei analize cromozomiale, a unei analize a acidului dezoxiribonucleic (ADN) sau a acidului ribonucleic (ARN) sau a unei analize a oricărui alt element ce permite obținerea unor informații echivalente.

(35) Datele cu caracter personal privind sănătatea ar trebui să includă toate datele având legătură cu starea de sănătate a persoanei vizate care dezvăluie informații despre starea de sănătate fizică sau mentală trecută, prezentă sau viitoare a persoanei vizate. Acestea includ informații despre persoana

fizică colectate în cadrul înscrierii acesteia la serviciile de asistență medicală sau în cadrul acordării serviciilor respective persoanei fizice în cauză, astfel cum sunt menționate în Directiva [2011/24/UE](#) a Parlamentului European și a Consiliului; un număr, un simbol sau un semn distinctiv atribuit unei persoane fizice pentru identificarea singulară a acesteia în scopuri medicale; informații rezultate din testarea sau examinarea unei părți a corpului sau a unei substanțe corporale, inclusiv din date genetice și eșantioane de material biologic; precum și orice informații privind, de exemplu, o boală, un handicap, un risc de îmbolnăvire, istoricul medical, tratamentul clinic sau starea fiziologică sau biomedicală a persoanei vizate, indiferent de sursa acestora, ca de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro.

(36) Sediul principal al unui operator în Uniune ar trebui să fie locul în care se află administrația centrală a acestuia în Uniune, cu excepția cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului în Uniune. În acest caz, acesta din urmă ar trebui considerat drept sediul principal. Sediul principal al unui operator în Uniune ar trebui să fie determinat conform unor criterii obiective și ar trebui să implice exercitarea efectivă și reală a unor activități de gestionare care să determine principalele decizii cu privire la scopurile și mijloacele de prelucrare în cadrul unor înțelegeri stabile. Acest criteriu nu ar trebui să depindă de realizarea prelucrării datelor cu caracter personal în locul respectiv. Prezența și utilizarea mijloacelor tehnice și a tehnologiilor de prelucrare a datelor cu caracter personal sau activitățile de prelucrare nu constituie un sediu principal și, prin urmare, nu sunt criteriul determinant în acest sens. Sediul principal al persoanei împuternicite de operator ar trebui să fie locul în care se află administrația centrală a acestuia în Uniune sau, în cazul în care nu are o administrație centrală în Uniune, locul în care se desfășoară principalele activități de prelucrare în Uniune. În cazurile care implică atât operatorul, cât și persoana împuternicită de operator, autoritatea de supraveghere principală competentă ar trebui să rămână autoritatea de supraveghere a statului membru în care operatorul își are sediul principal, dar autoritatea de supraveghere a persoanei împuternicite de operator ar trebui considerată ca fiind o autoritate de supraveghere vizată și acea autoritate de supraveghere ar trebui să participe la procedura de cooperare prevăzută de prezentul regulament. În orice caz, autoritățile de supraveghere ale statului membru sau ale statelor membre în care persoana împuternicită de operator are unul sau mai multe sedii nu ar trebui considerate ca fiind autorități de supraveghere vizate în cazul în care proiectul de decizie nu se referă decât la operator. În cazul în care prelucrarea este efectuată de un grup de întreprinderi, sediul principal al întreprinderii care exercită controlul ar trebui considerat drept sediul principal al grupului de întreprinderi, cu excepția cazului în care scopurile și mijloacele aferente prelucrării sunt stabilite de o altă întreprindere.

(37) Un grup de întreprinderi ar trebui să cuprindă o întreprindere care exercită controlul și întreprinderile controlate de aceasta, în cadrul căruia întreprinderea care exercită controlul ar trebui să fie întreprinderea care poate exercita o influență dominantă asupra celorlalte întreprinderi, de exemplu în temeiul proprietății, al participării financiare sau al regulilor care o reglementează sau al competenței de a pune în aplicare norme în materie de protecție a datelor cu caracter personal. O întreprindere care controlează prelucrarea datelor cu caracter personal în întreprinderile sale afiliate ar trebui considerată, împreună cu acestea din urmă, drept "grup de întreprinderi".

(38) Copiii au nevoie de o protecție specifică a datelor lor cu caracter personal, întrucât pot fi mai puțin conștienți de riscurile, consecințele, garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal. Această protecție specifică ar trebui să se aplice în special utilizării datelor cu caracter personal ale copiilor în scopuri de marketing sau pentru crearea de profiluri de personalitate sau de utilizator și la colectarea datelor cu caracter personal privind copiii în momentul utilizării serviciilor oferite direct copiilor. Consimțământul titularului răspunderii părintești nu ar trebui să fie necesar în contextul serviciilor de prevenire sau consiliere oferite direct copiilor.

(39) Orice prelucrare de date cu caracter personal ar trebui să fie legală și echitabilă. Ar trebui să fie transparent pentru persoanele fizice că sunt colectate, utilizate, consultate sau prelucrate în alt mod datele cu caracter personal care le privesc și în ce măsură datele cu caracter personal sunt sau vor fi prelucrate. Principiul transparenței prevede că orice informații și comunicări referitoare la prelucrarea respectivelor date cu caracter personal sunt ușor accesibile și ușor de înțeles și că se utilizează un limbaj simplu și clar. Acest principiu se referă în special la informarea persoanelor vizate privind identitatea operatorului și scopurile prelucrării, precum și la oferirea de informații suplimentare, pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoanele fizice vizate și dreptul acestora de a li se confirma și comunica datele cu caracter personal care le privesc care sunt prelucrate. Persoanele fizice ar trebui informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal și cu privire la modul în care să își exercite drepturile în legătură cu prelucrarea. În special, scopurile specifice în care datele cu caracter personal sunt prelucrate ar trebui să fie explicite și legitime și să fie determinate la momentul colectării datelor respective. Datele cu caracter personal ar trebui să fie adecvate, relevante și limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Aceasta necesită, în special, asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum. Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace. În vederea asigurării faptului că datele cu caracter personal nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ștergere sau revizuirea periodică. Ar trebui să fie luate toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau șterse. Datele cu caracter personal ar trebui prelucrate într-un mod care să asigure în mod adecvat securitatea și confidențialitatea acestora, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizată a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare.

(40) Pentru ca prelucrarea datelor cu caracter personal să fie legală, aceasta ar trebui efectuată pe baza consimțământului persoanei vizate sau în temeiul unui alt motiv legitim, prevăzut de lege, fie în prezentul regulament, fie în alt act din dreptul Uniunii sau din dreptul intern, după cum se prevede în prezentul regulament, inclusiv necesitatea respectării obligațiilor legale la care este supus operatorul sau necesitatea de a executa un contract la care persoana vizată este parte sau pentru a parcurge etapele premergătoare încheierii unui contract, la solicitarea persoanei vizate.

(41) Ori de câte ori prezentul regulament face trimitere la un temei juridic sau la o măsură legislativă, aceasta nu necesită neapărat un act legislativ adoptat de către un parlament, fără a aduce atingere cerințelor care decurg din ordinea constituțională a statului membru în cauză. Cu toate acestea, un

astfel de teme juridic sau o astfel de măsură legislativă ar trebui să fie clară și precisă, iar aplicarea acesteia ar trebui să fie previzibilă pentru persoanele vizate de aceasta, în conformitate cu jurisprudența Curții de Justiție a Uniunii Europene ("Curtea de Justiție") și a Curții Europene a Drepturilor Omului.

(42) În cazul în care prelucrarea se bazează pe consimțământul persoanei vizate, operatorul ar trebui să fie în măsură să demonstreze faptul că persoana vizată și-a dat consimțământul pentru operațiunea de prelucrare. În special, în contextul unei declarații scrise cu privire la un alt aspect, garanțiile ar trebui să asigure că persoana vizată este conștientă de faptul că și-a dat consimțământul și în ce măsură a făcut acest lucru. În conformitate cu Directiva [93/13/CEE](#) a Consiliului, ar trebui furnizată o declarație de consimțământ formulată în prealabil de către operator, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, iar această declarație nu ar trebui să conțină clauze abuzive. Pentru ca acordarea consimțământului să fie în cunoștință de cauză, persoana vizată ar trebui să fie la curent cel puțin cu identitatea operatorului și cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal. Consimțământul nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată.

(43) Pentru a garanta faptul că a fost acordat în mod liber, consimțământul nu ar trebui să constituie un temel juridic valabil pentru prelucrarea datelor cu caracter personal în cazul particular în care există un dezechilibru evident între persoana vizată și operator, în special în cazul în care operatorul este o autoritate publică, iar acest lucru face improbabilă acordarea consimțământului în mod liber în toate circumstanțele aferente respectivei situații particulare. Consimțământul este considerat a nu fi acordat în mod liber în cazul în care aceasta nu permite să se acorde consimțământul separat pentru diferitele operațiuni de prelucrare a datelor cu caracter personal, deși acest lucru este adecvat în cazul particular, sau dacă executarea unui contract, inclusiv furnizarea unui serviciu, este condiționată de consimțământ, în ciuda faptului că consimțământul în cauză nu este necesar pentru executarea contractului.

(44) Prelucrarea ar trebui să fie considerată legală în cazul în care este necesară în cadrul unui contract sau în vederea încheierii unui contract.

(45) În cazul în care prelucrarea este efectuată în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice, prelucrarea ar trebui să aibă un temel în dreptul Uniunii sau în dreptul intern. Prezentul regulament nu impune existența unei legi specifice pentru fiecare prelucrare în parte. Poate fi suficientă o singură lege drept temel pentru mai multe operațiuni de prelucrare efectuate în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice. De asemenea, ar trebui ca scopul prelucrării să fie stabilit în dreptul Uniunii sau în dreptul intern. Mai mult decât atât, dreptul respectiv ar putea să specifice condițiile generale ale prezentului regulament care reglementează legalitatea prelucrării datelor cu caracter personal, să determine specificațiile pentru stabilirea operatorului, a tipului de date cu caracter personal care fac obiectul prelucrării, a persoanelor vizate, a entităților cărora le pot fi divulgate datele

cu caracter personal, a limitărilor în funcție de scop, a perioadei de stocare și a altor măsuri pentru a garanta o prelucrare legală și echitabilă. De asemenea, ar trebui să se stabilească în dreptul Uniunii sau în dreptul intern dacă operatorul care îndeplinește o sarcină care servește unui interes public sau care face parte din exercitarea autorității publice ar trebui să fie o autoritate publică sau o altă persoană fizică sau juridică guvernată de dreptul public sau, atunci când motive de interes public justifică acest lucru, inclusiv în scopuri medicale, precum sănătatea publică și protecția socială, precum și gestionarea serviciilor de asistență medicală, de dreptul privat, cum ar fi o asociație profesională.

(46) Prelucrarea datelor cu caracter personal ar trebui, de asemenea, să fie considerată legală în cazul în care este necesară în scopul asigurării protecției unui interes care este esențial pentru viața persoanei vizate sau pentru viața unei alte persoane fizice. Prelucrarea datelor cu caracter personal care are drept temei interesele vitale ale unei alte persoane fizice ar trebui efectuată numai în cazul în care prelucrarea nu se poate baza în mod evident pe un alt temei juridic. Unele tipuri de prelucrare pot servi atât unor motive importante de interes public, cât și intereselor vitale ale persoanei vizate, de exemplu în cazul în care prelucrarea este necesară în scopuri umanitare, inclusiv în vederea monitorizării unei epidemii și a răspândirii acesteia sau în situații de urgențe umanitare, în special în situații de dezastre naturale sau provocate de om.

(47) Interesele legitime ale unui operator, inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terțe părți, pot constitui un temei juridic pentru prelucrare, cu condiția să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate, luând în considerare așteptările rezonabile ale persoanelor vizate bazate pe relația acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relație relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia. În orice caz, existența unui interes legitim ar necesita o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată poate preconiza în mod rezonabil, în momentul și în contextul colectării datelor cu caracter personal, posibilitatea prelucrării în acest scop. Interesele și drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date atunci când datele cu caracter personal sunt prelucrate în circumstanțe în care persoanele vizate nu preconizează în mod rezonabil o prelucrare ulterioară. Întrucât legiuitorul trebuie să furnizeze temeiul juridic pentru prelucrarea datelor cu caracter personal de către autoritățile publice, temeiul juridic respectiv nu ar trebui să se aplice prelucrării de către autoritățile publice în îndeplinirea sarcinilor care le revin. Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor constituie, de asemenea, un interes legitim al operatorului de date în cauză. Prelucrarea de date cu caracter personal care are drept scop marketingul direct poate fi considerată ca fiind desfășurată pentru un interes legitim.

(48) Operatorii care fac parte dintr-un grup de întreprinderi sau instituții afiliate unui organism central pot avea un interes legitim de a transmite date cu caracter personal în cadrul grupului de întreprinderi în scopuri administrative interne, inclusiv în scopul prelucrării datelor cu caracter personal ale clienților sau angajaților. Principiile generale ale transferului de date cu caracter personal, în cadrul unui grup de întreprinderi, către o întreprindere situată într-o țară terță rămân neschimbate.

(49) Prelucrarea datelor cu caracter personal în măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor, și anume capacitatea unei rețele sau a unui sistem de informații de a face față, la un anumit nivel de încredere, evenimentelor accidentale sau acțiunilor ilegale sau rău intenționate care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor cu caracter personal stocate sau transmise, precum și securitatea serviciilor conexe oferite de aceste rețele și sisteme, sau accesibile prin intermediul acestora, de către autoritățile publice, echipele de intervenție în caz de urgență informatică, echipele de intervenție în cazul producerii unor incidente care afectează securitatea informatică, furnizorii de rețele și servicii de comunicații electronice, precum și de către furnizorii de servicii și tehnologii de securitate, constituie un interes legitim al operatorului de date în cauză. Acesta ar putea include, de exemplu, prevenirea accesului neautorizat la rețelele de comunicații electronice și a difuzării de coduri dăunătoare și oprirea atacurilor de "blocare a serviciului", precum și prevenirea daunelor aduse calculatoarelor și sistemelor de comunicații electronice.

(50) Prelucrarea datelor cu caracter personal în alte scopuri decât scopurile pentru care datele cu caracter personal au fost inițial colectate ar trebui să fie permisă doar atunci când prelucrarea este compatibilă cu scopurile respective pentru care datele cu caracter personal au fost inițial colectate. În acest caz nu este necesar un temei juridic separat de cel pe baza căruia a fost permisă colectarea datelor cu caracter personal. În cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul, dreptul Uniunii sau dreptul intern poate stabili și specifica sarcinile și scopurile pentru care prelucrarea ulterioară ar trebui considerată a fi compatibilă și legală. Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ar trebui considerată ca reprezentând operațiuni de prelucrare legale compatibile. Temeiul juridic prevăzut în dreptul Uniunii sau în dreptul intern pentru prelucrarea datelor cu caracter personal poate constitui, de asemenea, un temei juridic pentru prelucrarea ulterioară. Pentru a stabili dacă scopul prelucrării ulterioare este compatibil cu scopul pentru care au fost colectate inițial datele cu caracter personal, operatorul, după ce a îndeplinit toate cerințele privind legalitatea prelucrării inițiale, ar trebui să țină seama, printre altele, de orice legătură între respectivele scopuri și scopurile prelucrării ulterioare preconizate, de contextul în care au fost colectate datele cu caracter personal, în special de așteptările rezonabile ale persoanelor vizate, bazate pe relația lor cu operatorul, în ceea ce privește utilizarea ulterioară a datelor, de natura datelor cu caracter personal, de consecințele prelucrării ulterioare preconizate asupra persoanelor vizate, precum și de existența garanțiilor corespunzătoare atât în cadrul operațiunilor de prelucrare inițiale, cât și în cadrul operațiunilor de prelucrare ulterioare preconizate.

În cazul în care persoana vizată și-a dat consimțământul sau prelucrarea se bazează pe dreptul Uniunii sau pe dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja, în special, obiective importante de interes public general, operatorul ar trebui să aibă posibilitatea de a prelucra în continuare datele cu caracter personal, indiferent de compatibilitatea scopurilor. În orice caz, aplicarea principiilor stabilite de prezentul regulament și, în special, informarea persoanei vizate cu privire la aceste alte scopuri și la drepturile sale, inclusiv dreptul la opoziție, ar

trebui să fie garantate. Indicarea unor posibile infracțiuni sau amenințări la adresa siguranței publice de către operator și transmiterea către o autoritate competentă a datelor cu caracter personal relevante în cazuri individuale sau în mai multe cazuri legate de aceeași infracțiune sau de aceeași amenințări la adresa siguranței publice ar trebui considerată ca fiind în interesul legitim urmărit de operator. Cu toate acestea, o astfel de transmitere în interesul legitim al operatorului sau prelucrarea ulterioară a datelor cu caracter personal ar trebui interzisă în cazul în care prelucrarea nu este compatibilă cu o obligație legală, profesională sau cu o altă obligație de păstrare a confidențialității.

(51) Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale necesită o protecție specifică, deoarece contextul prelucrării acestora ar putea genera riscuri considerabile la adresa drepturilor și libertăților fundamentale. Aceste date cu caracter personal ar trebui să includă datele cu caracter personal care dezvăluie originea rasială sau etnică, utilizarea termenului "origine rasială" în prezentul regulament neimplicând o acceptare de către Uniune a teoriilor care urmăresc să stabilească existența unor rase umane separate. Prelucrarea fotografiilor nu ar trebui să fie considerată în mod sistematic ca fiind o prelucrare de categorii speciale de date cu caracter personal, întrucât fotografiile intră sub incidența definiției datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice. Asemenea date cu caracter personal nu ar trebui prelucrate, cu excepția cazului în care prelucrarea este permisă în cazuri specifice prevăzute de prezentul regulament, ținând seama de faptul că dreptul statelor membre poate prevedea dispoziții specifice cu privire la protecția datelor în scopul adaptării aplicării normelor din prezentul regulament în vederea respectării unei obligații legale sau a îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul. Pe lângă cerințele specifice pentru o astfel de prelucrare, ar trebui să se aplice principiile generale și alte norme prevăzute de prezentul regulament, în special în ceea ce privește condițiile pentru prelucrarea legală. Ar trebui prevăzute în mod explicit derogări de la interdicția generală de prelucrare a acestor categorii speciale de date cu caracter personal, printre altele atunci când persoana vizată își dă consimțământul explicit sau în ceea ce privește nevoile specifice în special atunci când prelucrarea este efectuată în cadrul unor activități legitime de către anumite asociații sau fundații al căror scop este de a permite exercitarea libertăților fundamentale.

(52) Derogarea de la interdicția privind prelucrarea categoriilor speciale de date cu caracter personal ar trebui să fie permisă, de asemenea, în cazul în care dreptul Uniunii sau dreptul intern prevede acest lucru și ar trebui să facă obiectul unor garanții adecvate, astfel încât să fie protejate datele cu caracter personal și alte drepturi fundamentale, atunci când acest lucru se justifică din motive de interes public, în special în cazul prelucrării datelor cu caracter personal în domeniul legislației privind ocuparea forței de muncă, protecția socială, inclusiv pensiile, precum și în scopuri de securitate, supraveghere și alertă în materie de sănătate, pentru prevenirea sau controlul bolilor transmisibile și a altor amenințări grave la adresa sănătății. Această derogare poate fi acordată în scopuri medicale, inclusiv sănătatea publică și gestionarea serviciilor de asistență medicală, în special în vederea asigurării calității și eficienței din punctul de vedere al costurilor ale procedurilor utilizate pentru soluționarea cererilor de prestații și servicii în cadrul sistemului de asigurări de sănătate, sau în scopuri de arhivare în interes public, în

scopuri de cercetare științifică sau istorică ori în scopuri statistice. De asemenea, prelucrarea unor asemenea date cu caracter personal ar trebui permisă, printr-o derogare, atunci când este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiție, indiferent dacă are loc în cadrul unei proceduri în fața unei instanțe sau în cadrul unei proceduri administrative sau a unei proceduri extrajudiciare.

(53) Categoriile speciale de date cu caracter personal care necesită un nivel mai ridicat de protecție ar trebui prelucrate doar în scopuri legate de sănătate atunci când este necesar pentru realizarea acestor scopuri în beneficiul persoanelor fizice și al societății în general, în special în contextul gestionării serviciilor și sistemelor de sănătate sau de asistență socială, inclusiv prelucrarea acestor date de către autoritățile de management și de către autoritățile centrale naționale din domeniul sănătății în scopul controlului calității, furnizării de informații de gestiune și al supravegherii generale a sistemului de sănătate sau de asistență socială la nivel național și local, precum și în contextul asigurării continuității asistenței medicale sau sociale și a asistenței medicale transfrontaliere ori în scopuri de securitate, supraveghere și alertă în materie de sănătate ori în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice în temeiul dreptului Uniunii sau al dreptului intern, care trebuie să urmărească un obiectiv de interes public, precum și în cazul studiilor realizate în interes public în domeniul sănătății publice. Prin urmare, prezentul regulament ar trebui să prevadă condiții armonizate pentru prelucrarea categoriilor speciale de date cu caracter personal privind sănătatea, în ceea ce privește nevoile specifice, în special atunci când prelucrarea acestor date este efectuată în anumite scopuri legate de sănătate de către persoane care fac obiectul unei obligații legale de a păstra secretul profesional. Dreptul Uniunii sau dreptul intern ar trebui să prevadă măsuri specifice și adecvate pentru a proteja drepturile fundamentale și datele cu caracter personal ale persoanelor fizice. Statele membre ar trebui să aibă posibilitatea de a menține sau de a introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea. Totuși, acest lucru nu ar trebui să împiedice libera circulație a datelor cu caracter personal în cadrul Uniunii atunci când aceste condiții se aplică prelucrării transfrontaliere a unor astfel de date.

(54) Prelucrarea categoriilor speciale de date cu caracter personal poate fi necesară din motive de interes public în domeniile sănătății publice, fără consimțământul persoanei vizate. O astfel de prelucrare ar trebui condiționată de măsuri adecvate și specifice destinate să protejeze drepturile și libertățile persoanelor fizice. În acest context, conceptul de "sănătate publică" ar trebui interpretat astfel cum este definit în Regulamentul (CE) [nr. 1338/2008](#) al Parlamentului European și al Consiliului, și anume toate elementele referitoare la sănătate și anume starea de sănătate, inclusiv morbiditatea sau handicapul, factorii determinanți care au efect asupra stării de sănătate, necesitățile în domeniul asistenței medicale, resursele alocate asistenței medicale, furnizarea asistenței medicale și asigurarea accesului universal la aceasta, precum și cheltuielile și sursele de finanțare în domeniul sănătății și cauzele mortalității. Această prelucrare a datelor privind sănătatea din motive de interes public nu ar trebui să ducă la prelucrarea acestor date în alte scopuri de către părți terțe, cum ar fi angajatorii sau societățile de asigurări și băncile.

(55) În plus, prelucrarea datelor cu caracter personal de către autoritățile publice în vederea realizării obiectivelor prevăzute de dreptul constituțional sau de dreptul internațional public, ale asociațiilor religioase recunoscute oficial se efectuează din motive de interes public.

(56) În cazul în care, în cadrul activităților electorale, funcționarea sistemului democratic necesită, într-un stat membru, ca partidele politice să colecteze date cu caracter personal privind opiniile politice ale persoanelor, prelucrarea unor astfel de date poate fi permisă din motive de interes public, cu condiția să se prevadă garanțiile corespunzătoare.

(57) Dacă datele cu caracter personal prelucrate de un operator nu îi permit acestuia să identifice o persoană fizică, operatorul de date nu ar trebui să aibă obligația de a obține informații suplimentare în vederea identificării persoanei vizate, cu unicul scop de a respecta oricare dintre dispozițiile prezentului regulament. Cu toate acestea, operatorul nu ar trebui să refuze să preia informațiile suplimentare furnizate de persoana vizată cu scopul de a sprijini exercitarea drepturilor acesteia. Identificarea ar trebui să includă identificarea digitală a unei persoane vizate, de exemplu prin mecanisme de autentificare precum aceleași acreditări utilizate de către persoana vizată pentru a accesa serviciile online oferite de operatorul de date.

(58) Principiul transparenței prevede că orice informații care se adresează publicului sau persoanei vizate să fie concise, ușor accesibile și ușor de înțeles și să se utilizeze un limbaj simplu și clar, precum și vizualizare acolo unde este cazul. Aceste informații ar putea fi furnizate în format electronic, de exemplu atunci când sunt adresate publicului, prin intermediul unui site. Acest lucru este important în special în situații în care datorită multitudinii actorilor și a complexității, din punct de vedere tehnologic, a practicii, este dificil ca persoana vizată să știe și să înțeleagă dacă datele cu caracter personal care o privesc sunt colectate, de către cine și în ce scop, cum este cazul publicității online. Întrucât copiii necesită o protecție specifică, orice informații și orice comunicare, în cazul în care prelucrarea vizează un copil, ar trebui să fie exprimate într-un limbaj simplu și clar, astfel încât copilul să îl poată înțelege cu ușurință.

(59) Ar trebui să fie prevăzute modalități de facilitare a exercitării de către persoana vizată a drepturilor care îi sunt conferite prin prezentul regulament, inclusiv mecanismele prin care aceasta poate solicita și, dacă este cazul, obține, în mod gratuit, în special, acces la datele cu caracter personal, precum și rectificarea sau ștergerea acestora, și exercitarea dreptului la opoziție. Operatorul ar trebui să ofere, de asemenea, modalități de introducere a cererilor pe cale electronică, mai ales în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice. Operatorul ar trebui să aibă obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate și cel târziu în termen de o lună și, în cazul în care nu intenționează să se conformeze respectivele cereri, să motiveze acest refuz.

(60) Conform principiilor prelucrării echitabile și transparente, persoana vizată este informată cu privire la existența unei operațiuni de prelucrare și la scopurile acesteia. Operatorul ar trebui să furnizeze persoanei vizate orice informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă, ținând seama de circumstanțele specifice și de contextul în care sunt prelucrate datele cu caracter personal. În plus, persoana vizată ar trebui informată cu privire la crearea de profiluri, precum și la consecințele acesteia. Atunci când datele cu caracter personal sunt colectate de la persoana vizată, aceasta ar trebui informată, de asemenea, dacă are obligația de a furniza datele

cu caracter personal și care sunt consecințele în cazul unui refuz. Aceste informații pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea ar trebui să poată fi citite automat.

(61) Informațiile în legătură cu prelucrarea datelor cu caracter personal referitoare la persoana vizată ar trebui furnizate acesteia la momentul colectării de la persoana vizată sau, în cazul în care datele cu caracter personal sunt obținute din altă sursă, într-o perioadă rezonabilă, în funcție de circumstanțele cazului. În cazul în care datele cu caracter personal pot fi divulgate în mod legitim unui alt destinatar, persoana vizată ar trebui informată atunci când datele cu caracter personal sunt divulgate pentru prima dată destinatarului. În cazul în care operatorul intenționează să prelucreze datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul ar trebui să furnizeze persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și alte informații necesare. În cazul în care originea datelor cu caracter personal nu a putut fi comunicată persoanei vizate din cauză că au fost utilizate surse diverse, informațiile generale ar trebui furnizate.

(62) Cu toate acestea, nu este necesară impunerea obligației de a furniza informații în cazul în care persoana vizată deține deja informațiile, în cazul în care înregistrarea sau divulgarea datelor cu caracter personal este prevăzută în mod expres de lege sau în cazul în care informarea persoanei vizate se dovedește imposibilă sau ar implica eforturi disproporționate. Acesta din urmă ar putea fi cazul în special atunci când prelucrarea se efectuează în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. În această privință, ar trebui luate în considerare numărul persoanelor vizate, vechimea datelor și orice garanții adecvate adoptate.

(63) O persoană vizată ar trebui să aibă drept de acces la datele cu caracter personal colectate care o privesc și ar trebui să își exercite acest drept cu ușurință și la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia. Acest lucru include dreptul persoanelor vizate de a avea acces la datele lor privind sănătatea, de exemplu datele din registrele lor medicale conținând informații precum diagnostice, rezultate ale examinărilor, evaluări ale medicilor curanți și orice tratament sau intervenție efectuată. Orice persoană vizată ar trebui, prin urmare, să aibă dreptul de a cunoaște și de a i se comunica în special scopurile în care sunt prelucrate datele, dacă este posibil perioada pentru care se prelucrează datele cu caracter personal, destinatarii datelor cu caracter personal, logica de prelucrare automată a datelor cu caracter personal și, cel puțin în cazul în care se bazează pe crearea de profiluri, consecințele unei astfel de prelucrări. Dacă acest lucru este posibil, operatorul de date ar trebui să poată furniza acces de la distanță la un sistem sigur, care să ofere persoanei vizate acces direct la datele sale cu caracter personal. Acest drept nu ar trebui să aducă atingere drepturilor sau libertăților altora, inclusiv secretului comercial sau proprietății intelectuale și, în special, drepturilor de autor care asigură protecția programelor software. Cu toate acestea, considerațiile de mai sus nu ar trebui să aibă drept rezultat refuzul de a furniza toate informațiile persoanei vizate. Atunci când operatorul prelucrează un volum mare de informații privind persoana vizată, operatorul ar trebui să poată solicita ca, înainte de a îi fi furnizate informațiile, persoana vizată să precizeze informațiile sau activitățile de prelucrare la care se referă cererea sa.

(64) Operatorul ar trebui să ia toate măsurile rezonabile pentru a verifica identitatea unei persoane vizate care solicită acces la date, în special în contextul serviciilor online și al identificatorilor online. Un operator nu ar trebui să rețină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacționeze la cereri potențiale.

(65) O persoană vizată ar trebui să aibă dreptul la rectificarea datelor cu caracter personal care o privesc și "dreptul de a fi uitată", în cazul în care păstrarea acestor date încalcă prezentul regulament sau dreptul Uniunii sau dreptul intern sub incidența căruia intră operatorul. În special, persoanele vizate ar trebui să aibă dreptul ca datele lor cu caracter personal să fie șterse și să nu mai fie prelucrate, în cazul în care datele cu caracter personal nu mai sunt necesare pentru scopurile în care sunt colectate sau sunt prelucrate, în cazul în care persoanele vizate și-au retras consimțământul pentru prelucrare sau în cazul în care acestea se opun prelucrării datelor cu caracter personal care le privesc sau în cazul în care prelucrarea datelor cu caracter personal ale acestora nu este conformă cu prezentul regulament. Acest drept este relevant în special în cazul în care persoana vizată și-a dat consimțământul când era copil și nu cunoștea pe deplin riscurile pe care le implică prelucrarea, iar ulterior dorește să elimine astfel de date cu caracter personal, în special de pe internet. Persoana vizată ar trebui să aibă posibilitatea de a-și exercita acest drept în pofida faptului că nu mai este copil. Cu toate acestea, păstrarea în continuare a datelor cu caracter personal ar trebui să fie legală în cazul în care este necesară pentru exercitarea dreptului la libertatea de exprimare și de informare, pentru respectarea unei obligații legale, pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul, din motive de interes public în domeniul sănătății publice, în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice sau pentru constatarea, exercitarea sau apărarea unui drept în instanță.

(66) Pentru a se consolida "dreptul de a fi uitat" în mediul online, dreptul de ștergere ar trebui să fie extins astfel încât un operator care a făcut publice date cu caracter personal ar trebui să aibă obligația de a informa operatorii care prelucrează respectivele date cu caracter personal să șteargă orice linkuri către datele respective sau copii sau reproduceri ale acestora. În acest scop, operatorul în cauză ar trebui să ia măsuri rezonabile, ținând seama de tehnologia disponibilă și de mijloacele aflate la dispoziția lui, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal în ceea ce privește cererea persoanei vizate.

(67) Metodele de restricționare a prelucrării de date cu caracter personal ar putea include, printre altele, mutarea temporară a datelor cu caracter personal selectate într-un alt sistem de prelucrare, sau anularea accesului utilizatorilor la datele selectate sau înlăturarea temporară a datelor publicate de pe un site. În ceea ce privește sistemele automatizate de evidență a datelor, restricționarea prelucrării ar trebui, în principiu, asigurată prin mijloace tehnice în așa fel încât datele cu caracter personal să nu facă obiectul unor operațiuni de prelucrare ulterioară și să nu mai poată fi schimbate. Faptul că prelucrarea datelor cu caracter personal este restricționată ar trebui indicat în mod clar în sistem.

(68) Pentru a spori suplimentar controlul asupra propriilor date, persoana vizată ar trebui, în cazul în care datele cu caracter personal sunt prelucrate prin mijloace automate, să poată primi datele cu caracter personal care o privesc și pe care le-a furnizat unui operator, într-un format structurat, utilizat

în mod curent, prelucrabil automat și interoperabil și să le poată transmite unui alt operator. Operatorii de date ar trebui să fie încurajați să dezvolte formate interoperabile care să permită portabilitatea datelor. Acest drept ar trebui să se aplice în cazul în care persoana vizată a furnizat datele cu caracter personal pe baza propriului consimțământ sau în cazul în care prelucrarea datelor este necesară pentru executarea unui contract. Acest drept nu ar trebui să se aplice în cazul în care prelucrarea se bazează pe un alt temei juridic decât consimțământul sau contractul. Prin însăși natura sa, acest drept nu ar trebui exercitat împotriva operatorilor care prelucrează date cu caracter personal în cadrul exercitării funcțiilor lor publice. Acesta nu ar trebui să se aplice în special în cazul în care prelucrarea de date cu caracter personal este necesară în vederea respectării unei obligații legale căreia îi este supus operatorul sau în cazul îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea unei autorități publice cu care este investit operatorul. Dreptul persoanei vizate de a transmite sau de a primi date cu caracter personal care o privesc nu ar trebui să creeze pentru operatori obligația de a adopta sau de a menține sisteme de prelucrare care să fie compatibile din punct de vedere tehnic. În cazul în care, într-un anumit set de date cu caracter personal, sunt implicate mai multe persoane vizate, dreptul de a primi datele cu caracter personal nu ar trebui să aducă atingere drepturilor și libertăților altor persoane vizate, în conformitate cu prezentul regulament. De asemenea, acest drept nu ar trebui să aducă atingere dreptului persoanei vizate de a obține ștergerea datelor cu caracter personal și limitărilor dreptului respectiv, astfel cum sunt prevăzute în prezentul regulament, și nu ar trebui, în special, să implice ștergerea acelor date cu caracter personal referitoare la persoana vizată care au fost furnizate de către aceasta în vederea executării unui contract, în măsura în care și atât timp cât datele respective sunt necesare pentru executarea contractului. Persoana vizată ar trebui să aibă dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul, dacă acest lucru este fezabil din punct de vedere tehnic.

(69) În cazurile în care datele cu caracter personal ar putea fi prelucrate în mod legal deoarece prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul sau pe baza intereselor legitime ale unui operator sau ale unei părți terțe, o persoană vizată ar trebui să aibă totuși dreptul de a se opune prelucrării oricăror date cu caracter personal care se referă la situația sa particulară. Ar trebui să revină operatorului sarcina de a demonstra că interesele sale legitime și imperioase prevalează asupra intereselor sau a drepturilor și libertăților fundamentale ale persoanei vizate.

(70) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de marketing direct, persoana vizată ar trebui să aibă dreptul de a se opune unei astfel de prelucrări, inclusiv creării de profiluri în măsura în care aceasta are legătură cu marketingul direct, indiferent dacă prelucrarea în cauză este cea inițială sau una ulterioară, în orice moment și în mod gratuit. Acest drept ar trebui adus în mod explicit în atenția persoanei vizate și prezentat în mod clar și separat de orice alte informații.

(71) Persoana vizată ar trebui să aibă dreptul de a nu face obiectul unei decizii, care poate include o măsură, care evaluează aspecte personale referitoare la persoana vizată, care se bazează exclusiv pe prelucrarea automată și care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă, cum ar fi refuzul automat al unei cereri de credit online sau practicile de recrutare pe cale electronică, fără intervenție umană. O astfel de prelucrare include

"crearea de profiluri", care constă în orice formă de prelucrare automată a datelor cu caracter personal prin evaluarea aspectelor personale referitoare la o persoană fizică, în special în vederea analizării sau preconizării anumitor aspecte privind randamentul la locul de muncă al persoanei vizate, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările, atunci când aceasta produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă. Cu toate acestea, luarea de decizii pe baza unei astfel de prelucrări, inclusiv crearea de profiluri, ar trebui permisă în cazul în care este autorizată în mod expres în dreptul Uniunii sau în dreptul intern care se aplică operatorului, inclusiv în scopul monitorizării și prevenirii fraudei și a evaziunii fiscale, desfășurate în conformitate cu reglementările, standardele și recomandările instituțiilor Uniunii sau ale organismelor naționale de supraveghere, și în scopul asigurării securității și fiabilității unui serviciu oferit de operator sau în cazul în care este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator sau în cazul în care persoana vizată și-a dat în mod explicit consimțământul. În orice caz, o astfel de prelucrare ar trebui să facă obiectul unor garanții corespunzătoare, care ar trebui să includă o informare specifică a persoanei vizate și dreptul acesteia de a obține intervenție umană, de a-și exprima punctul de vedere, de a primi o explicație privind decizia luată în urma unei astfel de evaluări, precum și dreptul de a contesta decizia. O astfel de măsură nu ar trebui să se refere la un copil.

Pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată, având în vedere circumstanțele specifice și contextul în care sunt prelucrate datele cu caracter personal, operatorul ar trebui să utilizeze proceduri matematice sau statistice adecvate pentru crearea de profiluri, să implementeze măsuri tehnice și organizatorice adecvate pentru a asigura în special faptul că factorii care duc la inexactități ale datelor cu caracter personal sunt corecți și că riscul de erori este redus la minimum, precum și să securizeze datele cu caracter personal într-un mod care să țină seama de pericolele potențiale la adresa intereselor și drepturilor persoanei vizate și să prevină, printre altele, efectele discriminatorii împotriva persoanelor pe motiv de rasă sau origine etnică, opinii politice, religie sau convingeri, apartenență sindicală, caracteristici genetice, stare de sănătate sau orientare sexuală sau prelucrări care să ducă la măsuri care să aibă astfel de efecte. Procesul decizional automatizat și crearea de profiluri pe baza unor categorii speciale de date cu caracter personal ar trebui permise numai în condiții specifice.

(72) Crearea de profiluri este supusă normelor prezentului regulament care reglementează prelucrarea datelor cu caracter personal, precum temeiurile juridice ale prelucrării sau principiile de protecție a datelor. Comitetul european pentru protecția datelor instituit prin prezentul regulament ("comitetul") ar trebui să poată emite orientări în acest context.

(73) Dreptul Uniunii sau dreptul intern poate impune restricții în privința unor principii specifice, în privința dreptului de informare, a dreptului de acces la datele cu caracter personal și de rectificare sau ștergere a acestora, în privința dreptului la portabilitatea datelor, a dreptului la opoziție, a deciziilor bazate pe crearea de profiluri, precum și în privința comunicării unei încălcări a securității datelor cu caracter personal persoanei vizate și a anumitor obligații conexe ale operatorilor, în măsura în care acest lucru este necesar și proporțional într-o societate democratică pentru a se garanta siguranța publică, inclusiv protecția vieții oamenilor, în special ca răspuns la dezastre naturale sau provocate de

om, prevenirea, investigarea și urmărirea penală a infracțiunilor sau executarea pedepselor, inclusiv protejarea împotriva amenințărilor la adresa siguranței publice sau împotriva încălcării eticii în cazul profesiilor reglementate și prevenirea acestora, alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, menținerea de registre publice din motive de interes public general, prelucrarea ulterioară a datelor cu caracter personal arhivate pentru a transmite informații specifice legate de comportamentul politic în perioada regimurilor fostelor state totalitare, protecția persoanei vizate sau a drepturilor și libertăților unor terți, inclusiv protecția socială, sănătatea publică și scopurile umanitare. Aceste restricții ar trebui să fie conforme cu cerințele prevăzute de [cartă](#) și de [Convenția](#) europeană pentru apărarea drepturilor omului și a libertăților fundamentale.

(74) Ar trebui să se stabilească responsabilitatea și răspunderea operatorului pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său. În special, operatorul ar trebui să fie obligat să implementeze măsuri adecvate și eficiente și să fie în măsură să demonstreze conformitatea activităților de prelucrare cu prezentul regulament, inclusiv eficacitatea măsurilor. Aceste măsuri ar trebui să țină seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul pentru drepturile și libertățile persoanelor fizice.

(75) Riscul pentru drepturile și libertățile persoanelor fizice, prezentând grade diferite de probabilitate de materializare și de gravitate, poate fi rezultatul unei prelucrări a datelor cu caracter personal care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care: prelucrarea poate conduce la discriminare, furt sau fraudă a identității, pierdere financiară, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional, inversarea neautorizată a pseudonimizării sau la orice alt dezavantaj semnificativ de natură economică sau socială; persoanele vizate ar putea fi private de drepturile și libertățile lor sau împiedicate să-și exercite controlul asupra datelor lor cu caracter personal; datele cu caracter personal prelucrate sunt date care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența sindicală; sunt prelucrate date genetice, date privind sănătatea sau date privind viața sexuală sau privind condamnările penale și infracțiunile sau măsurile de securitate conexe; sunt evaluate aspecte de natură personală, în special analizarea sau previzionarea unor aspecte privind randamentul la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările, în scopul de a se crea sau de a se utiliza profiluri personale; sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale unor copii; sau prelucrarea implică un volum mare de date cu caracter personal și afectează un număr larg de persoane vizate.

(76) Probabilitatea de a se materializa și gravitatea riscului pentru drepturile și libertățile persoanei vizate ar trebui să fie determinate în funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor cu caracter personal. Riscul ar trebui apreciat pe baza unei evaluări obiective prin care se stabilește dacă operațiunile de prelucrare a datelor prezintă un risc sau un risc ridicat.

(77) Orientări pentru implementarea unor măsuri adecvate și pentru demonstrarea conformității de către operator sau persoana împuternicită de operator, mai ales în ceea ce privește identificarea riscului legat de prelucrare, evaluarea acestuia din punctul de vedere al originii, naturii, probabilității de a se

materializa și al gravității, precum și identificarea bunelor practici pentru atenuarea riscului ar putea fi oferite în special prin coduri de conduită aprobate, certificări aprobate, orientări ale comitetului sau prin indicații furnizate de un responsabil cu protecția datelor. Comitetul poate, de asemenea, să emită orientări cu privire la operațiunile de prelucrare care sunt considerate puțin susceptibile de a genera un risc ridicat pentru drepturile și libertățile persoanelor fizice și să indice măsurile care se pot dovedi suficiente în asemenea cazuri pentru a aborda un astfel de risc.

(78) Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare pentru a se asigura îndeplinirea cerințelor din prezentul regulament. Pentru a fi în măsură să demonstreze conformitatea cu prezentul regulament, operatorul ar trebui să adopte politici interne și să pună în aplicare măsuri care să respecte în special principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor. Astfel de măsuri ar putea consta, printre altele, în reducerea la minimum a prelucrării datelor cu caracter personal, pseudonimizarea acestor date cât mai curând posibil, transparența în ceea ce privește funcțiile și prelucrarea datelor cu caracter personal, abilitarea persoanei vizate să monitorizeze prelucrarea datelor, abilitarea operatorului să creeze elemente de siguranță și să le îmbunătățească. Atunci când elaborează, proiectează, selectează și utilizează aplicații, servicii și produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează date cu caracter personal pentru a-și îndeplini rolul, producătorii acestor produse și furnizorii acestor servicii și aplicații ar trebui să fie încurajați să aibă în vedere dreptul la protecția datelor la momentul elaborării și proiectării unor astfel de produse, servicii și aplicații și, ținând cont de stadiul actual al dezvoltării, să se asigure că operatorii și persoanele împuternicite de operatori sunt în măsură să își îndeplinească obligațiile referitoare la protecția datelor. Principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor ar trebui să fie luate în considerare și în contextul licitațiilor publice.

(79) Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și a persoanelor împuternicite de operator, inclusiv în ceea ce privește monitorizarea de către autoritățile de supraveghere și măsurile adoptate de acestea, necesită o atribuire clară a responsabilităților în temeiul prezentului regulament, inclusiv în cazul în care un operator stabilește scopurile și mijloacele prelucrării împreună cu alți operatori sau în cazul în care o operațiune de prelucrare este efectuată în numele unui operator.

(80) Atunci când un operator sau o persoană împuternicită de operator care nu este stabilită în Uniune prelucrează date cu caracter personal ale unor persoane vizate care se află pe teritoriul Uniunii, iar activitățile sale de prelucrare au legătură cu oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată, sau cu monitorizarea comportamentului unor persoane vizate dacă acesta se manifestă în cadrul Uniunii, operatorul sau persoana împuternicită de operator ar trebui să desemneze un reprezentant, cu excepția cazului în care prelucrarea are caracter ocazional, nu include prelucrarea pe scară largă a unor categorii speciale de date cu caracter personal și nici prelucrarea de date referitoare la condamnări penale și la infracțiuni, și este puțin susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice, având în vedere natura, contextul, domeniul de aplicare și scopurile prelucrării,

precum și a cazului în care operatorul este o autoritate publică sau un organism public. Reprezentantul ar trebui să acționeze în numele operatorului sau al persoanei împuternicite de operator, putând fi contactat de orice autoritate de supraveghere. Reprezentantul ar trebui desemnat în mod explicit, printr-un mandat scris al operatorului sau al persoanei împuternicite de operator, să acționeze în numele acestuia (acesteia) în ceea ce privește obligațiile lor în temeiul prezentului regulament. Desemnarea unui astfel de reprezentant nu aduce atingere responsabilității sau răspunderii operatorului sau a persoanei împuternicite de operator în temeiul prezentului regulament. Un astfel de reprezentant ar trebui să își îndeplinească sarcinile în conformitate cu mandatul primit de la operator sau de la persoana împuternicită de operator, inclusiv să coopereze cu autoritățile de supraveghere competente în ceea ce privește orice acțiune întreprinsă pentru a asigura respectarea prezentului regulament. Reprezentantul desemnat ar trebui să fie supus unor proceduri de asigurare a respectării legii în cazul nerespectării prezentului regulament de către operator sau de către persoana împuternicită de operator.

(81) Pentru a asigura respectarea cerințelor impuse de prezentul regulament în ceea ce privește prelucrarea care trebuie efectuată în numele operatorului de către persoana împuternicită de operator, atunci când atribuie activități de prelucrare unei persoane împuternicite de operator, acesta din urmă ar trebui să utilizeze numai persoane împuternicite care oferă garanții suficiente, în special în ceea ce privește cunoștințele de specialitate, fiabilitatea și resursele, pentru a implementa măsuri tehnice și organizatorice care îndeplinesc cerințele impuse de prezentul regulament, inclusiv pentru securitatea prelucrării. Aderarea de către persoana împuternicită de operator la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate fi utilizată drept element care să demonstreze respectarea obligațiilor de către operator. Efectuarea prelucrării de către o persoană împuternicită de un operator ar trebui să fie reglementată printr-un contract sau un alt tip de act juridic, în temeiul dreptului Uniunii sau al dreptului intern, care creează obligații pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopurile prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate, și ar trebui să țină seama de sarcinile și responsabilitățile specifice ale persoanei împuternicite de operator în contextul prelucrării care trebuie efectuată, precum și de riscul pentru drepturile și libertățile persoanei vizate. Operatorul și persoana împuternicită de operator pot alege să utilizeze un contract individual sau clauze contractuale standard care sunt adoptate fie direct de Comisie, fie de o autoritate de supraveghere în conformitate cu mecanismul de asigurare a coerenței și apoi adoptate de Comisie. După finalizarea prelucrării în numele operatorului, persoana împuternicită de operator ar trebui să returneze sau să șteargă, în funcție de opțiunea operatorului, datele cu caracter personal, cu excepția cazului în care există o cerință de stocare a datelor cu caracter personal în temeiul dreptului Uniunii sau al dreptului intern care instituie obligații pentru persoana împuternicită de operator.

(82) În vederea demonstrării conformității cu prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să păstreze evidențe ale activităților de prelucrare aflate în responsabilitatea sa. Fiecare operator și fiecare persoană împuternicită de operator ar trebui să aibă obligația de a coopera cu autoritatea de supraveghere și de a pune la dispoziția acesteia, la cerere,

aceste evidențe, pentru a putea fi utilizate în scopul monitorizării operațiunilor de prelucrare respective.

(83) În vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să evalueze riscurile inerente prelucrării și să implementeze măsuri pentru atenuarea acestor riscuri, cum ar fi criptarea. Măsurile respective ar trebui să asigure un nivel corespunzător de securitate, inclusiv confidențialitatea, luând în considerare stadiul actual al dezvoltării și costurile implementării în raport cu riscurile și cu natura datelor cu caracter personal a căror protecție trebuie asigurată. La evaluarea riscului pentru securitatea datelor cu caracter personal, ar trebui să se acorde atenție riscurilor pe care le prezintă prelucrarea datelor, cum ar fi distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, în mod accidental sau ilegal, care pot duce în special la prejudicii fizice, materiale sau morale.

(84) Pentru a favoriza respectarea dispozițiilor prezentului regulament în cazurile în care operațiunile de prelucrare sunt susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul ar trebui să fie responsabil de efectuarea unei evaluări a impactului asupra protecției datelor, care să estimeze, în special, originea, natura, specificitatea și gravitatea acestui risc. Rezultatul evaluării ar trebui luat în considerare la stabilirea măsurilor adecvate care trebuie luate pentru a demonstra că prelucrarea datelor cu caracter personal respectă prezentul regulament. În cazul în care o evaluare a impactului asupra protecției datelor arată că operațiunile de prelucrare implică un risc ridicat, pe care operatorul nu îl poate atenua prin măsuri adecvate sub aspectul tehnologiei disponibile și al costurilor implementării, ar trebui să aibă loc o consultare a autorității de supraveghere înainte de prelucrare.

(85) Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză. Prin urmare, de îndată ce a luat cunoștință de producerea unei încălcări a securității datelor cu caracter personal, operatorul ar trebui să notifice această încălcare autorității de supraveghere, fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore după ce a luat la cunoștință de existența acesteia, cu excepția cazului în care operatorul este în măsură să demonstreze, în conformitate cu principiul responsabilității, că încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. Atunci când notificarea nu se poate realiza în termen de 72 de ore, aceasta ar trebui să cuprindă motivele întârzierii, iar informațiile pot fi furnizate treptat, fără altă întârziere.

(86) Operatorul ar trebui să comunice persoanei vizate o încălcare a securității datelor cu caracter personal, fără întârzieri nejustificate, atunci când încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanei fizice, pentru a-i permite să ia măsurile de precauție necesare. Comunicarea ar trebui să descrie natura încălcării securității datelor cu caracter personal și să cuprindă

recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative. Comunicările către persoanele vizate ar trebui efectuate în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu autoritatea de supraveghere, respectându-se orientările furnizate de aceasta sau de alte autorități competente, cum ar fi autoritățile de aplicare a legii. De exemplu, necesitatea de a atenua un risc imediat de producere a unui prejudiciu ar presupune comunicarea cu promptitudine către persoanele vizate, în timp ce necesitatea de a implementa măsuri corespunzătoare împotriva încălcării în continuare a securității datelor cu caracter personal sau împotriva unor încălcări similare ale securității datelor cu caracter personal ar putea justifica un termen mai îndelungat pentru comunicare.

(87) Ar trebui să se stabilească dacă au fost implementate toate măsurile tehnologice de protecție și organizatorice corespunzătoare în scopul de a se stabili imediat dacă s-a produs o încălcare a securității datelor cu caracter personal și de a se informa cu promptitudine autoritatea de supraveghere și persoana vizată. Faptul că notificarea a fost efectuată fără întârziere nejustificată ar trebui stabilit luându-se în considerare, în special, natura și gravitatea încălcării securității datelor cu caracter personal, precum și consecințele și efectele negative ale acesteia asupra persoanei vizate. Această notificare poate conduce la o intervenție a autorității de supraveghere, în conformitate cu sarcinile și competențele specificate în prezentul regulament.

(88) La stabilirea de norme detaliate privind formatul și procedurile aplicabile notificării referitoare la încălcările securității datelor cu caracter personal, ar trebui să se acorde atenția cuvenită circumstanțelor în care a avut loc încălcarea, stabilindu-se inclusiv dacă protecția datelor cu caracter personal a fost sau nu a fost asigurată prin măsuri tehnice de protecție corespunzătoare, care să limiteze efectiv probabilitatea fraudării identității sau a altor forme de utilizare abuzivă. În plus, astfel de norme și proceduri ar trebui să țină cont de interesele legitime ale autorităților de aplicare a legii în cazurile în care divulgarea timpurie ar putea îngreuna în mod inutil investigarea circumstanțelor în care a avut loc o încălcare a datelor cu caracter personal.

(89) Directiva [95/46/CE](#) a prevăzut o obligație generală de a notifica prelucrarea datelor cu caracter personal autorităților de supraveghere. Cu toate că obligația respectivă generează sarcini administrative și financiare, aceasta nu a contribuit întotdeauna la îmbunătățirea protecției datelor cu caracter personal. Prin urmare, astfel de obligații de notificare generală nediferențiată ar trebui să fie abrogate și înlocuite cu proceduri și mecanisme eficace care să pună accentul, în schimb, pe acele tipuri de operațiuni de prelucrare susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice prin însăși natura lor, prin domeniul lor de aplicare, prin contextul și prin scopurile lor. Astfel de tipuri de operațiuni de prelucrare pot fi cele care presupun, în special, utilizarea unor noi tehnologii sau care reprezintă un nou tip de operațiuni, pentru care nicio evaluare a impactului asupra protecției datelor nu a fost efectuată anterior de către operator ori care devin necesare dată fiind perioada de timp care s-a scurs de la prelucrarea inițială.

(90) În astfel de cazuri, operatorul ar trebui să efectueze, înainte de prelucrare, o evaluare a impactului asupra protecției datelor, în scopul evaluării gradului specific de probabilitate a materializării riscului ridicat și gravitatea acestuia, având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și sursele riscului. Respectiva evaluare a impactului ar trebui să includă, în special, măsurile, garanțiile și mecanismele avute în vedere pentru atenuarea riscului respectiv, pentru

asigurarea protecției datelor cu caracter personal și pentru demonstrarea conformității cu prezentul regulament.

(91) Aceasta ar trebui să se aplice, în special, operațiunilor de prelucrare la scară largă, care au drept obiectiv prelucrarea unui volum considerabil de date cu caracter personal la nivel regional, național sau supranațional, care ar putea afecta un număr mare de persoane vizate și care sunt susceptibile de a genera un risc ridicat, de exemplu, din cauza sensibilității lor, în cazul în care, în conformitate cu nivelul atins al cunoștințelor tehnologice, se folosește la scară largă o tehnologie nouă, precum și altor operațiuni de prelucrare care generează un risc ridicat pentru drepturile și libertățile persoanelor vizate, în special în cazul în care operațiunile respective limitează capacitatea persoanelor vizate de a-și exercita drepturile. Ar trebui efectuată o evaluare a impactului asupra protecției datelor și în situațiile în care datele cu caracter personal sunt prelucrate în scopul luării de decizii care vizează anumite persoane fizice în urma unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, pe baza creării de profiluri pentru datele respective, sau în urma prelucrării unor categorii speciale de date cu caracter personal, a unor date biometrice sau a unor date privind condamnările penale și infracțiunile sau măsurile de securitate conexe. Este la fel de necesară o evaluare a impactului asupra protecției datelor pentru monitorizarea la scară largă a zonelor accesibile publicului, mai ales în cazul utilizării dispozitivelor optoelectronice sau pentru orice alte operațiuni în cazul în care autoritatea de supraveghere competentă consideră că prelucrarea este susceptibilă de a genera un risc ridicat pentru drepturile și libertățile persoanelor vizate, în special deoarece acestea împiedică persoanele vizate să exercite un drept sau să utilizeze un serviciu ori un contract, sau deoarece acestea sunt efectuate în mod sistematic la scară largă. Prelucrarea datelor cu caracter personal nu ar trebui considerată a fi la scară largă în cazul în care prelucrarea se referă la date cu caracter personal de la pacienți sau clienți de către un anumit medic, un alt profesionist în domeniul sănătății sau un avocat. În aceste cazuri, o evaluare a impactului asupra protecției datelor nu ar trebui să fie obligatorie.

(92) În unele circumstanțe ar putea fi rezonabil și util din punct de vedere economic ca o evaluare a impactului asupra protecției datelor să aibă o perspectivă mai extinsă decât cea a unui singur proiect, de exemplu în cazul în care autorități sau organisme publice intenționează să instituie o aplicație sau o platformă de prelucrare comună sau în cazul în care mai mulți operatori preconizează să introducă o aplicație comună sau un mediu de prelucrare comun în cadrul unui sector sau segment industrial sau pentru o activitate orizontală utilizată la scară largă.

(93) În contextul adoptării legislației naționale pe care se bazează îndeplinirea sarcinilor autorității publice sau ale organismului public și care reglementează operațiunea sau seria de operațiuni de prelucrare în cauză, statele membre pot considera că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.

(94) În cazul în care o evaluare a impactului asupra protecției datelor arată că prelucrarea ar genera, în absența garanțiilor, măsurilor de securitate și mecanismelor de atenuare a riscului, un risc ridicat pentru drepturile și libertățile persoanelor fizice, iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile și al costurilor implementării, autoritatea de supraveghere ar trebui să fie consultată înainte de începerea activităților de prelucrare. Un astfel de risc

ridicat este susceptibil să fie generat de anumite tipuri de prelucrare, precum și de amploarea și frecvența prelucrării, care pot duce și la producerea unor prejudicii sau pot atinge drepturile și libertățile persoanelor fizice. Autoritatea de supraveghere ar trebui să răspundă cererii de consultare într-un anumit termen. Cu toate acestea, lipsa unei reacții din partea autorității de supraveghere în termenul respectiv ar trebui să nu aducă atingere niciunei intervenții a autorității de supraveghere în conformitate cu sarcinile și competențele sale prevăzute în prezentul regulament, inclusiv competența de a interzice operațiuni de prelucrare. Ca parte a acestui proces de consultare, rezultatul unei evaluări a impactului asupra protecției datelor efectuate cu privire la prelucrarea în cauză poate fi transmis autorității de supraveghere, în special măsurile avute în vedere pentru a atenua riscul pentru drepturile și libertățile persoanelor fizice.

(95) Persoana împuternicită de operator ar trebui să acorde asistență operatorului, dacă este necesar și la cerere, la asigurarea respectării obligațiilor care decurg din realizarea de evaluări ale impactului asupra protecției datelor și din consultarea prealabilă a autorității de supraveghere.

(96) În timpul elaborării unei măsuri legislative sau de reglementare care prevede prelucrarea unor date cu caracter personal ar trebui, de asemenea, să aibă loc o consultare a autorității de supraveghere, pentru a garanta conformitatea prelucrării avute în vedere cu prezentul regulament și, în special, pentru a atenua riscul la care este expusă persoana vizată.

(97) În cazul în care prelucrarea este efectuată de o autoritate publică, cu excepția instanțelor sau a autorităților judiciare independente atunci când acționează în calitatea lor judiciară, în cazul în care, în sectorul privat, prelucrarea este efectuată de un operator a cărui activitate principală constă în operațiuni de prelucrare care necesită o monitorizare regulată și sistematică a persoanelor vizate pe scară largă, sau în cazul în care activitatea principală a operatorului sau a persoanei împuternicite de operator constă în prelucrarea pe scară largă de categorii speciale de date cu caracter personal și de date privind condamnările penale și infracțiunile, o persoană care deține cunoștințe de specialitate în materie de legislație și practici privind protecția datelor ar trebui să acorde asistență operatorului sau persoanei împuternicite de operator pentru monitorizarea conformității, la nivel intern, cu prezentul regulament. În sectorul privat, activitățile principale ale unui operator se referă la activitățile sale de bază, și nu la prelucrarea datelor cu caracter personal drept activități auxiliare. Nivelul necesar al cunoștințelor de specialitate ar trebui să fie stabilit în special în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate de operator sau de persoana împuternicită de operator. Acești responsabili cu protecția datelor, indiferent dacă sunt sau nu angajați ai operatorului, ar trebui să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent.

(98) Asociațiile sau alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori ar trebui încurajate să elaboreze coduri de conduită, în limitele prezentului regulament, astfel încât să se faciliteze aplicarea efectivă a prezentului regulament, luându-se în considerare caracteristicile specifice ale prelucrării efectuate în anumite sectoare și necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii. În special, astfel de coduri de conduită ar putea să ajusteze obligațiile operatorilor și ale persoanelor împuternicite de operatori, ținând seama de

riscul aferent prelucrării care este susceptibil de a fi generat pentru drepturile și libertățile persoanelor fizice.

(99) Atunci când elaborează un cod de conduită sau când modifică sau extind un astfel de cod, asociațiile și alte organisme care reprezintă categorii de operatori sau persoane împuternicite de operatori ar trebui să consulte părțile implicate relevante, inclusiv persoanele vizate, dacă este fezabil, și să ia în considerare contribuțiile transmise și opiniile exprimate în cadrul unor astfel de consultări.

(100) Pentru a se îmbunătăți transparența și conformitatea cu prezentul regulament, ar trebui să se încurajeze instituirea de mecanisme de certificare, precum și de sigilii și mărci în materie de protecție a datelor, care să permită persoanelor vizate să evalueze rapid nivelul de protecție a datelor aferent produselor și serviciilor relevante.

(101) Fluxurile de date cu caracter personal către și dinspre țări situate în afara Uniunii și organizații internaționale sunt necesare pentru dezvoltarea comerțului internațional și a cooperării internaționale. Creșterea acestor fluxuri a generat noi provocări și preocupări cu privire la protecția datelor cu caracter personal. Cu toate acestea, în cazul în care se transferă date cu caracter personal din Uniune către operatori, persoane împuternicite de operatori sau alți destinatari din țări terțe sau organizații internaționale, nivelul de protecție a persoanelor fizice asigurat în Uniune prin prezentul regulament nu ar trebui să fie diminuat, inclusiv în cazurile de transferuri ulterioare de date cu caracter personal dinspre țara terță sau organizația internațională către operatori, persoane împuternicite de operatori din aceeași sau dintr-o altă țară terță sau organizație internațională. În orice caz, transferurile către țări terțe și organizații internaționale pot fi desfășurate numai în conformitate deplină cu prezentul regulament. Un transfer ar putea avea loc numai dacă, sub rezerva respectării celorlalte dispoziții ale prezentului regulament, operatorul sau persoana împuternicită de operator îndeplinește condițiile prevăzute de dispozițiile prezentului regulament privind transferul de date cu caracter personal către țări terțe sau organizații internaționale.

(102) Prezentul regulament nu aduce atingere acordurilor internaționale încheiate între Uniune și țări terțe în vederea reglementării transferului de date cu caracter personal, inclusiv garanții adecvate pentru persoanele vizate. Statele membre pot încheia acorduri internaționale care implică transferul de date cu caracter personal către țări terțe sau organizații internaționale, în măsura în care astfel de acorduri nu afectează prezentul regulament și nici alte dispoziții din dreptul Uniunii și includ un nivel corespunzător de protecție a drepturilor fundamentale ale persoanelor vizate.

(103) Comisia poate decide, cu efect în întreaga Uniune, că o țară terță, un teritoriu sau un anumit sector dintr-o țară terță sau o organizație internațională oferă un nivel adecvat de protecție a datelor, asigurând astfel securitate juridică și uniformitate în Uniune în ceea ce privește țara terță sau organizația internațională care este considerată a furniza un astfel de nivel de protecție. În aceste cazuri, transferurile de date cu caracter personal către țara terță sau organizația internațională respectivă pot avea loc fără a fi necesar să se obțină autorizări suplimentare. De asemenea, Comisia poate să decidă, după trimiterea unei notificări și a unei justificări complete țării terțe sau organizației internaționale, să anuleze o astfel de decizie.

(104) În conformitate cu valorile fundamentale pe care se întemeiază Uniunea, în special protecția drepturilor omului, Comisia ar trebui, în evaluarea sa referitoare la țara terță sau la un teritoriu sau la un

sector specificat dintr-o țară terță, să ia în considerare modul în care aceasta respectă statul de drept, accesul la justiție, precum și normele și standardele internaționale în materie de drepturi ale omului și legislația sa generală și sectorială, inclusiv legislația privind securitatea publică, apărarea și securitatea națională, precum și ordinea publică și dreptul penal. Adoptarea unei decizii privind caracterul adecvat al nivelului de protecție pentru un teritoriu sau un sector specificat dintr-o țară terță ar trebui să țină seama de criterii clare și obiective, cum ar fi activitățile specifice de prelucrare și domeniul de aplicare al standardelor legale aplicabile și legislația în vigoare în țara terță respectivă. Țara terță ar trebui să ofere garanții care să asigure un nivel adecvat de protecție, echivalent în esență cu cel asigurat în cadrul Uniunii, în special atunci când datele cu caracter personal sunt prelucrate în unul sau mai multe sectoare specifice. În special, țara terță ar trebui să asigure o supraveghere efectivă independentă în materie de protecție a datelor și să prevadă mecanisme de cooperare cu autoritățile statelor membre de protecție a datelor, iar persoanele vizate ar trebui să beneficieze de drepturi efective și opozabile și de reparații efective pe cale administrativă și judiciară.

(105) Pe lângă angajamentele internaționale asumate de țara terță sau de organizația internațională, Comisia ar trebui să țină seama de obligațiile care decurg din participarea țării terțe sau a organizației internaționale la sistemele multilaterale sau regionale, în special în ceea ce privește protecția datelor cu caracter personal, precum și de punerea în aplicare a unor astfel de obligații. În special, ar trebui să fie luată în considerare aderarea țării terțe la [Convenția](#) Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal și protocolul adițional la aceasta. Comisia ar trebui să consulte comitetul atunci când evaluează nivelul de protecție din țările terțe sau din organizațiile internaționale.

(106) Comisia ar trebui să monitorizeze funcționarea deciziilor privind nivelul de protecție dintr-o țară terță sau un teritoriu sau un anumit sector dintr-o țară terță sau dintr-o organizație internațională și să monitorizeze funcționarea deciziilor adoptate în temeiul articolului 25 [alineatul \(6\)](#) sau al articolului 26 [alineatul \(4\)](#) din Directiva 95/46/CE. În deciziile sale privind caracterul adecvat al nivelului de protecție, Comisia ar trebui să prevadă un mecanism de revizuire periodică a modului lor de funcționare. Această revizuire periodică ar trebui să fie efectuată în consultare cu țara terță sau organizația internațională în cauză și ar trebui să ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională. În scopul monitorizării și al efectuării revizuirilor periodice, Comisia ar trebui să ia în considerare opiniile și constatările Parlamentului European și ale Consiliului, precum și ale altor organisme și surse relevante. Comisia ar trebui să evalueze, într-un termen rezonabil, funcționarea deciziilor din urmă și să raporteze toate constatările relevante comitetului, în sensul Regulamentului (UE) [nr. 182/2011](#) al Parlamentului European și al Consiliului, după cum s-a stabilit în temeiul prezentului regulament, Parlamentului European și Consiliului.

(107) Comisia poate să recunoască faptul că o țară terță, un teritoriu sau un sector specificat dintr-o țară terță sau o organizație internațională nu mai asigură un nivel adecvat de protecție a datelor. În consecință, transferul de date cu caracter personal către țara terță sau organizația internațională respectivă ar trebui să fie interzis, cu excepția cazului în care sunt îndeplinite cerințele prevăzute în prezentul regulament privind transferurile în baza unor garanții adecvate, inclusiv regulile corporatiste obligatorii și derogările de la situațiile specifice. În acest caz, ar trebui să se prevadă dispoziții pentru

consultări între Comisie și astfel de țări terțe sau organizații internaționale. Comisia ar trebui ca, în timp util, să informeze țara terță sau organizația internațională cu privire la aceste motive și să inițieze consultări cu aceasta pentru remedierea situației.

(108) În absența unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator ar trebui să adopte măsuri pentru a compensa lipsa protecției datelor într-o țară terță prin intermediul unor garanții adecvate pentru persoana vizată. Astfel de garanții adecvate pot consta în utilizarea regulilor corporatiste obligatorii, a clauzelor standard de protecție a datelor adoptate de Comisie, a clauzelor standard de protecție a datelor adoptate de o autoritate de supraveghere sau a clauzelor contractuale autorizate de o autoritate de supraveghere. Respectivetele garanții ar trebui să asigure respectarea cerințelor în materie de protecție a datelor și drepturi ale persoanelor vizate corespunzătoare prelucrării în interiorul Uniunii, inclusiv disponibilitatea unor drepturi opozabile ale persoanelor vizate și a unor căi de atac eficiente, printre care dreptul de acces la reparații efective pe cale administrativă sau judiciară și dreptul de a solicita despăgubiri, în Uniune sau într-o țară terță. Acestea ar trebui să se refere în special la respectarea principiilor generale privind prelucrarea datelor cu caracter personal: principiul protecției datelor începând cu momentul conceperii și principiul protecției implicite a datelor. Transferurile pot fi efectuate și de către autoritățile sau organismele publice cu autorități sau organisme publice în țări terțe sau cu organizații internaționale cu atribuții și funcții corespunzătoare, inclusiv pe baza dispozițiilor care prevăd drepturi opozabile și efective pentru persoanele vizate, care trebuie introduse în acordurile administrative, cum ar fi un memorandum de înțelegere. Autorizația din partea autorității de supraveghere competente ar trebui obținută atunci când garanțiile sunt oferite în cadrul unor acorduri administrative fără caracter juridic obligatoriu.

(109) Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecție a datelor, adoptate de Comisie sau de o autoritate de supraveghere, nu ar trebui să împiedice operatorii sau persoanele împuternicite de aceștia să includă clauzele standard în materie de protecție a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator și o altă persoană împuternicită de operator, și nici să adauge alte clauze sau garanții suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de o autoritate de supraveghere sau nu prejudiciază drepturile sau libertățile fundamentale ale persoanelor vizate. Operatorii și persoanele împuternicite de operatori ar trebui să fie încurajați să ofere garanții suplimentare prin intermediul unor angajamente contractuale care să completeze clauzele standard în materie de protecție.

(110) Un grup de întreprinderi sau un grup de întreprinderi implicat într-o activitate economică comună ar trebui să poată utiliza regulile corporatiste obligatorii aprobate pentru transferurile sale internaționale dinspre Uniune către organizații din cadrul aceluiași grup de întreprinderi sau grup de întreprinderi implicate într-o activitate economică comună, cu condiția ca astfel de reguli corporatiste să includă toate principiile esențiale și drepturile opozabile în scopul asigurării unor garanții adecvate pentru transferurile sau categoriile de transferuri de date cu caracter personal.

(111) Ar trebui să se prevadă posibilitatea de a se efectua transferuri în anumite circumstanțe în care persoana vizată și-a dat consimțământul explicit, în care transferul este ocazional și necesar în legătură

cu un contract sau cu o acțiune în justiție, indiferent dacă este în contextul unei proceduri judiciare sau în contextul unei proceduri administrative sau extrajudiciare, inclusiv în cadrul procedurilor înaintate organismelor de reglementare. De asemenea, ar trebui să se prevadă posibilitatea de a se efectua transferuri în cazul în care motive importante de interes public stabilite de dreptul Uniunii sau de dreptul intern impun acest lucru sau în cazul în care transferul se efectuează dintr-un registru instituit prin lege și destinat să fie consultat de către public sau de către persoane care au un interes legitim. În acest ultim caz, un astfel de transfer nu ar trebui să implice totalitatea datelor cu caracter personal sau ansamblul categoriilor de date conținute în registru, iar atunci când registrul este destinat să fie consultat de persoane care au un interes legitim, transferul ar trebui să fie efectuat doar la cererea persoanelor respective sau dacă acestea sunt destinatarii, luând pe deplin în considerare interesele și drepturile fundamentale ale persoanei vizate.

(112) Aceste derogări ar trebui să se aplice, în special, transferurilor de date solicitate și necesare din considerente importante de interes public, de exemplu în cazul schimbului internațional de date între autoritățile din domeniul concurenței, administrațiile fiscale sau vamale, între autoritățile de supraveghere financiară, între serviciile competente în materie de securitate socială sau de sănătate publică, de exemplu în cazul depistării punctelor de contact pentru bolile contagioase sau pentru reducerea și/sau eliminarea dopajului în sport. Un transfer de date cu caracter personal ar trebui, de asemenea, să fie considerat legal în cazul în care este necesar în scopul protejării unui interes care este esențial în interesele vitale ale persoanei vizate sau ale unei alte persoane, inclusiv pentru integritatea fizică sau pentru viața acesteia, în cazul în care persona vizată nu are capacitatea să își dea consimțământul. În absența unei decizii privind caracterul adecvat al nivelului de protecție, dreptul Uniunii sau dreptul intern poate, din considerente importante de interes public, stabili în mod expres limite asupra transferului unor categorii specifice de date către o țară terță sau o organizație internațională. Statele membre ar trebui să notifice Comisiei aceste dispoziții. Orice transfer către o organizație umanitară internațională al datelor cu caracter personal ale unei persoane vizate care se află în incapacitate fizică sau juridică de a își da consimțământul, în vederea îndeplinirii unei sarcini care decurge din Convențiile de la Geneva sau în vederea conformării cu dreptul internațional umanitar aplicabil în conflictele armate, ar putea fi considerat necesar pentru un motiv important de interes public sau pentru că este în interesul vital al persoanei vizate.

(113) Transferurile care pot fi considerate ca nefiind repetitive și care se referă doar la un număr limitat de persoane vizate, ar putea, de asemenea, să fie efectuate în scopul realizării intereselor legitime urmărite de operator, atunci când asupra respectivelor interese nu prevalează interesele sau drepturile și libertățile persoanei vizate și atunci când operatorul a evaluat toate circumstanțele aferente transferului de date. Operatorul ar trebui să acorde o atenție deosebită naturii datelor cu caracter personal, scopului și duratei operațiunii sau operațiunilor propuse de prelucrare, precum și situației din țara de origine, din țara terță și din țara de destinație finală și ar trebui să ofere garanții adecvate pentru protecția drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Astfel de transferuri ar trebui să fie posibile numai în cazurile reziduale în care nu se poate aplica niciunul dintre celelalte motive de transfer. În ceea ce privește scopurile de cercetare științifică sau istorică sau scopurile statistice, ar trebui să se ia în considerare așteptările

legitime ale societății cu privire la creșterea nivelului de cunoștințe. Operatorul ar trebui să informeze autoritatea de supraveghere și persoana vizată cu privire la transfer.

(114) În orice caz, atunci când Comisia nu a luat o decizie cu privire la nivelul adecvat de protecție a datelor dintr-o țară terță, operatorul sau persoana împuternicită de operator ar trebui să utilizeze soluții care să ofere persoanelor vizate drepturi opozabile și efective în ceea ce privește prelucrarea datelor lor în Uniune odată ce aceste date au fost transferate, astfel încât persoanele vizate să beneficieze în continuare de drepturi fundamentale și garanții.

(115) Unele țări terțe au adoptat legi, reglementări și alte acte juridice care au drept obiectiv să reglementeze în mod direct activitățile de prelucrare a datelor ale persoanelor fizice și juridice aflate sub jurisdicția statelor membre. Aceasta poate include hotărâri ale instanțelor judecătorești sau decizii ale autorităților administrative din țări terțe care solicită unui operator sau unei persoane împuternicite de operator să transfere sau să divulge date cu caracter personal și care nu se bazează pe un acord internațional, cum ar fi un tratat de asistență juridică reciprocă, în vigoare între țara terță solicitantă și Uniune sau un stat membru. Aplicarea extraterritorială a acestor legi, reglementări și alte acte juridice poate încălca dreptul internațional și poate împiedica asigurarea protecției persoanelor fizice asigurate în Uniune prin prezentul regulament. Transferurile ar trebui să fie permise numai în cazul îndeplinirii condițiilor prevăzute de prezentul regulament pentru un transfer către țări terțe. Acesta ar putea fi cazul, inter alia, atunci când divulgarea este necesară dintr-un motiv important de interes public recunoscut în dreptul Uniunii sau în dreptul intern care se aplică operatorului.

(116) Fluxul transfrontalier de date cu caracter personal în afara Uniunii poate expune unui risc sporit capacitatea persoanelor fizice de a-și exercita drepturile în materie de protecție a datelor, în special pentru a-și asigura protecția împotriva utilizării sau a divulgării ilegale a acestor informații. În același timp, autoritățile de supraveghere pot constata că se află în imposibilitatea de a trata plângeri sau de a efectua investigații referitoare la activitățile desfășurate în afara frontierelor lor. Eforturile acestora de a conlucra în context transfrontalier pot fi, de asemenea, îngreunate de insuficiența competențelor de prevenire sau remediere, de caracterul eterogen al regimurilor juridice și de existența unor obstacole de ordin practic, cum ar fi constrângerile în materie de resurse. Prin urmare, este necesar să se promoveze o cooperare mai strânsă între autoritățile de supraveghere a protecției datelor pentru a putea face schimb de informații și a desfășura investigații împreună cu omologii lor internaționali. În scopul elaborării de mecanisme de cooperare internațională pentru a facilita și a oferi asistență internațională reciprocă în asigurarea aplicării legislației din domeniul protecției datelor cu caracter personal, Comisia și autoritățile de supraveghere ar trebui să facă schimb de informații și să coopereze în cadrul activităților legate de exercitarea competențelor lor cu autoritățile competente din țări terțe, pe bază de reciprocitate și în conformitate cu prezentul regulament.

(117) Instituirea în statele membre a unor autorități de supraveghere, împuternicite să își îndeplinească sarcinile și să își exercite competențele în deplină independență, este un element esențial al protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Statele membre ar trebui să poată institui mai multe autorități de supraveghere, pentru a reflecta structura lor constituțională, organizatorică și administrativă.

(118) Independența autorităților de supraveghere nu ar trebui să însemne că autoritățile de supraveghere nu pot face obiectul unor mecanisme de control sau de monitorizare în ceea ce privește cheltuielile acestora sau unui control jurisdicțional.

(119) În cazul în care un stat membru instituie mai multe autorități de supraveghere, acesta ar trebui să stabilească prin lege mecanisme care să asigure participarea efectivă a autorităților de supraveghere respective la mecanismul pentru asigurarea coerenței. Statul membru respectiv ar trebui, în special, să desemneze autoritatea de supraveghere care îndeplinește funcția de punct unic de contact pentru participarea efectivă a acestor autorități la mecanism, în scopul asigurării unei cooperări rapide și armonioase cu alte autorități de supraveghere, cu comitetul și cu Comisia.

(120) Fiecare autoritate de supraveghere ar trebui să beneficieze de resurse financiare și umane, de spațiile și de infrastructura necesare pentru îndeplinirea cu eficacitate a sarcinilor lor, inclusiv a celor legate de asistența reciprocă și cooperarea cu alte autorități de supraveghere în întreaga Uniune. Fiecare autoritate de supraveghere ar trebui să aibă un buget public anual separat, care poate face parte din bugetul general de stat sau național.

(121) Condițiile generale pentru membrul sau membrii autorității de supraveghere ar trebui stabilite de lege în fiecare stat membru și ar trebui, în special, să prevadă că respectivii membri sunt numiți printr-o procedură transparentă fie de parlamentul, de guvernul ori șeful de stat al statului membru pe baza unei propuneri din partea guvernului, a unui membru al guvernului, a parlamentului sau a unei camere a parlamentului, fie de către un organism independent împuternicit prin dreptul intern. În vederea asigurării independenței autorității de supraveghere, membrul sau membrii acesteia ar trebui să acționeze cu integritate, să nu întreprindă acțiuni incompatibile cu îndatoririle lor, iar, pe durata mandatului, ar trebui să nu desfășoare activități incompatibile, remunerate sau nu. Autoritatea de supraveghere ar trebui să aibă personal propriu, ales de autoritatea de supraveghere sau de un organism independent înființat în temeiul dreptului intern, care ar trebui să fie subordonat exclusiv membrului sau membrilor autorității de supraveghere.

(122) Fiecare autoritate de supraveghere ar trebui să aibă, pe teritoriul statului membru de care aparține, atribuția de a exercita competențele și de a îndeplini sarcinile cu care este investită în conformitate cu prezentul regulament. Aceasta ar trebui să includă în special prelucrarea în contextul activităților unui sediu al operatorului sau al persoanei împuternicite de operator pe teritoriul propriului stat membru, prelucrarea datelor cu caracter personal efectuată de autoritățile publice sau de organisme private care acționează în interes public, prelucrarea care afectează persoanele vizate de pe teritoriul său sau prelucrarea efectuată de către un operator sau o persoană împuternicită de operator care nu își are sediul în Uniune în cazul în care aceasta privește persoane vizate care își au reședința pe teritoriul său. Aceasta ar trebui să includă tratarea plângerilor depuse de o persoană vizată, efectuarea de investigații privind aplicarea prezentului regulament și promovarea informării publicului cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal.

(123) Autoritățile de supraveghere ar trebui să monitorizeze aplicarea dispozițiilor prevăzute de prezentul regulament și să contribuie la aplicarea coerentă a acestuia în întreaga Uniune, în scopul asigurării protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal și al facilitării liberei circulații a datelor cu caracter personal în interiorul pieței interne. În acest sens,

autoritățile de supraveghere ar trebui să coopereze reciproc, precum și cu Comisia, fără să fie necesar niciun acord între statele membre cu privire la acordarea de asistență reciprocă sau cu privire la respectiva cooperare.

(124) În cazul în care prelucrarea datelor cu caracter personal se desfășoară în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune, iar operatorul sau persoana împuternicită de operator are sedii în mai multe state membre, sau în cazul în care prelucrarea care se desfășoară în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator din Uniune afectează sau este susceptibilă să afecteze semnificativ persoane vizate din mai multe state membre, autoritatea de supraveghere a sediului principal al operatorului sau al persoanei împuternicite de operator ori a sediului unic al operatorului sau al persoanei împuternicite de operator ar trebui să acționeze în calitate de autoritate principală. Aceasta ar trebui să coopereze cu celelalte autorități vizate, pentru că operatorul sau persoana împuternicită de operator are un sediu pe teritoriul statului lor membru, pentru că persoanele vizate care își au reședința pe teritoriul lor sunt afectate în mod semnificativ sau pentru că le-a fost înaintată o plângere. De asemenea, în cazul în care o persoană vizată care nu își are reședința în statul membru respectiv a depus o plângere, autoritatea de supraveghere la care a fost depusă plângerea ar trebui, de asemenea, să fie o autoritate de supraveghere vizată. În cadrul sarcinilor sale de a emite orientări cu privire la orice chestiune referitoare la punerea în aplicare a prezentului regulament, comitetul ar trebui să poată emite orientări privind, în special, criteriile care trebuie luate în considerare pentru a se stabili dacă prelucrarea în cauză afectează în mod semnificativ persoane vizate din mai multe state membre și privind conținutul unei obiecții relevante și motivate.

(125) Autoritatea principală ar trebui să aibă competența de a adopta decizii obligatorii privind măsurile de aplicare a competențelor care îi sunt conferite în conformitate cu prezentul regulament. În calitatea sa de autoritate principală, autoritatea de supraveghere ar trebui să implice îndeaproape și să coordoneze activitățile autorităților de supraveghere vizate în procesul decizional. În cazurile în care decizia este de respingere parțială sau totală a plângerii din partea persoanei vizate, o asemenea decizie ar trebui adoptată de către autoritatea de supraveghere la care s-a depus plângerea.

(126) Decizia ar trebui convenită în comun de autoritatea de supraveghere principală și de autoritățile de supraveghere vizate și ar trebui să vizeze sediul principal sau sediul unic al operatorului sau al persoanei împuternicite de operator și să fie obligatorie pentru operator și pentru persoana împuternicită de operator. Operatorul sau persoana împuternicită de operator ar trebui să ia măsurile necesare pentru a asigura conformitatea cu prezentul regulament și punerea în aplicare a deciziei notificate de autoritatea de supraveghere principală sediului principal al operatorului sau al persoanei împuternicite de operator în ceea ce privește activitățile de prelucrare în Uniune.

(127) Fiecare autoritate de supraveghere care nu acționează ca autoritate de supraveghere principală ar trebui să aibă competența de a trata cazuri locale, în care operatorul sau persoana împuternicită de operator are sedii în mai multe state membre, dar obiectul respectivei prelucrări privește doar prelucrarea efectuată într-un singur stat membru și implicând doar persoane vizate din acel unic stat membru, de exemplu în cazul în care obiectul îl constituie prelucrarea datelor cu caracter personal ale angajaților în contextul specific legat de forța de muncă dintr-un stat membru. În astfel de cazuri,

autoritatea de supraveghere ar trebui să informeze fără întârziere autoritatea de supraveghere principală cu privire la această chestiune. După ce a fost informată, autoritatea de supraveghere principală ar trebui să decidă dacă va trata ea însăși cazul în temeiul dispoziției privind cooperarea între autoritatea de supraveghere principală și alte autorități de supraveghere vizate ("mecanismul ghișeului unic"), sau dacă autoritatea de supraveghere care a informat-o ar trebui să se ocupe de caz la nivel local. Atunci când decide dacă va trata cazul, autoritatea de supraveghere principală ar trebui să ia în considerare dacă există un sediu al operatorului sau al persoanei împuternicite de operator în statul membru al autorității de supraveghere care a informat-o, în vederea garantării respectării efective a unei decizii în ceea ce privește operatorul sau persoana împuternicită de operator. În cazul în care autoritatea de supraveghere principală decide să trateze cazul, autoritatea de supraveghere care a informat-o ar trebui să beneficieze de posibilitatea de a prezenta un proiect de decizie, de care autoritatea de supraveghere principală ar trebui să țină seama în cea mai mare măsură atunci când pregătește proiectul său de decizie în cadrul respectivului mecanism al ghișeului unic.

(128) Normele privind autoritatea de supraveghere principală și mecanismul ghișeului unic nu ar trebui să se aplice în cazul în care prelucrarea este efectuată de autorități publice sau organisme private în interes public. În asemenea cazuri, singura autoritate de supraveghere competentă să își exercite competențele care i-au fost atribuite în conformitate cu prezentul regulament ar trebui să fie autoritatea de supraveghere a statului membru în care autoritatea publică sau organismul privat își are sediul.

(129) Pentru a se asigura consecvența monitorizării și a aplicării prezentului regulament în întreaga Uniune, autoritățile de supraveghere ar trebui să aibă în fiecare stat membru aceleași sarcini și competențe efective, inclusiv competențe de investigare, competențe corective și sancționari, precum și competențe de autorizare și de consiliere, în special în cazul plângerilor depuse de persoane fizice, precum și, fără a aduce atingere competențelor autorităților de urmărire penală în temeiul dreptului intern, de a aduce în atenția autorităților judiciare cazurile de încălcare a prezentului regulament și de a se implica în proceduri judiciare. Aceste competențe ar trebui să includă și competența de a impune o limitare temporară sau definitivă, inclusiv o interdicție, asupra prelucrării. Statele membre pot stabili alte sarcini legate de protecția datelor cu caracter personal în temeiul prezentului regulament. Competențele autorităților de supraveghere ar trebui exercitate în conformitate cu garanții procedurale adecvate prevăzute în dreptul Uniunii și în dreptul intern, în mod imparțial, echitabil și într-un termen rezonabil. În special, fiecare măsură ar trebui să fie adecvată, necesară și proporțională în scopul de a asigura conformitatea cu dispozițiile prezentului regulament, luând în considerare circumstanțele fiecărui caz în parte, să respecte dreptul oricărei persoane de a fi ascultată înainte de luarea oricărei măsuri individuale care ar putea să îi aducă atingere și să evite costurile inutile și inconvenientele excesive pentru persoanele în cauză. Competențele de investigare în ceea ce privește accesul în incinte ar trebui exercitate în conformitate cu cerințele specifice din dreptul procedural național, cum ar fi obligația de a obține în prealabil o autorizare judiciară. Fiecare măsură obligatorie din punct de vedere juridic luată de autoritatea de supraveghere ar trebui să fie prezentată în scris, să fie clară și lipsită de ambiguitate, să indice autoritatea de supraveghere care a emis măsura, data emiterii măsurii, să poarte semnătura șefului sau a unui membru al autorității de supraveghere autorizat de

acesta, să furnizeze motivele pentru care s-a luat măsura și să facă trimitere la dreptul la o cale de atac eficientă. Acest lucru nu ar trebui să excludă cerințe suplimentare în conformitate cu dreptul procedural național. Adoptarea unor astfel de decizii obligatorii din punct de vedere juridic implică faptul că se poate da naștere unui control jurisdicțional în statul membru al autorității de supraveghere care a adoptat decizia.

(130) În cazul în care autoritatea de supraveghere la care s-a depus plângerea nu este autoritatea de supraveghere principală, autoritatea de supraveghere principală ar trebui să coopereze îndeaproape cu autoritatea de supraveghere la care s-a depus plângerea, în conformitate cu dispozițiile privind cooperarea și consecvența prevăzute în prezentul regulament. În astfel de cazuri, autoritatea de supraveghere principală ar trebui, atunci când ia măsuri destinate să producă efecte juridice, inclusiv impunerea de amenzi administrative, să țină seama cât mai mult posibil de opinia autorității de supraveghere la care a fost depusă plângerea și care ar trebui să își mențină competența de a desfășura orice investigație pe teritoriul propriului stat membru, în colaborare cu autoritatea de supraveghere principală.

(131) În cazurile în care o altă autoritate de supraveghere ar trebui să acționeze în calitate de autoritate de supraveghere principală pentru activitățile de prelucrare ale operatorului sau ale persoanei împuternicite de operator, dar obiectul concret al unei plângeri sau posibila încălcare vizează numai activitățile de prelucrare ale operatorului sau ale persoanei împuternicite de operator în statul membru în care a fost depusă plângerea sau a fost depistată posibila încălcare, iar chestiunea nu afectează în mod substanțial sau nu este susceptibilă să afecteze în mod substanțial persoane vizate din alte state membre, autoritatea de supraveghere care a primit o plângere sau a depistat ori a fost informată în alt mod asupra unor situații de posibile încălcări ale prezentului regulament ar trebui să încerce o soluționare pe cale amiabilă cu operatorul și, în cazul în care aceasta eșuează, să își exercite plenitudinea competențelor. Aceasta ar trebui să includă activități specifice de prelucrare efectuate pe teritoriul statului membru al autorității de supraveghere ori cu privire la persoane vizate de pe teritoriul aceluși stat membru, activități de prelucrare care au loc în contextul unei oferte de bunuri sau servicii destinate în mod special persoanelor vizate pe teritoriul statului membru al autorității de supraveghere sau activități de prelucrare care trebuie evaluate ținând seama de obligațiile juridice relevante în temeiul dreptului intern.

(132) Activitățile de creștere a gradului de conștientizare organizate pentru public de autoritățile de supraveghere ar trebui să includă măsuri specifice care să vizeze operatorii și persoanele împuternicite de operatori, inclusiv microîntreprinderile și întreprinderile mici și mijlocii, precum și persoanele fizice, în special în context educațional.

(133) Autoritățile de supraveghere ar trebui să își acorde reciproc asistență în îndeplinirea sarcinilor care le revin, pentru a se asigura coerența aplicării prezentului regulament pe piața internă. O autoritate de supraveghere care solicită asistență reciprocă poate adopta o măsură provizorie în cazul în care nu primește un răspuns la o solicitare de asistență reciprocă în termen de o lună de la primirea solicitării de către cealaltă autoritate de supraveghere.

(134) Fiecare autoritate de supraveghere ar trebui să participe, după caz, la operațiuni comune între autoritățile de supraveghere. Autoritatea de supraveghere căreia i s-a adresat solicitarea ar trebui să aibă obligația de a răspunde cererii într-un anumit termen.

(135) Pentru a se asigura aplicarea coerentă a prezentului regulament în întreaga Uniune, ar trebui să se instituie un mecanism pentru asigurarea coerenței în cadrul căruia autoritățile de supraveghere să coopereze. Acest mecanism ar trebui să se aplice, în special, în cazul în care o autoritate de supraveghere intenționează să adopte o măsură prevăzută a produce efecte juridice în ceea ce privește operațiunile de prelucrare care afectează în mod substanțial un număr semnificativ de persoane vizate din mai multe state membre. Mecanismul ar trebui să se aplice, de asemenea, în cazul în care o autoritate de supraveghere vizată sau Comisia solicită ca aspectul respectiv să fie tratat în cadrul mecanismului pentru asigurarea coerenței. Acest mecanism nu ar trebui să aducă atingere măsurilor pe care Comisia le poate adopta în exercitarea competențelor care îi revin în temeiul tratatelor.

(136) În aplicarea mecanismului pentru asigurarea coerenței, comitetul ar trebui, într-un anumit termen, să emită un aviz în cazul în care o majoritate a membrilor săi decide astfel sau în cazul în care orice autoritate de supraveghere vizată sau Comisia solicită acest lucru. Comitetul ar trebui, de asemenea, să fie împuternicit să adopte decizii obligatorii din punct de vedere juridic în cazul unor litigii între autoritățile de supraveghere. În acest scop, acesta ar trebui să emită, în principiu cu o majoritate de două treimi din membrii săi, decizii obligatorii din punct de vedere juridic, în cazuri bine definite, în cazul în care există opinii divergente între autoritățile de supraveghere, în special în cadrul mecanismului de cooperare între autoritatea de supraveghere principală și autoritățile de supraveghere vizate privind fondul cauzei, în special existența sau nu a unei încălcări a prezentului regulament.

(137) Este posibil să existe o necesitate urgentă de a se acționa pentru asigurarea protecției drepturilor și libertăților persoanelor vizate, în special în cazul în care există pericolul ca exercitarea unui drept al unei persoane vizate să fie împiedicată în mod considerabil. Prin urmare, o autoritate de supraveghere ar trebui să poată adopta măsuri provizorii pe teritoriul său, justificate în mod corespunzător, având o perioadă de valabilitate determinată care nu ar trebui să depășească trei luni.

(138) Aplicarea unui astfel de mecanism ar trebui să constituie o condiție pentru legalitatea unei măsuri destinate să producă efecte juridice, luate de o autoritate de supraveghere, în cazurile în care aplicarea acesteia este obligatorie. În alte cazuri cu relevanță transfrontalieră, ar trebui pus în aplicare mecanismul de cooperare între autoritatea de supraveghere principală și autoritățile de supraveghere vizate, iar între autoritățile de supraveghere vizate s-ar putea acorda asistență reciprocă și s-ar putea desfășura operațiuni comune pe bază bilaterală sau multilaterală, fără declanșarea mecanismului pentru asigurarea coerenței.

(139) Cu scopul de a promova aplicarea coerentă a prezentului regulament, comitetul ar trebui instituit ca organ independent al Uniunii. Pentru a-și îndeplini obiectivele, comitetul ar trebui să aibă personalitate juridică. Comitetul ar trebui să fie reprezentat de președintele său. Acesta ar trebui să înlocuiască Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, instituit prin Directiva 95/46/CE. Acesta ar trebui să fie alcătuit din șefii autorităților de supraveghere din fiecare stat membru și din Autoritatea Europeană pentru Protecția Datelor sau reprezentanții acestora. Comisia ar trebui să participe la activitățile comitetului fără a avea drept de vot,

iar Autoritatea Europeană pentru Protecția Datelor ar trebui să aibă drepturi de vot speciale. Comitetul ar trebui să contribuie la aplicarea coerentă a prezentului regulament în întreaga Uniune, inclusiv prin oferirea de consiliere Comisiei, în special cu privire la nivelul de protecție în țările terțe și în cadrul organizațiilor internaționale, și prin promovarea cooperării autorităților de supraveghere în întreaga Uniune. Comitetul ar trebui să acționeze în mod independent în îndeplinirea sarcinilor sale.

(140) Comitetul ar trebui să fie asistat de un secretariat asigurat de Autoritatea Europeană pentru Protecția Datelor. Personalul Autorității Europene pentru Protecția Datelor implicat în îndeplinirea sarcinilor conferite comitetului în temeiul prezentului regulament ar trebui să își îndeplinească sarcinile exclusiv conform instrucțiunilor președintelui comitetului și să raporteze acestuia.

(141) Orice persoană vizată ar trebui să aibă dreptul de a depune o plângere la o singură autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, precum și dreptul la o cale de atac eficientă în conformitate cu [articolul 47](#) din cartă, în cazul în care persoana vizată consideră că drepturile sale în temeiul prezentului regulament sunt încălcate sau în cazul în care autoritatea de supraveghere nu reacționează la o plângere, respinge sau refuză parțial sau total o plângere sau nu acționează atunci când o astfel de acțiune este necesară pentru asigurarea protecției drepturilor persoanei vizate. Investigația în urma unei plângeri ar trebui să fie efectuată, sub control judiciar, în măsura în care este necesar, în funcție de caz. Autoritatea de supraveghere ar trebui să informeze persoana vizată cu privire la evoluția și soluționarea plângerii într-un termen rezonabil. În eventualitatea în care cazul necesită o investigație suplimentară sau coordonarea cu o altă autoritate de supraveghere, ar trebui să se furnizeze informații intermediare persoanei vizate. În vederea facilitării depunerii plângerilor, fiecare autoritate de supraveghere ar trebui să ia măsuri precum punerea la dispoziție a unui formular de depunere a plângerii, care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.

(142) În cazul în care persoana vizată consideră că drepturile sale în temeiul prezentului regulament sunt încălcate, aceasta ar trebui să aibă dreptul de a mandata un organism, o organizație sau o asociație fără scop lucrativ care este înființat(ă) în conformitate cu dreptul intern, ale cărui (cărei) obiective statutare sunt în interesul public și care își desfășoară activitatea în domeniul asigurării protecției datelor cu caracter personal, să depună o plângere în numele său la o autoritate de supraveghere, să exercite dreptul la o cale de atac în numele persoanelor vizate sau, în cazul în care se prevede în dreptul intern, să exercite dreptul de a primi despăgubiri în numele persoanelor vizate. Un stat membru poate prevedea ca un astfel de organism, organizație sau asociație să aibă dreptul de a depune o plângere în statul membru respectiv, independent de mandatul acordat de o persoană vizată, și să aibă dreptul la o cale de atac eficientă în cazul în care are motive să considere că drepturile unei persoane vizate au fost încălcate ca rezultat al unei prelucrări a datelor cu caracter personal care încalcă prezentul regulament. Organismul, organizația sau asociația în cauza nu poate pretinde despăgubiri în numele unei persoane vizate, independent de mandatul acordat de persoana vizată.

(143) Orice persoană fizică sau juridică are dreptul de a introduce o acțiune în anulare împotriva deciziilor comitetului în fața Curții de Justiție, în conformitate cu condițiile prevăzute la [articolul 263](#) din TFUE. În calitate de destinatari ale acestor decizii, autoritățile de supraveghere vizate care doresc să le conteste trebuie să introducă o acțiune împotriva deciziilor respective în termen de două luni de la

data la care le-au fost notificate, în conformitate cu [articolul 263](#) din TFUE. În cazul în care deciziile comitetului vizează în mod direct și individual un operator, o persoană împuternicită de operator sau reclamantul, aceștia din urmă pot introduce o acțiune în anularea respectivelor decizii în termen de două luni de la publicarea acestora pe site-ul comitetului, în conformitate cu [articolul 263](#) din TFUE. Fără a aduce atingere acestui drept în temeiul [articolului 263](#) din TFUE, orice persoană fizică sau juridică ar trebui să aibă dreptul la o cale de atac judiciară eficientă în fața instanței naționale competente împotriva unei decizii a unei autorități de supraveghere care produce efecte juridice privind respectiva persoană. O astfel de decizie se referă în special la exercitarea competențelor de investigare, corective și de autorizare de către autoritatea de supraveghere sau la refuzul sau respingerea plângerilor. Cu toate acestea, dreptul la o cale de atac judiciară eficientă nu include măsuri ale autorităților de supraveghere care nu sunt obligatorii din punct de vedere juridic, cum ar fi avizele emise de autoritatea de supraveghere sau consiliere furnizată de aceasta. Acțiunile împotriva unei autorități de supraveghere ar trebui să fie aduse în fața instanțelor statului membru în care este stabilită autoritatea de supraveghere și ar trebui să se desfășoare în conformitate cu dreptul procesual al statului membru respectiv. Respectivul instanțe ar trebui să își exercite competența judiciară deplină, care ar trebui să includă competența de a examina toate aspectele de fapt sau de drept care au relevanță pentru litigiul cu care acestea sunt sesizate.

În cazul în care o plângere a fost respinsă sau refuzată de o autoritate de supraveghere, reclamantul poate introduce o acțiune la instanțele din același stat membru. În contextul căilor de atac judiciare privind aplicarea prezentului regulament, instanțele naționale care consideră necesară o decizie privind chestiunea respectivă pentru a le permite să ia o hotărâre pot sau, în cazul prevăzut la [articolul 267](#) din TFUE, trebuie să solicite Curții de Justiție să pronunțe o decizie preliminară privind interpretarea dreptului Uniunii, inclusiv a prezentului regulament. În plus, în cazul în care o decizie a unei autorități de supraveghere care pune în aplicare o decizie a comitetului este contestată în fața unei instanțe naționale și este în discuție validitatea deciziei comitetului, respectiva instanță națională nu are competența de a declara nulă decizia comitetului, ci trebuie să aducă chestiunea validității în fața Curții de Justiție, în conformitate cu [articolul 267](#) din TFUE, astfel cum a fost interpretat de Curtea de Justiție, ori de câte ori instanța națională consideră decizia nulă. Cu toate acestea, o instanță națională nu poate să transmită o chestiune cu privire la validitatea deciziei comitetului la cererea unei persoane fizice sau juridice care a avut posibilitatea de a introduce o acțiune în anulare împotriva respectivei decizii, în special dacă aceasta era vizată în mod direct și individual de decizia în cauză, dar nu a făcut acest lucru în termenul prevăzut la [articolul 263](#) din TFUE.

(144) Atunci când o instanță sesizată cu o procedură împotriva unei decizii a unei autorități de supraveghere are motive să creadă că în fața unei instanțe competente dintr-un alt stat membru au fost introduse proceduri cu privire la aceeași prelucrare, cum ar fi același obiect al prelucrării, de către același operator sau aceleiași persoană împuternicită de operator, sau aceeași cauză, instanța respectivă ar trebui să contacteze cea de a doua instanță pentru a confirma existența unor astfel de proceduri conexe. În cazul în care aceste proceduri conexe se află pe rolul unei instanțe dintr-un alt stat membru, orice instanță, cu excepția celei sesizate inițial, poate să își suspende procedurile sau, la cererea uneia dintre părți, își poate declina competența în favoarea instanței sesizate inițial, cu condiția

ca aceasta din urmă să aibă competența de a soluționa procedurile în cauză și ca dreptul care i se aplică să îi permită consolidarea acestor proceduri conexe. Procedurile sunt considerate conexe atunci când sunt atât de strâns legate între ele încât este oportună instrumentarea și judecarea lor în același timp pentru a se evita riscul pronunțării unor hotărâri ireconciliabile în cazul judecării lor în mod separat.

(145) În ceea ce privește acțiunile inițiate împotriva unui operator sau unei persoane împuternicite de operator, reclamantul ar trebui să aibă posibilitatea de a introduce acțiunea în fața instanțelor din statele membre în care operatorul sau persoana împuternicită de operator are un sediu sau în care persoana vizată își are reședința, cu excepția cazului în care operatorul este o autoritate publică dintr-un stat membru ce acționează în exercitarea competențelor sale publice.

(146) Operatorul sau persoana împuternicită de operator ar trebui să plătească despăgubiri pentru orice prejudiciu pe care o persoană îl poate suferi ca urmare a unei prelucrări care încalcă prezentul regulament. Operatorul sau persoana împuternicită de operator ar trebui să fie exonerată de răspundere dacă dovedesc că nu sunt în niciun fel răspunzători pentru prejudiciu. Conceptul de prejudiciu ar trebui interpretat în sens larg, din perspectiva jurisprudenței Curții de Justiție, într-un mod care să reflecte pe deplin obiectivele prezentului regulament. Această dispoziție nu aduce atingere niciunei cereri de despăgubire care rezultă din încălcarea altor norme din dreptul Uniunii sau din dreptul intern. O prelucrare care încalcă prezentul regulament include și prelucrarea care încalcă actele delegate și de punere în aplicare adoptate în conformitate cu prezentul regulament și cu dreptul intern care specifică norme din prezentul regulament. Persoanele vizate ar trebui să primească despăgubiri integrale și eficiente pentru prejudiciul pe care le-au suferit. În cazul în care operatorii sau persoanele împuternicite de operatori sunt implicate în aceeași prelucrare, fiecare operator sau fiecare persoană împuternicită de operator ar trebui să fie considerată răspunzătoare pentru întregul prejudiciu. Cu toate acestea, atunci când procedurile juridice care le vizează sunt conexe, în conformitate cu dreptul intern, despăgubirile pot fi împărțite în funcție de răspunderea fiecărui operator sau a fiecărei persoane împuternicite de operator, cu condiția să se asigure despăgubirea integrală și efectivă a persoanei vizate care a suferit prejudiciul. Orice operator sau persoană împuternicită de operator care a plătit despăgubiri integrale poate formula ulterior o acțiune în regres împotriva altor operatori sau persoane împuternicite de operatori implicate în aceeași prelucrare.

(147) În cazul în care prezentul regulament cuprinde norme specifice privind competența judiciară, în special în ceea ce privește căile de atac judiciare, inclusiv acțiunile în despăgubiri, împotriva unui operator sau a unei persoane împuternicite de operator, normele generale privind competența judiciară precum cele din Regulamentul (UE) [nr. 1215/2012](#) al Parlamentului European și al Consiliului nu ar trebui să aducă atingere aplicării unor astfel de norme specifice.

(148) Pentru a consolida respectarea aplicării normelor prevăzute în prezentul regulament, ar trebui impuse sancțiuni, inclusiv amenzi administrative, pentru orice încălcare a prezentului regulament, pe lângă sau în locul măsurilor adecvate impuse de autoritatea de supraveghere în temeiul prezentului regulament. În cazul unei încălcări minore sau în cazul în care amenda susceptibilă de a fi impusă ar constitui o sarcină disproporționată pentru o persoană fizică, poate fi emis un avertisment în locul unei amenzi. Cu toate acestea, ar trebui să se ia în considerare în mod corespunzător natura, gravitatea și durata încălcării, caracterul deliberat al încălcării, acțiunile întreprinse pentru a reduce prejudiciul

cauzat, gradul de răspundere sau orice încălcări anterioare relevante, modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, conformitatea cu măsurile adoptate împotriva operatorului sau a persoanei împuternicite de operator, aderarea la un cod de conduită și orice alt factor agravant sau atenuant. Impunerea de sancțiuni, inclusiv de amenzi administrative, ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu [carta](#), inclusiv o protecție judiciară eficientă și un proces echitabil.

(149) Statele membre ar trebui să poată stabili normele privind sancțiunile penale pentru încălcările prezentului regulament, inclusiv pentru încălcarea normelor de drept intern adoptate în temeiul și în limitele prezentului regulament. Respectivul sancțiuni penale pot, de asemenea, permite privarea de profiturile obținute prin încălcarea prezentului regulament. Cu toate acestea, impunerea de sancțiuni penale pentru încălcări ale unor asemenea norme de drept intern și de sancțiuni administrative nu ar trebui să ducă la încălcarea principiului ne bis in idem, astfel cum a fost interpretat de Curtea de Justiție.

(150) Pentru consolidarea și armonizarea sancțiunilor administrative în cazul încălcării prezentului regulament, fiecare autoritate de supraveghere ar trebui să aibă competența de a impune amenzi administrative. Prezentul regulament ar trebui să indice încălcările, și limita maximă și criteriile pentru stabilirea amenzilor administrative aferente, care ar trebui să fie stabilite de autoritatea de supraveghere competentă în fiecare caz în parte, ținând seama de toate circumstanțele relevante ale situației specifice, luându-se în considerare în mod corespunzător, în special, natura, gravitatea și durata încălcării, precum și consecințele acesteia și măsurile luate pentru a se asigura respectarea obligațiilor în temeiul prezentului regulament și pentru a se preveni sau atenua consecințele încălcării. În cazul în care amenzile administrative sunt impuse unei întreprinderi, o întreprindere ar trebui înțeleasă ca fiind o întreprindere în conformitate cu [articolele 101 și 102](#) din TFUE în aceste scopuri. În cazul în care se impun amenzi administrative unor persoane care nu sunt întreprinderi, autoritatea de supraveghere ar trebui să țină seama de nivelul general al veniturilor din statul membru respectiv, precum și de situația economică a persoanei atunci când estimează quantumul adecvat al amenzii. Mecanismul pentru asigurarea coerenței poate fi, de asemenea, utilizat pentru a promova aplicarea consecventă a amenzilor administrative. Competența de a stabili dacă și în ce măsură autoritățile publice ar trebui să facă obiectul unor amenzi administrative ar trebui să revină statelor membre. Impunerea unei amenzi administrative sau transmiterea unei avertizări nu afectează aplicarea altor competențe ale autorităților de supraveghere sau a altor sancțiuni în temeiul prezentului regulament.

(151) Sistemele juridice ale Danemarcei și Estoniei nu permit amenzi administrative astfel cum sunt prevăzute în prezentul regulament. Normele privind amenzile administrative pot fi aplicate astfel încât, în Danemarca, amenda să fie impusă de instanțele naționale competente ca sancțiune penală, iar în Estonia amenda să fie impusă de autoritatea de supraveghere în cadrul unei proceduri privind delictele, cu condiția ca o astfel de aplicare a normelor în statele membre respective să aibă un efect echivalent cu cel al amenzilor administrative impuse de autoritățile de supraveghere. Prin urmare, instanțele naționale competente ar trebui să țină seama de recomandarea autorității de supraveghere care a inițiat amenda. În orice caz, amenzile impuse ar trebui să fie eficace, proporționale și disuasive.

(152) În cazul în care prezentul regulament nu armonizează sancțiunile administrative sau în alte cazuri, acolo unde este necesar, de exemplu în cazul unor încălcări grave ale prezentului regulament, statele

membre ar trebui să pună în aplicare un sistem care să prevadă sancțiuni eficace, proporționale și disuasive. Natura unor astfel de sancțiuni, penale sau administrative, ar trebui stabilită în dreptul intern.

(153) Dreptul statelor membre ar trebui să stabilească un echilibru între normele care reglementează libertatea de exprimare și de informare, inclusiv exprimarea jurnalistică, academică, artistică și/sau literară, și dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament. Prelucrarea datelor cu caracter personal exclusiv în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare ar trebui să facă obiectul unor derogări sau al unor excepții de la anumite dispoziții ale prezentului regulament în cazul în care este necesară stabilirea unui echilibru între dreptul la protecția datelor cu caracter personal și dreptul la libertatea de exprimare și de informare, astfel cum este prevăzut în [articolul 11](#) din cartă. Acest lucru ar trebui să se aplice în special prelucrării datelor cu caracter personal în domeniul audiovizualului, precum și în arhivele de știri și în bibliotecile ziarelor. Prin urmare, statele membre ar trebui să adopte măsuri legislative care să prevadă excepțiile și derogările necesare în vederea asigurării echilibrului între aceste drepturi fundamentale. Statele membre ar trebui să adopte astfel de excepții și derogări în ceea ce privește principiile generale, drepturile persoanelor vizate, operatorul și persoana împuternicită de operator, transferul de date cu caracter personal către țări terțe sau organizații internaționale, autoritățile de supraveghere independente, cooperarea și coerența, precum și în ceea ce privește situații specifice de prelucrare a datelor. În cazul în care aceste excepții sau derogări diferă de la un stat membru la altul, ar trebui să se aplice dreptul statului membru sub incidența căruia intră operatorul. Pentru a ține seama de importanța dreptului la libertatea de exprimare în fiecare societate democratică, este necesar ca noțiunile legate de această libertate, cum ar fi jurnalismul, să fie interpretate în sens larg.

(154) Prezentul regulament permite luarea în considerare a principiului accesului public la documente oficiale în aplicarea prezentului regulament. Accesul public la documente oficiale poate fi considerat a fi în interes public. Datele cu caracter personal din documentele deținute de o autoritate publică sau de un organism public ar trebui să poată fi divulgate de autoritatea respectivă sau de organismul respectiv în cazul în care dreptul Uniunii sau dreptul intern sub incidența căruia intră autoritatea publică sau organismul public prevede acest lucru. Dreptul Uniunii și dreptul intern ar trebui să asigure un echilibru între accesul public la documentele oficiale și reutilizarea informațiilor din sectorul public, pe de o parte, și dreptul la protecția datelor cu caracter personal, pe de altă parte, și ar putea prin urmare să prevadă echilibrul necesar cu dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament. Trimiterea la autoritățile și organismele publice ar trebui, în acest context, să includă toate autoritățile sau alte organisme reglementate de dreptul intern privind accesul public la documente. Directiva [2003/98/CE](#) a Parlamentului European și a Consiliului lasă intact și nu aduce atingere în niciun fel nivelului de protecție a persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal în conformitate cu dreptul Uniunii și cu cel intern și, în special, nu modifică drepturile și obligațiile prevăzute de prezentul regulament. În special, directiva sus-menționată nu se aplică documentelor la care accesul este exclus sau restrâns în temeiul regimurilor de acces din motive legate de protecția datelor cu caracter personal și nici părților din documente accesibile în temeiul respectivelor regimuri care conțin date cu caracter personal a căror reutilizare a fost stabilită prin lege

ca fiind incompatibilă cu dreptul privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

(155) Dreptul intern sau acordurile colective, inclusiv "acordurile de muncă", pot prevedea norme specifice care să reglementeze prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă, în special condițiile în care datele cu caracter personal în contextul ocupării unui loc de muncă pot fi prelucrate pe baza consimțământului angajatului, în scopul recrutării, al respectării clauzelor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii, al egalității și diversității la locul de muncă, al asigurării sănătății și securității la locul de muncă, precum și în scopul exercitării și beneficierii, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și în scopul încetării raporturilor de muncă.

(156) Prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ar trebui să facă obiectul unor garanții adecvate pentru drepturile și libertățile persoanei vizate în temeiul prezentului regulament. Respectivul garanții ar trebui să asigure faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, principiul reducerii la minimum a datelor. Prelucrarea ulterioară a datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice se efectuează atunci când operatorul a evaluat fezabilitatea pentru îndeplinirea acestor obiective prin prelucrarea unor date cu caracter personal care nu permit sau nu mai permit identificarea persoanelor vizate, cu condiția să existe garanții adecvate (cum ar fi pseudonimizarea datelor cu caracter personal). Statele membre ar trebui să prevadă garanții adecvate pentru prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. Statele membre ar trebui să fie autorizate să ofere, în anumite condiții și sub rezerva unor garanții adecvate pentru persoanele vizate, precizări și derogări în ceea ce privește cererile de informații și dreptul la rectificare, dreptul la ștergere, dreptul de a fi uitat, dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, precum și dreptul la opoziție în cazul prelucrării datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. Condițiile și garanțiile în cauză pot genera proceduri specifice astfel încât persoanele vizate să își exercite respectivele drepturi dacă acest lucru este adecvat în contextul scopurilor vizate de prelucrarea specifică, precum și măsuri tehnice și organizaționale vizând reducerea la minimum a prelucrării datelor cu caracter personal, în conformitate cu principiile proporționalității și necesității. Prelucrarea datelor cu caracter personal în scopuri științifice ar trebui să fie, de asemenea, conformă cu alte acte legislative relevante, cum ar fi cele privind studiile clinice.

(157) Prin combinarea informațiilor din registre, cercetătorii pot obține noi cunoștințe de mare valoare în ceea ce privește bolile cu largă răspândire, cum ar fi bolile cardiovasculare, cancerul și depresia. Pe baza registrelor, rezultatele cercetărilor pot fi întărite, întrucât acestea se bazează pe o populație mai mare. În domeniul științelor sociale, cercetarea pe baza registrelor le permite cercetătorilor să obțină informații esențiale despre corelarea pe termen lung a unei serii de condiții sociale, precum șomajul sau educația, cu alte condiții de viață. Rezultatele cercetărilor obținute pe baza registrelor furnizează

cunoștințe solide, de înaltă calitate, care pot constitui baza pentru elaborarea și punerea în aplicare a unor politici bazate pe cunoaștere și care pot îmbunătăți calitatea vieții pentru un număr de persoane, eficiența serviciilor sociale. Pentru a facilita cercetarea științifică, datele cu caracter personal pot fi prelucrate în scopuri de cercetare științifică, sub rezerva condițiilor și a garanțiilor corespunzătoare stabilite în dreptul Uniunii sau în dreptul intern.

(158) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare, prezentul regulament ar trebui să se aplice și prelucrării respective, ținând seama de faptul că prezentul regulament nu ar trebui să se aplice persoanelor decedate. Autoritățile publice sau organismele publice sau private care dețin evidențe de interes public ar trebui, în temeiul dreptului Uniunii sau al dreptului național, să aibă o obligație legală de a dobândi, a păstra, a evalua, a pregăti, a descrie, a comunica, a promova, a disemina și a asigura accesul la evidențe de valoare durabilă de interes public general. Statele membre ar trebui, de asemenea, să poată să prevadă prelucrarea ulterioară a datelor cu caracter personal în scopuri de arhivare, de exemplu cu scopul de a furniza informații specifice referitoare la comportamentul politic în perioada fostelor regimuri de stat totalitare, la genociduri, la crime împotriva umanității, în special holocaustul, sau la crime de război.

(159) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică, prezentul regulament ar trebui să se aplice și prelucrării respective. În sensul prezentului regulament, prelucrarea datelor cu caracter personal în scopuri de cercetare științifică ar trebui să fie interpretată în sens larg, incluzând de exemplu dezvoltarea tehnologică și activitățile demonstrative, cercetarea fundamentală, cercetarea aplicată și cercetarea finanțată din surse private. Ar trebui, în plus, luat în considerare obiectivul Uniunii de creare a unui Spațiu european de cercetare, astfel cum este menționat la articolul 179 [alineatul \(1\)](#) din TFUE. Scopurile de cercetare științifică ar trebui să includă, de asemenea, studii efectuate în interes public în domeniul sănătății publice. Pentru a îndeplini caracteristicile specifice ale prelucrării datelor cu caracter personal în scopuri de cercetare științifică, ar trebui să se aplice condiții specifice, în special în ceea ce privește publicarea sau divulgarea într-un alt mod a datelor cu caracter personal în contextul scopurilor de cercetare științifică. În cazul în care rezultatul cercetării științifice, în special în contextul sănătății, constituie un motiv pentru măsuri suplimentare în interesul persoanei vizate, normele generale ale prezentului regulament ar trebui să se aplice având în vedere aceste măsuri.

(160) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare istorică, prezentul regulament ar trebui să se aplice și prelucrării respective. Acest lucru ar trebui să includă, de asemenea, cercetarea istorică și cercetarea în scopuri genealogice, ținând seama de faptul că prezentul regulament nu ar trebui să se aplice persoanelor decedate.

(161) În scopul acordării consimțământului de a participa la activități de cercetare științifică în cadrul testelor clinice, ar trebui să se aplice dispozițiile relevante ale Regulamentului (UE) [nr. 536/2014](#) al Parlamentului European și al Consiliului.

(162) În cazul în care datele cu caracter personal sunt prelucrate în scopuri statistice, prezentul regulament ar trebui să se aplice prelucrării respective. Dreptul Uniunii sau dreptul intern ar trebui, în limitele prezentului regulament, să determine conținutul statistic, controlul accesului, specificațiile pentru prelucrarea datelor cu caracter personal în scopuri statistice și măsurile adecvate pentru a

proteja drepturile și libertățile persoanelor vizate și pentru a asigura confidențialitatea datelor statistice. Aceste rezultate statistice pot fi utilizate ulterior în diferite scopuri, inclusiv în scopuri de cercetare științifică. Scopuri statistice înseamnă orice operațiune de colectare și prelucrare de date cu caracter personal necesară pentru anchetele statistice sau pentru producerea de rezultate statistice. Scopurile statistice presupun că rezultatul prelucrării în scopuri statistice nu constituie date cu caracter personal, ci date agregate și că acest rezultat sau datele cu caracter personal nu sunt utilizate în sprijinul unor măsuri sau decizii privind o anumită persoană fizică.

(163) Informațiile confidențiale pe care autoritățile statistice de la nivelul Uniunii și de la nivel național le colectează în vederea elaborării de statistici europene și naționale oficiale ar trebui să fie protejate. Statisticile europene ar trebui concepute, elaborate și difuzate în conformitate cu principiile statistice prevăzute la articolul 338 [alineatul \(2\)](#) din TFUE, în timp ce statisticile naționale ar trebui, de asemenea, să fie în conformitate cu dreptul intern. Regulamentul (CE) [nr. 223/2009](#) al Parlamentului European și al Consiliului prevede specificații suplimentare privind confidențialitatea datelor statistice pentru statisticile europene.

(164) În ceea ce privește competențele autorităților de supraveghere de a obține de la operator sau de la persoana împuternicită de operator accesul la datele cu caracter personal și accesul în clădirile lor, statele membre pot adopta, pe cale legislativă și în limitele stabilite de prezentul regulament, norme specifice pentru protejarea secretului profesional sau a altor obligații echivalente, în măsura în care acest lucru este necesar pentru a asigura un echilibru între dreptul la protecția datelor cu caracter personal și obligația de păstrare a secretului profesional. Aceasta nu aduce atingere obligațiilor existente ale statelor membre de a adopta norme privind secretul profesional în situațiile cerute de dreptul Uniunii.

(165) Prezentul regulament respectă și nu aduce atingere statutului de care beneficiază, în temeiul dreptului constituțional existent, bisericile și asociațiile sau comunitățile religioase din statele membre, astfel cum este recunoscut în [articolul 17](#) din TFUE.

(166) În vederea îndeplinirii obiectivelor prezentului regulament, și anume protejarea drepturilor și libertăților fundamentale ale persoanelor fizice și, în special, a dreptului acestora la protecția datelor cu caracter personal, și pentru a se garanta libera circulație a datelor cu caracter personal pe teritoriul Uniunii, competența de a adopta acte în conformitate cu [articolul 290](#) din TFUE ar trebui să fie delegată Comisiei. În special, ar trebui adoptate acte delegate în ceea ce privește criteriile și cerințele privind mecanismele de certificare, informațiile care trebuie prezentate prin pictograme standardizate și procedurile pentru furnizarea unor astfel de pictograme. Este deosebit de important ca, în cadrul activității sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți. Atunci când pregătește și elaborează acte delegate, Comisia ar trebui să asigure transmiterea simultană, la timp și în mod corespunzător a documentelor relevante către Parlamentul European și către Consiliu.

(167) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentului regulament, Comisia ar trebui investită cu competențe de executare în situațiile stabilite de prezentul regulament. Competențele respective ar trebui să fie exercitate în conformitate cu Regulamentul (UE) [nr. 182/2011](#).

În acest context, Comisia ar trebui să ia în considerare măsuri specifice pentru microîntreprinderi și pentru întreprinderile mici și mijlocii.

(168) Procedura de examinare ar trebui utilizată pentru adoptarea de acte de punere în aplicare privind: clauzele contractuale standard dintre operatori și persoanele împuternicite de operatori, precum și dintre persoanele împuternicite de operatori; codurile de conduită; standardele tehnice și mecanismele de certificare; nivelul adecvat de protecție oferit de o țară terță, de un teritoriu sau de un anumit sector de prelucrare din țara terță respectivă, sau de o organizație internațională; clauzele standard de protecție a datelor; formatele și procedurile pentru schimbul electronic de informații între operatori, persoanele împuternicite de operatori și autoritățile de supraveghere pentru regulile corporatiste obligatorii; asistența reciprocă; precum și modalitățile de realizare a schimbului electronic de informații între autoritățile de supraveghere, precum și între autoritățile de supraveghere și comitetul.

(169) Comisia ar trebui să adopte acte de punere în aplicare imediat aplicabile atunci când dovezile disponibile arată că o țară terță, un teritoriu sau un anumit sector de prelucrare din țara terță respectivă, sau o organizație internațională nu asigură un nivel de protecție adecvat, precum și din motive imperative de urgență.

(170) Deoarece obiectivul prezentului regulament, și anume asigurarea unui nivel echivalent de protecție a persoanelor fizice și libera circulație a datelor cu caracter personal în întreaga Uniune, nu poate fi realizat în mod satisfăcător de către statele membre dar, având în vedere amploarea sau efectele acțiunii, poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este definit la [articolul 5](#) din Tratatul privind Uniunea Europeană ("Tratatul UE"). În conformitate cu principiul proporționalității, astfel cum este definit la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivelor menționate.

(171) Directiva [95/46/CE](#) ar trebui să fie abrogată prin prezentul regulament. Prelucrările în derulare la data aplicării prezentului regulament ar trebui să fie aduse în conformitate cu prezentul regulament în termen de doi ani de la data intrării în vigoare a prezentului regulament. În cazul în care prelucrările se bazează pe consimțământ în temeiul Directivei 95/46/CE, nu este necesar ca persoana vizată să își dea încă o dată consimțământul în cazul în care modul în care consimțământul a fost dat este în conformitate cu condițiile din prezentul regulament, astfel încât operatorului să i se permită să continue o astfel de prelucrare după data aplicării prezentului regulament. Deciziile adoptate ale Comisiei și autorizațiile autorităților de supraveghere emise pe baza Directivei 95/46/CE rămân în vigoare până când vor fi modificate, înlocuite sau abrogate.

(172) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 [alineatul \(2\)](#) din Regulamentul (CE) nr. 45/2001 și a emis un aviz la 7 martie 2012.

(173) Prezentul regulament ar trebui să se aplice tuturor aspectelor referitoare la protecția drepturilor și libertăților fundamentale legate de prelucrarea datelor cu caracter personal, care nu fac obiectul unor obligații specifice cu același obiectiv ca cel stabilit în Directiva [2002/58/CE](#) a Parlamentului European și a Consiliului, inclusiv obligațiile privind operatorul și drepturile persoanelor fizice. Pentru a se clarifica relația dintre prezentul regulament și Directiva 2002/58/CE, respectiva directivă ar trebui să fie

modificată în consecință. După adoptarea prezentului regulament, Directiva 2002/58/CE ar trebui să fie revizuită în special pentru a se asigura coerența cu prezentul regulament,
ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

Dispoziții generale

Articolul 1 Obiect și obiective (1) Prezentul regulament stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, precum și normele referitoare la libera circulație a datelor cu caracter personal.

(2) Prezentul regulament asigură protecția drepturilor și libertăților fundamentale ale persoanelor fizice și în special a dreptului acestora la protecția datelor cu caracter personal.

(3) Libera circulație a datelor cu caracter personal în interiorul Uniunii nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

Articolul 2 Domeniul de aplicare material (1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.

(2) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:

(a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii;

(b) de către statele membre atunci când desfășoară activități care intră sub incidența [capitolului 2](#) al titlului V din Tratatul UE;

(c) de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice;

(d) de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor, sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.

(3) Pentru prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii, se aplică Regulamentul (CE) [nr. 45/2001](#). Regulamentul (CE) nr. 45/2001 și alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal se adaptează la principiile și normele din prezentul regulament în conformitate cu [articolul 98](#).

(4) Prezentul regulament nu aduce atingere aplicării Directivei [2000/31/CE](#), în special normelor privind răspunderea furnizorilor de servicii intermediari, prevăzute la [articolele 12-15](#) din directiva menționată.

Articolul 3 Domeniul de aplicare teritorial (1) Prezentul regulament se aplică prelucrării datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.

(2) Prezentul regulament se aplică prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activitățile de prelucrare sunt legate de:

(a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată; sau

(b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.

(3) Prezentul regulament se aplică prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internațional public.

Articolul 4 Definiții În sensul prezentului regulament:

1. "date cu caracter personal" înseamnă orice informații privind o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

2. "prelucrare" înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

3. "restricționarea prelucrării" înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

4. "creare de profiluri" înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

5. "pseudonimizare" înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

6. "sistem de evidență a datelor" înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;

7. "operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

8. "persoană împuternicită de operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

9. "destinatar" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

10. "parte terță" înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

11. "consimțământ" al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

12. "încălcarea securității datelor cu caracter personal" înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

13. "date genetice" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

14. "date biometrice" înseamnă o date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

15. "date privind sănătatea" înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;

16. "sediul principal" înseamnă:

(a) în cazul unui operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acestuia în Uniune, cu excepția cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are competența de a dispune punerea în aplicare a acestor decizii, caz în care sediul care a luat deciziile respective este considerat a fi sediul principal;

(b) în cazul unei persoane împuternicite de operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acesteia în Uniune, sau, în cazul în care persoana împuternicită de operator nu are o administrație centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activitățile principale de prelucrare, în contextul activităților unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligații specifice în temeiul prezentului regulament;

17. "reprezentant" înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul [articolului 27](#), care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul prezentului regulament;

18. "întreprindere" înseamnă o persoană fizică sau juridică ce desfășoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații care desfășoară în mod regulat o activitate economică;

19. "grup de întreprinderi" înseamnă o întreprindere care exercită controlul și întreprinderile controlate de aceasta;

20. "reguli corporatiste obligatorii" înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

21. "autoritate de supraveghere" înseamnă o autoritate publică independentă instituită de un stat membru în temeiul [articolului 51](#);

22. "autoritate de supraveghere vizată" înseamnă o autoritate de supraveghere care este vizată de procesul de prelucrare a datelor cu caracter personal deoarece:

(a) operatorul sau persoana împuternicită de operator este stabilită pe teritoriul statului membru al autorității de supraveghere respective;

(b) persoanele vizate care își au reședința în statul membru în care se află autoritatea de supraveghere respectivă sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare; sau

(c) la autoritatea de supraveghere respectivă a fost depusă o plângere;

23. "prelucrare transfrontalieră" înseamnă:

(a) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre; sau

(b) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre;

24. "obiecție relevantă și motivată" înseamnă o obiecție la un proiect de decizie în scopul de a stabili dacă există o încălcare a prezentului regulament sau dacă măsurile preconizate în ceea ce privește operatorul sau persoana împuternicită de operator respectă prezentul regulament, care demonstrează în mod clar importanța riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate și, după caz, libera circulație a datelor cu caracter personal în cadrul Uniunii;

25. "serviciile societății informaționale" înseamnă un serviciu astfel cum este definit la articolul 1 [alineatul \(1\)](#) litera (b) din Directiva 98/34/CE a Parlamentului European și a Consiliului;

26. "organizație internațională" înseamnă o organizație și organismele sale subordonate reglementate de dreptul internațional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe țări sau în temeiul unui astfel de acord.

CAPITOLUL II

Principii

Articolul 5 Principii legate de prelucrarea datelor cu caracter personal (1) Datele cu caracter personal sunt:

(a) prelucrate în mod legal, echitabil și transparent față de persoana vizată ("legalitate, echitate și transparență");

(b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89 [alineatul \(1\)](#) ("limitări legate de scop");

(c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate ("reducerea la minimum a datelor");

(d) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere ("exactitate");

(e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 [alineatul \(1\)](#), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate ("limitări legate de stocare");

(f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("integritate și confidențialitate").

(2) Operatorul este responsabil de respectarea [alineatului \(1\)](#) și poate demonstra această respectare ("responsabilitate").

Articolul 6 Legalitatea prelucrării (1) Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

(a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

(b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

(c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;

(d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

(e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul;

(f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Litera (f) din primul paragraf nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor.

(2) Statele membre pot menține sau introduce dispoziții mai specifice de adaptare a aplicării normelor prezentului regulament în ceea ce privește prelucrarea în vederea respectării alineatului (1) [literale \(c\)](#) și [\(e\)](#) prin definirea unor cerințe specifice mai precise cu privire la prelucrare și a altor măsuri de asigurare a unei prelucrări legale și echitabile, inclusiv pentru alte situații concrete de prelucrare, astfel cum este prevăzut în capitolul IX.

(3) Temeiul pentru prelucrarea menționată la alineatul (1) [literale \(c\)](#) și [\(e\)](#) trebuie să fie prevăzut în:

(a) dreptul Uniunii; sau

(b) dreptul intern care se aplică operatorului.

Scopul prelucrării este stabilit pe baza respectivului temei juridic sau, în ceea ce privește prelucrarea menționată la alineatul (1) [litera \(e\)](#), este necesar pentru îndeplinirea unei sarcini efectuate în interes public sau în cadrul exercitării unei funcții publice atribuite operatorului. Respectivul temei juridic poate conține dispoziții specifice privind adaptarea aplicării normelor prezentului regulament, printre altele: condițiile generale care reglementează legalitatea prelucrării de către operator; tipurile de date care fac obiectul prelucrării; persoanele vizate; entitățile cărora le pot fi divulgate datele și scopul pentru care respectivele date cu caracter personal pot fi divulgate; limitările legate de scop; perioadele de stocare; și operațiunile și procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale și echitabile cum sunt cele pentru alte situații concrete de prelucrare astfel cum sunt prevăzute în capitolul IX. Dreptul Uniunii sau dreptul intern urmărește un obiectiv de interes public și este proporțional cu obiectivul legitim urmărit.

(4) În cazul în care prelucrarea în alt scop decât cel pentru care datele cu caracter personal au fost colectate nu se bazează pe consimțământul persoanei vizate sau pe dreptul Uniunii sau dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja obiectivele menționate la articolul 23 [alineatul \(1\)](#), operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial, ia în considerare, printre altele:

(a) orice legătură dintre scopurile în care datele cu caracter personal au fost colectate și scopurile prelucrării ulterioare preconizate;

(b) contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește relația dintre persoanele vizate și operator;

(c) natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date cu caracter personal, în conformitate cu [articolul 9](#), sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale și infracțiuni, în conformitate cu [articolul 10](#);

(d) posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;

(e) existența unor garanții adecvate, care pot include criptarea sau pseudonimizarea.

Articolul 7 Condiții privind consimțământul (1) În cazul în care prelucrarea se bazează pe consimțământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal.

(2) În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Nicio parte a respectivei declarații care constituie o încălcare a prezentului regulament nu este obligatorie.

(3) Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragera consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragera consimțământului se face la fel de simplu ca acordarea acestuia.

(4) Atunci când se evaluează dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

Articolul 8 Condiții aplicabile în ceea ce privește consimțământul copiilor în legătură cu serviciile societății informaționale (1) În cazul în care se aplică articolul 6 alineatul (1) [litera \(a\)](#), în ceea ce privește oferirea de servicii ale societății informaționale în mod direct unui copil, prelucrarea datelor cu caracter personal ale unui copil este legală dacă copilul are cel puțin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului.

Statele membre pot prevedea prin lege o vârstă inferioară în aceste scopuri, cu condiția ca acea vârstă inferioară să nu fie mai mică de 13 ani.

(2) Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile.

(3) Alineatul (1) nu afectează dreptul general al contractelor aplicabil în statele membre, cum ar fi normele privind valabilitatea, încheierea sau efectele unui contract în legătură cu un copil.

Articolul 9 Prelucrarea de categorii speciale de date cu caracter personal (1) Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de

date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

(2) Alineatul (1) nu se aplică în următoarele situații:

(a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicția prevăzută la [alineatul \(1\)](#) să nu poată fi ridicată prin consimțământul persoanei vizate;

(b) prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;

(c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;

(d) prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;

(e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;

(f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;

(g) prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate;

(h) prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la [alineatul \(3\)](#);

(i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional; sau

(j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 [alineatul \(1\)](#), în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate.

(3) Datele cu caracter personal menționate la [alineatul \(1\)](#) pot fi prelucrate în scopurile menționate la alineatul (2) [litera \(h\)](#) în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naționale competente.

(4) Statele membre pot menține sau introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea de date genetice, date biometrice sau date privind sănătatea.

Articolul 10 Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni
Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni sau la măsuri de securitate conexe în temeiul articolului 6 [alineatul \(1\)](#) se efectuează numai sub controlul unei autorități de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorități de stat.

Articolul 11 Prelucrarea care nu necesită identificare (1) În cazul în care scopurile pentru care un operator prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu are obligația de a păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizată în scopul unic al respectării prezentului regulament.

(2) Dacă, în cazurile menționate la alineatul (1) din prezentul articol, operatorul poate demonstra că nu este în măsură să identifice persoana vizată, operatorul informează persoana vizată în mod corespunzător, în cazul în care este posibil. În astfel de cazuri, [articolele 15-20](#) nu se aplică, cu excepția cazului în care persoana vizată, în scopul exercitării drepturilor sale în temeiul respectivelor articole, oferă informații suplimentare care permit identificarea sa.

CAPITOLUL III

Drepturile persoanei vizate

Secțiunea 1

Transparență și modalități

Articolul 12 Transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate (1) Operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informații menționate la [articolele 13](#) și [14](#) și orice comunicări în temeiul [articolelor 15-22](#) și [34](#) referitoare la

prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil. Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

(2) Operatorul facilitează exercitarea drepturilor persoanei vizate în temeiul [articolelor 15-22](#). În cazurile menționate la articolul 11 [alineatul \(2\)](#), operatorul nu refuză să dea curs cererii persoanei vizate de a-și exercita drepturile în conformitate cu [articolele 15-22](#), cu excepția cazului în care operatorul demonstrează că nu este în măsură să identifice persoana vizată.

(3) Operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri în temeiul [articolelor 15-22](#), fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.

(4) Dacă nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoana vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară.

(5) Informațiile furnizate în temeiul [articolelor 13](#) și [14](#) și orice comunicare și orice măsuri luate în temeiul [articolelor 15-22](#) și [34](#) sunt oferite gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate:

(a) fie să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;

(b) fie să refuze să dea curs cererii.

În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

(6) Fără a aduce atingere [articolului 11](#), în cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea menționată la [articolele 15-21](#), operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

(7) Informațiile care urmează să fie furnizate persoanelor vizate în temeiul [articolelor 13](#) și [14](#) pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea trebuie să poată fi citite automat.

(8) Comisia este împuternicită să adopte acte delegate în conformitate cu [articolul 92](#) în vederea determinării informațiilor care urmează să fie prezentate de pictograme și a procedurilor pentru furnizarea de pictograme standardizate.

Secțiunea 2

Informare și acces la date cu caracter personal

Articolul 13 Informații care se furnizează în cazul în care datele cu caracter personal sunt colectate de la persoana vizată (1) În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obținerii acestor date cu caracter personal, furnizează persoanei vizate toate informațiile următoare:

- (a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
- (b) datele de contact ale responsabilului cu protecția datelor, după caz;
- (c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- (d) în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) [litera \(f\)](#), interesele legitime urmărite de operator sau de o parte terță;
- (e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- (f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menționate la [articolul 46](#) sau [47](#) sau la articolul 49 [alineatul \(1\)](#) al doilea paragraf, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.

(2) În plus față de informațiile menționate la [alineatul \(1\)](#), în momentul în care datele cu caracter personal sunt obținute, operatorul furnizează persoanei vizate următoarele informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă:

- (a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- (b) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
- (c) atunci când prelucrarea se bazează pe articolul 6 alineatul (1) [litera \(a\)](#) sau pe articolul 9 alineatul (2) [litera \(a\)](#), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
- (d) dreptul de a depune o plângere în fața unei autorități de supraveghere;
- (e) dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;
- (f) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la articolul 22 [alineatele \(1\)](#) și [\(4\)](#), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(3) În cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte

de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu [alineatul \(2\)](#).

(4) [Alineatele \(1\), \(2\) și \(3\)](#) nu se aplică dacă și în măsura în care persoana vizată deține deja informațiile respective.

Articolul 14 Informații care se furnizează în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată (1) În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informații:

(a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;

(b) datele de contact ale responsabilului cu protecția datelor, după caz;

(c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;

(d) categoriile de date cu caracter personal vizate;

(e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;

(f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menționate la [articolul 46](#) sau [47](#) sau la articolul 49 [alineatul \(1\)](#) al doilea paragraf, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.

(2) Pe lângă informațiile menționate la [alineatul \(1\)](#), operatorul furnizează persoanei vizate următoarele informații necesare pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată:

(a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

(b) în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) [litera \(f\)](#), interesele legitime urmărite de operator sau de o parte terță;

(c) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării și a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;

(d) atunci când prelucrarea se bazează pe articolul 6 alineatul (1) [litera \(a\)](#) sau pe articolul 9 alineatul (2) [litera \(a\)](#), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;

(e) dreptul de a depune o plângere în fața unei autorități de supraveghere;

(f) sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public;

(g) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la articolul 22 [alineatele \(1\) și \(4\)](#), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(3) Operatorul furnizează informațiile menționate la [alineatele \(1\) și \(2\)](#):

(a) într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;

(b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă; sau

(c) dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.

(4) În cazul în care operatorul intenționează să prelucrez ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obținute, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu [alineatul \(2\)](#).

(5) [Alineatele \(1\) - \(4\)](#) nu se aplică dacă și în măsura în care:

(a) persoana vizată deține deja informațiile;

(b) furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva condițiilor și a garanțiilor prevăzute la articolul 89 [alineatul \(1\)](#), sau în măsura în care obligația menționată la alineatul (1) din prezentul articol este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective. În astfel de cazuri, operatorul ia măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate, inclusiv punerea informațiilor la dispoziția publicului;

(c) obținerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern sub incidența căruia intră operatorul și care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau

(d) în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligații legale de a păstra secretul.

Articolul 15 Dreptul de acces al persoanei vizate (1) Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrez sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații:

(a) scopurile prelucrării;

(b) categoriile de date cu caracter personal vizate;

(c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale;

(d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

(e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;

(f) dreptul de a depune o plângere în fața unei autorități de supraveghere;

(g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;

(h) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la articolul 22 [alineatele \(1\) și \(4\)](#), precum și, cel puțin în cazurile respective, informații pertinente privind logica

utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(2) În cazul în care datele cu caracter personal sunt transferate către o țară terță sau o organizație internațională, persoana vizată are dreptul să fie informată cu privire la garanțiile adecvate în temeiul [articolului 46](#) referitoare la transfer.

(3) Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative. În cazul în care persoana vizată introduce cererea în format electronic și cu excepția cazului în care persoana vizată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent.

(4) Dreptul de a obține o copie menționată la [alineatul \(3\)](#) nu aduce atingere drepturilor și libertăților altora.

Secțiunea 3 Rectificare și ștergere

Articolul 16 Dreptul la rectificare Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

Articolul 17 Dreptul la ștergerea datelor ("dreptul de a fi uitat") (1) Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:

(a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

(b) persoana vizată își retrace consimțământul pe baza căruia are loc prelucrarea, în conformitate cu articolul 6 alineatul (1) [litera \(a\)](#) sau cu articolul 9 [alineatul \(2\)](#) litera (a), și nu există niciun alt temei juridic pentru prelucrarea;

(c) persoana vizată se opune prelucrării în temeiul articolului 21 [alineatul \(1\)](#) și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării în temeiul articolului 21 [alineatul \(2\)](#);

(d) datele cu caracter personal au fost prelucrate ilegal;

(e) datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul;

(f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la articolul 8 [alineatul \(1\)](#).

(2) În cazul în care operatorul a făcut publice datele cu caracter personal și este obligat, în temeiul alineatului (1), să le șteargă, operatorul, ținând seama de tehnologia disponibilă și de costul implementării, ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care

prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

(3) Alineatele (1) și (2) nu se aplică în măsura în care prelucrarea este necesară:

(a) pentru exercitarea dreptului la liberă exprimare și la informare;

(b) pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este investit operatorul;

(c) din motive de interes public în domeniul sănătății publice, în conformitate cu articolul 9 alineatul (2) [literele \(h\) și \(i\)](#) și cu articolul 9 [alineatul \(3\)](#);

(d) în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 [alineatul \(1\)](#), în măsura în care dreptul menționat la alineatul (1) este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau

(e) pentru constatarea, exercitarea sau apărarea unui drept în instanță.

Articolul 18 Dreptul la restricționarea prelucrării (1) Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării în cazul în care se aplică unul din următoarele cazuri:

(a) persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;

(b) prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;

(c) operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță; sau

(d) persoana vizată s-a opus prelucrării în conformitate cu articolul 21 [alineatul \(1\)](#), pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

(2) În cazul în care prelucrarea a fost restricționată în temeiul alineatului (1), astfel de date cu caracter personal pot, cu excepția stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

(3) O persoană vizată care a obținut restricționarea prelucrării în temeiul [alineatului \(1\)](#) este informată de către operator înainte de ridicarea restricției de prelucrare.

Articolul 19 Obligația de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate în conformitate cu [articolul 16](#), articolul 17 [alineatul \(1\)](#) și [articolul 18](#), cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

Articolul 20 Dreptul la portabilitatea datelor (1) Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, în cazul în care:

- (a) prelucrarea se bazează pe consimțământ în temeiul articolului 6 alineatul (1) [litera \(a\)](#) sau al articolului 9 alineatul (2) [litera \(a\)](#) sau pe un contract în temeiul articolului 6 alineatul (1) [litera \(b\)](#); și
- (b) prelucrarea este efectuată prin mijloace automate.

(2) În exercitarea dreptului său la portabilitatea datelor în temeiul alineatului (1), persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic.

(3) Exercițarea dreptului menționat la [alineatul \(1\)](#) din prezentul articol nu aduce atingere [articolului 17](#). Respectivul drept nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este investit operatorul.

(4) Dreptul menționat la [alineatul \(1\)](#) nu aduce atingere drepturilor și libertăților altora.

Secțiunea 4

Dreptul la o poziție și procesul decizional individual automatizat

Articolul 21 Dreptul la opoziție (1) În orice moment, persoana vizată are dreptul să se opună, din motive legate de situația particulară în care se află, prelucrării în temeiul articolului 6 alineatul (1) litera (e) sau (f), a datelor cu caracter personal care o privesc, inclusiv creării de profiluri pe baza respectivelor dispoziții. Operatorul nu mai prelucrează datele cu caracter personal, cu excepția cazului în care operatorul demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

(2) Atunci când prelucrarea datelor cu caracter personal are drept scop marketingul direct, persoana vizată are dreptul de a se opune în orice moment prelucrării în acest scop a datelor cu caracter personal care o privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv.

(3) În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.

(4) Cel târziu în momentul primei comunicări cu persoana vizată, dreptul menționat la [alineatele \(1\)](#) și [\(2\)](#) este adus în mod explicit în atenția persoanei vizate și este prezentat în mod clar și separat de orice alte informații.

(5) În contextual utilizării serviciilor societății informaționale și în pofida Directivei [2002/58/CE](#), persoana vizată își poate exercita dreptul de a se opune prin mijloace automate care utilizează specificații tehnice.

(6) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică sau în scopuri statistice în conformitate cu articolul 89 [alineatul \(1\)](#), persoana vizată, din motive legate de situația sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o

privesc, cu excepția cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

Articolul 22 Procesul decizional individual automatizat, inclusiv crearea de profiluri (1) Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

(2) Alineatul (1) nu se aplică în cazul în care decizia:

(a) este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date;

(b) este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului și care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate; sau

(c) are la bază consimțământul explicit al persoanei vizate.

(3) În cazurile menționate la alineatul (2) [literele \(a\)](#) și [\(c\)](#), operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia.

(4) Deciziile menționate la [alineatul \(2\)](#) nu au la bază categoriile speciale de date cu caracter personal menționate la articolul 9 [alineatul \(1\)](#), cu excepția cazului în care se aplică articolul 9 alineatul (2) [litera \(a\)](#) sau [\(g\)](#) și în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate.

Secțiunea 5 Restricții

Articolul 23 Restricții (1) Dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la [articolele 12-22](#) și [34](#), precum și la [articolul 5](#) în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la [articolele 12-22](#), atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura:

(a) securitatea națională;

(b) apărarea;

(c) securitatea publică;

(d) prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;

(e) alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale;

(f) protejarea independenței judiciare și a procedurilor judiciare;

- (g) prevenirea, investigarea, depistarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate;
 - (h) funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale în cazurile menționate la literale (a)-(e) și (g);
 - (i) protecția persoanei vizate sau a drepturilor și libertăților altora;
 - (j) punerea în aplicare a pretențiilor de drept civil.
- (2) În special, orice măsură legislativă menționată la [alineatul \(1\)](#) conține dispoziții specifice cel puțin, dacă este cazul, în ceea ce privește:
- (a) scopurile prelucrării sau ale categoriilor de prelucrare;
 - (b) categoriile de date cu caracter personal;
 - (c) domeniul de aplicare al restricțiilor introduse;
 - (d) garanțiile pentru a preveni abuzurile sau accesul sau transferul ilegal;
 - (e) menționarea operatorului sau a categoriilor de operatori;
 - (f) perioadele de stocare și garanțiile aplicabile având în vedere natura, domeniul de aplicare și scopurile prelucrării sau ale categoriilor de prelucrare;
 - (g) riscurile pentru drepturile și libertățile persoanelor vizate; și
 - (h) dreptul persoanelor vizate de a fi informate cu privire la restricție, cu excepția cazului în care acest lucru poate aduce atingere scopului restricției.

CAPITOLUL IV

Operatorul și persoana împuternicită de operator

Secțiunea 1

Obligații generale

Articolul 24 Responsabilitatea operatorului (1) Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar.

(2) Atunci când sunt proporționale în raport cu operațiunile de prelucrare, măsurile menționate la alineatul (1) includ punerea în aplicare de către operator a unor politici adecvate de protecție a datelor.

(3) Aderarea la coduri de conduită aprobate, menționate la [articolul 40](#), sau la un mecanism de certificare aprobat, menționat la [articolul 42](#), poate fi utilizată ca element care să demonstreze respectarea obligațiilor de către operator.

Articolul 25 Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (1) Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru

drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.

(2) Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane.

(3) Un mecanism de certificare aprobat în conformitate cu [articolul 42](#) poate fi utilizat drept element care să demonstreze îndeplinirea cerințelor prevăzute la alineatele (1) și (2) ale prezentului articol.

Articolul 26 Operatori asociați (1) În cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați. Ei stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul prezentului regulament, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute la [articolele 13 și 14](#), prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

(2) Acordul menționat la alineatul (1) reflectă în mod adecvat rolurile și raporturile respective ale operatorilor asociați față de persoanele vizate. Esența acestui acord este făcută cunoscută persoanei vizate.

(3) Indiferent de clauzele acordului menționat la alineatul (1), persoana vizată își poate exercita drepturile în temeiul prezentului regulament cu privire la și în raport cu fiecare dintre operatori.

Articolul 27 Reprezentanții operatorilor sau ai persoanelor împuternicite de operatori care nu își au sediul în Uniune (1) În cazul în care se aplică articolul 3 [alineatul \(2\)](#), operatorul sau persoana împuternicită de operator desemnează în scris un reprezentant în Uniune.

(2) Obligația prevăzută la alineatul (1) din prezentul articol nu se aplică:

(a) prelucrării care are un caracter ocazional, care nu include, pe scară largă, prelucrarea unor categorii speciale de date, astfel cum se prevede la articolul 9 [alineatul \(1\)](#), sau prelucrarea unor date cu caracter personal referitoare la condamnări penale și infracțiuni menționată la [articolul 10](#), și care este puțin susceptibilă de a genera un risc pentru drepturile și libertățile persoanelor, ținând cont de natura, contextul, domeniul de aplicare și scopurile prelucrării; sau

(b) unei autorități sau unui organism public.

(3) Reprezentantul își are sediul în unul dintre statele membre în care se află persoanele vizate ale căror date cu caracter personal sunt prelucrate în legătură cu furnizarea de bunuri și servicii sau al căror comportament este monitorizat.

(4) Reprezentantul primește din partea operatorului sau a persoanei împuternicite de operator un mandat prin care autoritățile de supraveghere și persoanele vizate, în special, se pot adresa reprezentantului, în plus față de operator sau persoana împuternicită de operator sau în locul acestora, cu privire la toate chestiunile legate de prelucrarea, în scopul asigurării respectării prezentului regulament.

(5) Desemnarea unui reprezentant de către operator sau persoana împuternicită de operator nu aduce atingere acțiunilor în justiție care ar putea fi introduse împotriva operatorului sau persoanei împuternicite de operator înseși.

Articolul 28 Persoana împuternicită de operator (1) În cazul în care prelucrarea urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate.

(2) Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecții față de aceste modificări.

(3) Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoana împuternicită de operator:

(a) prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, inclusiv în ceea ce privește transferurile de date cu caracter personal către o țară terță sau o organizație internațională, cu excepția cazului în care această obligație îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

(b) se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație statutară adecvată de confidențialitate;

(c) adoptă toate măsurile necesare în conformitate cu [articolul 32](#);

(d) respectă condițiile menționate la alineatele (2) și (4) privind recrutarea unei alte persoane împuternicite de operator;

(e) ținând seama de natura prelucrării, oferă asistență operatorului prin măsuri tehnice și organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligației operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute în capitolul III;

(f) ajută operatorul să asigure respectarea obligațiilor prevăzute la [articolele 32-36](#), ținând seama de caracterul prelucrării și informațiile aflate la dispoziția persoanei împuternicite de operator;

(g) la alegerea operatorului, șterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;

(h) pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute la prezentul articol, permite desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea.

În ceea ce privește primul paragraf litera (h), persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucțiune încalcă prezentul regulament sau alte dispoziții din dreptul intern sau din dreptul Uniunii referitoare la protecția datelor.

(4) În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator, astfel cum se prevede la alineatul (3), revin celei de a doua persoane împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul dreptului Uniunii sau al dreptului intern, în special furnizarea de garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentului regulament. În cazul în care această a doua persoană împuternicită nu își respectă obligațiile privind protecția datelor, persoana împuternicită inițială rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor acestei a doua persoane împuternicite.

(5) Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, menționat la [articolul 40](#), sau la un mecanism de certificare aprobat, menționat la [articolul 42](#), poate fi utilizată ca element prin care să se demonstreze existența garanțiilor suficiente menționate la alineatele (1) și (4) din prezentul articol.

(6) Fără a aduce atingere unui contract individual încheiat între operator și persoana împuternicită de operator, contractul sau celălalt act juridic menționat la alineatele (3) și (4) din prezentul articol se poate baza, integral sau parțial, pe clauze contractuale standard menționate la alineatele (7) și (8) din prezentul articol, inclusiv atunci când fac parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator în temeiul [articolelor 42 și 43](#).

(7) Comisia poate să prevadă clauze contractuale standard pentru aspectele menționate la alineatele (3) și (4) din prezentul articol și în conformitate cu procedura de examinare menționată la [articolul 93 alineatul \(2\)](#).

(8) O autoritate de supraveghere poate să adopte clauze contractuale standard pentru aspectele menționate la alineatele (3) și (4) din prezentul articol și în conformitate cu mecanismul pentru asigurarea coerenței menționat la [articolul 63](#).

(9) Contractul sau celălalt act juridic menționat la alineatele (3) și (4) se formulează în scris, inclusiv în format electronic.

(10) Fără a aduce atingere [articolelor 82, 83 și 84](#), în cazul în care o persoană împuternicită de operator încalcă prezentul regulament, prin stabilirea scopurilor și mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă.

Articolul 29 Desfășurarea activității de prelucrare sub autoritatea operatorului sau a persoanei împuternicite de operator Persoana împuternicită de operator și orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru.

Articolul 30 Evidențele activităților de prelucrare (1) Fiecare operator și, după caz, reprezentantul acestuia păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor. Respectiva evidență cuprinde toate următoarele informații:

(a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;

(b) scopurile prelucrării;

(c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;

(d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;

(e) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor menționate la articolul 49 [alineatul \(1\)](#) al doilea paragraf, documentația care dovedește existența unor garanții adecvate;

(f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;

(g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 [alineatul \(1\)](#).

(2) Fiecare persoană împuternicită de operator și, după caz, reprezentantul persoanei împuternicite de operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind:

(a) numele și datele de contact ale persoanei sau persoanelor împuternicite de operator și ale fiecărui operator în numele căruia acționează această persoană (aceste persoane), precum și, după caz, ale reprezentantului operatorului sau ale reprezentantului persoanei împuternicite de operator, și ale responsabilului cu protecția datelor;

(b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;

(c) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor prevăzute la articolul 49 [alineatul \(1\)](#) al doilea paragraf, documentația care dovedește existența unor garanții adecvate;

(d) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 [alineatul \(1\)](#).

(3) Evidențele menționate la alineatele (1) și (2) se formulează în scris, inclusiv în format electronic.

(4) Operatorul sau persoana împuternicită de acesta, precum și, după caz, reprezentantul operatorului sau al persoanei împuternicite de operator pun evidențele la dispoziția autorității de supraveghere, la cererea acesteia.

(5) Obligațiile menționate la alineatele 1 și 2 nu se aplică unei întreprinderi sau organizații cu mai puțin de 250 de angajați, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 [alineatul \(1\)](#), sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează la [articolul 10](#).

Articolul 31 Cooperarea cu autoritatea de supraveghere Operatorul și persoana împuternicită de operator și, după caz, reprezentantul acestora cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor acesteia.

Secțiunea 2

Securitatea datelor cu caracter personal

Articolul 32 Securitatea prelucrării (1) Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

- (a) pseudonimizarea și criptarea datelor cu caracter personal;
- (b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
- (c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- (d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

(2) La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

(3) Aderarea la un cod de conduită aprobat, menționat la [articolul 40](#), sau la un mecanism de certificare aprobat, menționat la [articolul 42](#), poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute la alineatul (1) din prezentul articol.

(4) Operatorul și persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.

Articolul 33 Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal (1) În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere competente în temeiul articolului 55, fără întârzieri

nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea către autoritatea de supraveghere nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată pentru întârziere.

(2) Persoana împuternicită de operator înștiințează operatorul fără întârzieri nejustificate după ce ia cunoștință de o încălcare a securității datelor cu caracter personal.

(3) Notificarea menționată la alineatul (1) cel puțin:

(a) descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;

(b) comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;

(c) descrie consecințele probabile ale încălcării securității datelor cu caracter personal;

(d) descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

(4) Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

(5) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acestora și a măsurilor de remediere întreprinse. Această documentație permite autorității de supraveghere să verifice conformitatea cu prezentul articol.

Articolul 34 Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal (1) În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

(2) În informarea transmisă persoanei vizate prevăzută la alineatul (1) din prezentul articol se include o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile și măsurile menționate la articolul 33 alineatul (3) [literele \(b\), \(c\) și \(d\)](#).

(3) Informarea persoanei vizate menționată la alineatul (1) nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:

(a) operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

(b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate menționat la alineatul (1) nu mai este susceptibil să se materializeze;

(c) ar necesita un efort disproporționat. În această situație, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

(4) În cazul în care operatorul nu a comunicat deja încălcarea securității datelor cu caracter personal către persoana vizată, autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securității datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condițiile menționate la alineatul (3) sunt îndeplinite.

Secțiunea 3

Evaluarea impactului asupra protecției datelor și consultarea prealabilă

Articolul 35 Evaluarea impactului asupra protecției datelor (1) Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.

(2) La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat.

(3) Evaluarea impactului asupra protecției datelor menționată la alineatul (1) se impune mai ales în cazul:

(a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

(b) prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 9 [alineatul \(1\)](#), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la [articolul 10](#); sau

(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

(4) Autoritatea de supraveghere întocmește și publică o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor, în conformitate cu alineatul (1). Autoritatea de supraveghere comunică aceste liste comitetului menționat la [articolul 68](#).

(5) Autoritatea de supraveghere poate, de asemenea, să stabilească și să pună la dispoziția publicului o listă a tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor. Autoritatea de supraveghere comunică aceste liste comitetului.

(6) Înainte de adoptarea listelor menționate la alineatele (4) și (5), autoritatea de supraveghere competentă aplică mecanismul pentru asigurarea coerenței menționat la [articolul 63](#) în cazul în care aceste liste implică activități de prelucrare care presupun furnizarea de bunuri sau prestarea de servicii către persoane vizate sau monitorizarea comportamentului acestora în mai multe state membre ori care pot afecta în mod substanțial libera circulație a datelor cu caracter personal în cadrul Uniunii.

(7) Evaluarea conține cel puțin:

(a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

(b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

(c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la alineatul (1); și

(d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

(8) La evaluarea impactului operațiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevante, se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate menționate la [articolul 40](#), în special în vederea unei evaluări a impactului asupra protecției datelor.

(9) Operatorul solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.

(10) Atunci când prelucrarea în temeiul articolului 6 alineatul (1) [litera \(c\)](#) sau [\(e\)](#) are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidența căruia intră operatorul, iar dreptul respectiv reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, alineatele (1)-(7) nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înainte desfășurării activităților de prelucrare.

(11) Acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

Articolul 36 Consultarea prealabilă (1) Operatorul consultă autoritatea de supraveghere înainte de prelucrarea atunci când evaluarea impactului asupra protecției datelor prevăzută la [articolul 35](#) indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.

(2) Atunci când consideră că prelucrarea prevăzută menționată la alineatul (1) ar încălca prezentul regulament, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris operatorului și, după caz, persoanei împuternicite de operator, în cel mult opt săptămâni de la primirea cererii de consultare, și își poate utiliza oricare dintre competențele menționate la [articolul 58](#). Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute. Autoritatea de supraveghere informează operatorul și, după caz, persoana împuternicită de operator, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când autoritatea de supraveghere a obținut informațiile pe care le-a solicitat în scopul consultării.

(3) Atunci când consultă autoritatea de supraveghere în conformitate cu alineatul (1), operatorul îi furnizează acesteia:

(a) dacă este cazul, responsabilitățile respective ale operatorului, ale operatorilor asociați și ale persoanelor împuternicite de operator implicate în activitățile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;

(b) scopurile și mijloacele prelucrării preconizate;

(c) măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților persoanelor vizate, în conformitate cu prezentul regulament;

(d) dacă este cazul, datele de contact ale responsabilului cu protecția datelor;

(e) evaluarea impactului asupra protecției datelor prevăzută la [articolul 35](#); și

(f) orice alte informații solicitate de autoritatea de supraveghere.

(4) Statele membre consultă autoritatea de supraveghere în cadrul procesului de pregătire a unei propuneri de măsură legislativă care urmează să fie adoptată de un parlament național sau a unei măsuri de reglementare întemeiate pe o astfel de măsură legislativă, care se referă la prelucrarea.

(5) În pofida alineatului (1), dreptul intern poate impune operatorilor să se consulte cu autoritatea de supraveghere și să obțină în prealabil autorizarea din partea acesteia în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecția socială și sănătatea publică.

Secțiunea 4

Responsabilul cu protecția datelor

Articolul 37 Desemnarea responsabilului cu protecția datelor (1) Operatorul și persoana împuternicită de operator desemnează un responsabil cu protecția datelor ori de câte ori:

(a) prelucrarea este efectuată de o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;

(b) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă; sau

(c) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date în temeiul articolului 9 sau a unor date cu caracter personal referitoare la condamnări penale și infracțiuni, menționată la articolul 10.

(2) Un grup de întreprinderi poate numi un responsabil cu protecția datelor unic, cu condiția ca responsabilul cu protecția datelor să fie ușor accesibil din fiecare întreprindere.

(3) În cazul în care operatorul sau persoana împuternicită de operator este o autoritate publică sau un organism public, poate fi desemnat un responsabil cu protecția datelor unic pentru mai multe dintre aceste autorități sau organisme, luând în considerare structura organizatorică și dimensiunea acestora.

(4) În alte cazuri decât cele menționate la alineatul (1), operatorul sau persoana împuternicită de operator ori asociațiile și alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot desemna sau, acolo unde dreptul Uniunii sau dreptul intern solicită

acest lucru, desemnează un responsabil cu protecția datelor. Responsabilul cu protecția datelor poate să acționeze în favoarea unor astfel de asociații și alte organisme care reprezintă operatori sau persoane împuternicite de operatori.

(5) Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la [articolul 39](#).

(6) Responsabilul cu protecția datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să își îndeplinească sarcinile în baza unui contract de servicii.

(7) Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecția datelor și le comunică autorității de supraveghere.

Articolul 38 Funcția responsabilului cu protecția datelor (1) Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal.

(2) Operatorul și persoana împuternicită de operator sprijină responsabilul cu protecția datelor în îndeplinirea sarcinilor menționate la [articolul 39](#), asigurându-i resursele necesare pentru executarea acestor sarcini, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate.

(3) Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini. Acesta nu este demis sau sancționat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.

(4) Persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentului regulament.

(5) Responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.

(6) Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese.

Articolul 39 Sarcinile responsabilului cu protecția datelor (1) Responsabilul cu protecția datelor are cel puțin următoarele sarcini:

(a) informarea și consilierea operatorului, sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;

(b) monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

(c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu [articolul 35](#);

(d) cooperarea cu autoritatea de supraveghere;

(e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la [articolul 36](#), precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

(2) În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.

Secțiunea 5 Coduri de conduită și certificare

Articolul 40 Coduri de conduită (1) Statele membre, autoritățile de supraveghere, comitetul și Comisia încurajează elaborarea de coduri de conduită menite să contribuie la buna aplicare a prezentului regulament, ținând seama de caracteristicile specifice ale diverselor sectoare de prelucrare și de nevoile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii.

(2) Asociațiile și alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot pregăti coduri de conduită sau le pot modifica sau extinde pe cele existente, în scopul de a specifica modul de aplicare a prezentului regulament, cum ar fi în ceea ce privește:

(a) prelucrarea în mod echitabil și transparent;

(b) interesele legitime urmărite de operatori în contexte specifice;

(c) colectarea datelor cu caracter personal;

(d) pseudonimizarea datelor cu caracter personal;

(e) informarea publicului și a persoanelor vizate;

(f) exercitarea drepturilor persoanelor vizate;

(g) informarea și protejarea copiilor și modalitatea în care trebuie obținut consimțământul titularilor răspunderii părintești asupra copiilor;

(h) măsurile și procedurile menționate la [articolele 24 și 25](#) și măsurile de asigurare a securității prelucrării, menționate la [articolul 32](#);

(i) notificarea autorităților de supraveghere cu privire la încălcările securității datelor cu caracter personal și informarea persoanelor vizate cu privire la aceste încălcări;

(j) transferul de date cu caracter personal către țări terțe sau organizații internaționale; sau

(k) proceduri extrajudiciare și alte proceduri de soluționare a litigiilor pentru soluționarea litigiilor între operatori și persoanele vizate în ceea ce privește prelucrarea, fără a aduce atingere drepturilor persoanelor vizate, în temeiul [articolelor 77 și 79](#).

(3) La codurile de conduită aprobate în temeiul alineatului (5) din prezentul articol și care au o valabilitate generală în temeiul alineatului (9) din prezentul articol pot adera nu numai operatorii sau persoanele împuternicite de operatori care fac obiectul prezentului regulament, ci și operatorii sau persoanele împuternicite de operatori care nu fac obiectul prezentului regulament în temeiul

[articolului 3](#), în scopul de a oferi garanții adecvate în cadrul transferurilor de date cu caracter personal către țări terțe sau organizații internaționale în condițiile menționate la articolul 46 alineatul (2) [litera \(e\)](#). Acești operatori sau persoane împuternicite de operatori își asumă angajamente cu caracter obligatoriu și executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, în scopul aplicării garanțiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.

(4) Codul de conduită prevăzut la alineatul (2) din prezentul articol cuprinde mecanisme care permit organismului menționat la articolul 41 [alineatul \(1\)](#) să efectueze monitorizarea obligatorie a respectării dispozițiilor acestuia de către operatorii sau persoanele împuternicite de operatori care se angajează să îl aplice, fără a aduce atingere sarcinilor și competențelor autorităților de supraveghere care sunt competente în temeiul articolului 55 sau 56.

(5) Asociațiile și alte organisme menționate la alineatul (2) din prezentul articol care intenționează să pregătească un cod de conduită sau să modifice sau să extindă un cod existent transmit proiectul de cod, de modificare sau de extindere autorității de supraveghere care este competentă în temeiul [articolului 55](#). Autoritatea de supraveghere emite un aviz cu privire la conformitatea cu prezentul regulament a proiectului de cod, de modificare sau de extindere și îl aprobă în cazul în care se constată că acesta oferă garanții adecvate suficiente.

(6) În cazul în care proiectul de cod, de modificare sau de extindere este aprobat în conformitate cu alineatul (5), iar codul de conduită în cauză nu are legătură cu activitățile de prelucrare din mai multe state membre, autoritatea de supraveghere înregistrează și publică codul.

(7) În cazul în care un proiect de cod de conduită, de modificare sau de extindere are legătură cu activitățile de prelucrare din mai multe state membre, înainte de aprobare, autoritatea de supraveghere competentă în temeiul [articolului 55](#) îl transmite, prin procedura menționată la [articolul 63](#), comitetului, care emite un aviz cu privire la conformitatea cu prezentul regulament a proiectului respectiv, sau, în situația menționată la alineatul (3) din prezentul articol, oferă garanții adecvate.

(8) În cazul în care avizul menționat la alineatul (7) confirmă conformitatea cu prezentul regulament a proiectului de cod, de modificare sau de extindere sau în cazul în care, în situația menționată la alineatul (3), oferă garanții adecvate, comitetul transmite avizul său Comisiei.

(9) Comisia poate adopta acte de punere în aplicare pentru a decide că codul de conduită, modificarea sau extinderea aprobate care i-au fost prezentate în temeiul alineatului (8) din prezentul articol au valabilitate generală în Uniune. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 93 [alineatul \(2\)](#).

(10) Comisia asigură publicitatea adecvată pentru codurile aprobate asupra cărora s-a decis că au valabilitate generală în conformitate cu alineatul (9).

(11) Comitetul regrupează toate codurile de conduită, modificările și extinderile aprobate într-un registru și le pune la dispoziția publicului prin mijloace corespunzătoare.

Articolul 41 Monitorizarea codurilor de conduită aprobate (1) Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente în temeiul [articolelor 57](#) și 58, monitorizarea respectării unui cod de conduită în temeiul [articolului 40](#) poate fi realizată de un organism care

dispune de un nivel adecvat de expertiză în legătură cu obiectul codului și care este acreditat în acest scop de autoritatea de supraveghere competentă.

(2) Un organism menționat la alineatul (1) poate fi acreditat pentru monitorizarea respectării unui cod de conduită dacă:

(a) a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, independența și expertiza sa în legătură cu obiectul codului;

(b) a instituit proceduri care îi permit să evalueze eligibilitatea operatorilor și a persoanelor împuternicite de operatori în vederea aplicării codului, să monitorizeze respectarea de către aceștia a dispozițiilor codului și să revizuiască periodic funcționarea acestuia;

(c) a instituit proceduri și structuri pentru tratarea plângerilor privind încălcări ale codului sau privind modul în care codul a fost sau este pus în aplicare de un operator sau o persoană împuternicită de operator, precum și pentru asigurarea transparenței acestor proceduri și structuri pentru persoanele vizate și pentru public; și

(d) a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, că sarcinile și atribuțiile sale nu creează conflicte de interese.

(3) Autoritatea de supraveghere competentă transmite proiectul de cerințe pentru acreditarea unui organism menționat la alineatul (1) din prezentul articol comitetului, în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 63.

(4) Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente și dispozițiilor capitolului VIII, un organism menționat la alineatul (1) din prezentul articol ia măsuri corespunzătoare, sub rezerva unor garanții adecvate, în cazul încălcării codului de către un operator sau o persoană împuternicită de operator, inclusiv prin suspendarea sau excluderea respectivului operator sau a respectivei persoane din cadrul codului. Organismul în cauză informează autoritatea de supraveghere competentă cu privire la aceste măsuri și la motivele care le-au determinat.

(5) Autoritatea de supraveghere competentă revocă acreditarea unui organism menționat la alineatul (1) în cazul în care nu mai sunt îndeplinite cerințele pentru acreditare sau măsurile luate de organismul în cauză încalcă prezentul regulament.

(6) Prezentul articol nu se aplică prelucrării efectuate de autorități și organisme publice.

Articolul 42 Certificare (1) Statele membre, autoritățile de supraveghere, comitetul și Comisia încurajează, în special la nivelul Uniunii, instituirea de mecanisme de certificare în domeniul protecției datelor, precum și de sigilii și mărci în acest domeniu, care să permită demonstrarea faptului că operațiunile de prelucrare efectuate de operatori și de persoanele împuternicite de operatori respectă prezentul regulament. Sunt luate în considerare necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii.

(2) Mecanismele de certificare din domeniul protecției datelor, sigiliile sau mărcile aprobate în temeiul alineatului (5) din prezentul articol sunt instituite nu numai pentru a fi respectate de operatorii sau de persoanele împuternicite de operatori care fac obiectul prezentului regulament, ci și pentru a demonstra existența unor garanții adecvate oferite de operatorii sau de persoanele împuternicite de operatori care nu fac obiectul prezentului regulament, în temeiul [articolului 3](#), în cadrul transferurilor de date cu caracter personal către țări terțe sau organizații internaționale în condițiile menționate la

articolul 46 alineatul (2) [litera \(f\)](#). Acești operatori sau persoane împuternicite de operatori își asumă angajamente cu caracter obligatoriu și executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, în scopul aplicării garanțiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.

(3) Certificarea este voluntară și disponibilă prin intermediul unui proces transparent.

(4) Certificarea în conformitate cu prezentul articol nu reduce responsabilitatea operatorului sau a persoanei împuternicite de operator de a respecta prezentul regulament și nu aduce atingere sarcinilor și competențelor autorităților de supraveghere care sunt competente în temeiul [articolului 55](#) sau [56](#).

(5) Organismele de certificare menționate la [articolul 43](#) sau autoritatea de supraveghere competentă emit o certificare în temeiul prezentului articol, pe baza criteriilor aprobate de către autoritatea de supraveghere competentă respectivă în temeiul articolului 58 [alineatul \(3\)](#), sau de către comitet în temeiul articolului 63. În cazul în care criteriile sunt aprobate de comitet, aceasta poate duce la o certificare comună, și anume sigiliul european privind protecția datelor.

(6) Operatorul sau persoana împuternicită de operator care supune activitățile sale de prelucrare mecanismului de certificare oferă organismului de certificare menționat la [articolul 43](#) sau, după caz, autorității de supraveghere competente, toate informațiile necesare pentru desfășurarea procedurii de certificare, precum și accesul la activitățile de prelucrare respective.

(7) Certificarea este eliberată unui operator sau unei persoane împuternicite de operator pentru o perioadă maximă de trei ani și poate fi reînnoită în aceleași condiții, cu condiția ca criteriile relevante să fie îndeplinite în continuare. Certificarea este retrasă, după caz, de către organismele de certificare menționate la articolul 43 sau de către autoritatea de supraveghere competentă în cazul în care nu mai sunt îndeplinite criteriile pentru certificare.

(8) Comitetul regrupează toate mecanismele de certificare și sigiliile și mărcile de protecție a datelor într-un registru și le pune la dispoziția publicului prin orice mijloc corespunzător.

Articolul 43 Organisme de certificare (1) Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente, prevăzute la [articolele 57](#) și [58](#), organismele de certificare care dispun de un nivel adecvat de competență în domeniul protecției datelor, după ce informează autoritatea de supraveghere pentru a-i permite să își exercite competențele în temeiul articolului 58 alineatul (2) [litera \(h\)](#), emit și reînnoiesc certificarea. Statele membre se asigură că aceste organisme de certificare sunt acreditate de către una sau amândouă dintre următoarele entități:

(a) autoritatea de supraveghere care este competentă în temeiul [articolului 55](#) sau [56](#);

(b) organismul național de acreditare desemnat în conformitate cu Regulamentul (CE) [nr. 765/2008](#) al Parlamentului European și al Consiliului în conformitate cu standardul EN-ISO/IEC 17065/2012 și cu cerințele suplimentare stabilite de autoritatea de supraveghere care este competentă în temeiul [articolului 55](#) sau [56](#).

(2) Un organism de certificare menționat la alineatul (1) este acreditat în conformitate cu alineatul respectiv numai dacă:

(a) a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, independența și expertiza sa în legătură cu obiectul certificării;

(b) s-a angajat să respecte criteriile menționate la articolul 42 [alineatul \(5\)](#) și aprobate de autoritatea de supraveghere care este competentă în temeiul [articolului 55](#) sau [56](#), sau de către comitet în temeiul [articolului 63](#);

(c) a instituit proceduri pentru emiterea, revizuirea periodică și retragerea certificării, a sigiliilor și mărcilor din domeniul protecției datelor;

(d) a instituit proceduri și structuri pentru tratarea plângerilor privind încălcări ale certificării sau privind modul în care certificarea a fost sau este pusă în aplicare de un operator sau o persoană împuternicită de operator, precum și pentru asigurarea transparenței acestor proceduri și structuri pentru persoanele vizate și pentru public; și

(e) a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, că sarcinile și atribuțiile sale nu creează conflicte de interese.

(3) Acreditarea organismelor de certificare menționate la alineatele (1) și (2) din prezentul articol se realizează pe baza cerințelor aprobate de către autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56, sau de către comitet în temeiul articolului 63. În cazul unei acreditări în temeiul alineatului (1) litera (b) din prezentul articol, aceste cerințe le completează pe cele prevăzute în Regulamentul (CE) nr. 765/2008 și normele tehnice care descriu metodele și procedurile organismelor de certificare.

(4) Organismele de certificare menționate la alineatul (1) sunt responsabile cu realizarea unei evaluări adecvate în vederea certificării sau retragerii acestei certificări, fără a aduce atingere responsabilității operatorului sau a persoanei împuternicite de operator de a respecta prezentul regulament. Acreditarea se eliberează pentru o perioadă maximă de cinci ani și poate fi reînnoită în aceleași condiții, cu condiția ca organismul de certificare să îndeplinească cerințele prevăzute în prezentul articol.

(5) Organismele de certificare menționate la alineatul (1) transmite autorităților de supraveghere competente motivele acordării sau retragerii certificării solicitate.

(6) Cerințele menționate la alineatul (3) din prezentul articol și criteriile menționate la articolul 42 alineatul (5) se publică de către autoritatea de supraveghere într-o formă ușor de accesat. Autoritățile de supraveghere transmit, de asemenea, aceste cerințe și criterii comitetului.

(7) Fără a aduce atingere dispozițiilor capitolului VIII, autoritatea de supraveghere competentă sau organismul național de acreditare revocă acreditarea acordată unui organism de certificare în temeiul alineatului (1) din prezentul articol în cazul în care nu sunt sau nu mai sunt îndeplinite condițiile pentru acreditare sau măsurile luate de organismul de acreditare încalcă prezentul regulament.

(8) Comisia este împuternicită să adopte acte delegate în conformitate cu [articolul 92](#), în scopul specificării cerințelor care trebuie luate în considerare pentru mecanismele de certificare din domeniul protecției datelor, menționate la articolul 42 [alineatul \(1\)](#).

(9) Comisia poate adopta acte de punere în aplicare pentru a stabili standarde tehnice pentru mecanismele de certificare și pentru sigiliile și mărcile din domeniul protecției datelor, precum și mecanisme de promovare și recunoaștere a acelor mecanisme de certificare, sigilii și mărci. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 93 [alineatul \(2\)](#).

CAPITOLUL V

Transferurile de date cu caracter personal către țări terțe sau organizații internaționale

Articolul 44 Principiul general al transferurilor Orice date cu caracter personal care fac obiectul prelucrării sau care urmează a fi prelucrate după ce sunt transferate într-o țară terță sau către o organizație internațională pot fi transferate doar dacă, sub rezerva celorlalte dispoziții ale prezentului regulament, condițiile prevăzute în prezentul capitol sunt respectate de operator și de persoana împuternicită de operator, inclusiv în ceea ce privește transferurile ulterioare de date cu caracter personal din țara terță sau de la organizația internațională către o altă țară terță sau către o altă organizație internațională. Toate dispozițiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice garantat prin prezentul regulament nu este subminat.

Articolul 45 Transferuri în temeiul unei decizii privind caracterul adecvat al nivelului de protecție (1) Transferul de date cu caracter personal către o țară terță sau o organizație internațională se poate realiza atunci când Comisia a decis că țara terță, un teritoriu ori unul sau mai multe sectoare specificate din acea țară terță sau organizația internațională în cauză asigură un nivel de protecție adecvat. Transferurile realizate în aceste condiții nu necesită autorizări speciale.

(2) Atunci când evaluează caracterul adecvat al nivelului de protecție, Comisia ține seama, în special, de următoarele elemente:

(a) statul de drept, respectarea drepturilor omului și a libertăților fundamentale, legislația relevantă, atât generală, cât și sectorială, inclusiv privind securitatea publică, apărarea, securitatea națională și dreptul penal, precum și accesul autorităților publice la datele cu caracter personal, precum și punerea în aplicare a acestei legislații, normele de protecție a datelor, normele profesionale și măsurile de securitate, inclusiv normele privind transferul ulterior de date cu caracter personal către o altă țară terță sau organizație internațională, care sunt respectate în țara terță respectivă sau în organizația internațională respectivă, jurisprudența, precum și existența unor drepturi efective și opozabile ale persoanelor vizate și a unor reparatii efective pe cale administrativă și judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate;

(b) existența și funcționarea eficientă a uneia sau mai multor autorități de supraveghere independente în țara terță sau sub jurisdicția cărora intră o organizație internațională, cu responsabilitate pentru asigurarea și impunerea respectării normelor de protecție a datelor, incluzând competențe adecvate de asigurare a respectării aplicării, pentru acordarea de asistență și consiliere persoanelor vizate cu privire la exercitarea drepturilor acestora și pentru cooperarea cu autoritățile de supraveghere din statele membre; și

(c) angajamentele internaționale la care a aderat țara terță sau organizația internațională în cauză sau alte obligații care decurg din convenții sau instrumente obligatorii din punct de vedere juridic, precum și din participarea acestora la sisteme multilaterale sau regionale, mai ales în domeniul protecției datelor cu caracter personal.

(3) Comisia, după ce evaluează caracterul adecvat al nivelului de protecție, poate decide, printr-un act de punere în aplicare, că o țară terță, un teritoriu sau unul sau mai multe sectoare specificate dintr-o

țară terță sau o organizație internațională asigură un nivel de protecție adecvat în sensul alineatului (2) din prezentul articol. Actul de punere în aplicare prevede un mecanism de revizuire periodică, cel puțin o dată la patru ani, care ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională. Actul de punere în aplicare menționează aplicarea geografică și sectorială, și, după caz, identifică autoritatea sau autoritățile de supraveghere menționate la alineatul (2) litera (b) din prezentul articol. Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 93 [alineatul \(2\)](#).

(4) Comisia monitorizează continuu evoluțiile din țările terțe și de la nivelul organizațiilor internaționale care ar putea afecta funcționarea deciziilor adoptate în temeiul alineatului (3) din prezentul articol și a deciziilor adoptate în temeiul articolului 25 [alineatul \(6\)](#) din Directiva 95/46/CE.

(5) În cazul în care informațiile disponibile dezvăluie, în special în urma revizurii menționate la alineatul (3) din prezentul articol, că o țară terță, un teritoriu sau un sector specificat din acea țară terță sau o organizație internațională nu mai asigură un nivel de protecție adecvat în sensul alineatului (2) din prezentul articol, Comisia, dacă este necesar, abrogă, modifică sau suspendă, prin intermediul unui act de punere în aplicare, decizia menționată la alineatul (3) din prezentul articol fără efect retroactiv. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 93 [alineatul \(2\)](#).

Din motive imperioase de urgență, Comisia adoptă acte de punere în aplicare imediat aplicabile în conformitate cu procedura menționată la articolul 93 [alineatul \(3\)](#).

(6) Comisia inițiază consultări cu țara terță sau organizația internațională în vederea remedierii situației care a stat la baza deciziei luate în conformitate cu alineatul (5).

(7) O decizie luată în temeiul alineatului (5) din prezentul articol nu aduce atingere transferurilor de date cu caracter personal către țara terță, un teritoriu sau unul sau mai multe sectoare specificate din acea țară terță sau către organizația internațională în cauză în conformitate cu [articolele 46-49](#).

(8) Comisia publică în Jurnalul Oficial al Uniunii Europene și pe site-ul său o listă a țărilor terțe, a teritoriilor și sectoarelor specificate dintr-o țară terță și a organizațiilor internaționale în cazul cărora a decis că nivelul de protecție adecvat este asigurat sau nu mai este asigurat.

(9) Deciziile adoptate de Comisie în temeiul articolului 25 [alineatul \(6\)](#) din Directiva 95/46/CE rămân în vigoare până când sunt modificate, înlocuite sau abrogate de o decizie a Comisiei adoptată în conformitate cu alineatul (3) sau (5) din prezentul articol.

Articolul 46 Transferuri în baza unor garanții adecvate (1) În absența unei decizii în temeiul [articolului 45 alineatul \(3\)](#), operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o țară terță sau o organizație internațională numai dacă operatorul sau persoana împuternicită de operator a oferit garanții adecvate și cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate.

(2) Garanțiile adecvate menționate la alineatul 1 pot fi furnizate fără să fie nevoie de nicio autorizație specifică din partea unei autorități de supraveghere, prin:

(a) un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;

(b) reguli corporatiste obligatorii în conformitate cu [articolul 47](#);

(c) clauze standard de protecție a datelor adoptate de Comisie în conformitate cu procedura de examinare menționată la articolul 93 [alineatul \(2\)](#);

(d) clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisie în conformitate cu procedura de examinare menționată la articolul 93 [alineatul \(2\)](#);

(e) un cod de conduită aprobat în conformitate cu [articolul 40](#), însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

(f) un mecanism de certificare aprobat în conformitate cu [articolul 42](#), însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

(3) Sub rezerva autorizării din partea autorității de supraveghere competente, garanțiile adecvate menționate la alineatul (1) pot fi furnizate de asemenea, în special, prin:

(a) clauze contractuale între operator sau persoana împuternicită de operator și operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din țara terță sau organizația internațională; sau

(b) dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate.

(4) Autoritatea de supraveghere aplică mecanismul pentru asigurarea coerenței menționat la [articolul 63](#), în cazurile menționate la alineatul (3) din prezentul articol.

(5) Autorizațiile acordate de un stat membru sau de o autoritate de supraveghere în temeiul articolului 26 [alineatul \(2\)](#) din Directiva 95/46/CE sunt valabile până la data la care sunt modificate, înlocuite sau abrogate, dacă este necesar, de respectiva autoritate de supraveghere. Deciziile adoptate de Comisie în temeiul articolului 26 [alineatul \(4\)](#) din Directiva 95/46/CE rămân în vigoare până când sunt modificate, înlocuite sau abrogate, dacă este necesar, de o decizie a Comisiei adoptată în conformitate cu alineatul (2) din prezentul articol.

Articolul 47 Reguli corporatiste obligatorii (1) În conformitate cu mecanismul pentru asigurarea coerenței prevăzut la [articolul 63](#), autoritatea de supraveghere competentă aprobă reguli corporatiste obligatorii, cu condiția ca acestea:

(a) să fie obligatorii din punct de vedere juridic și să se aplice fiecărui membru vizat al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, inclusiv angajaților acestuia, precum și să fie puse în aplicare de membrii în cauză;

(b) să confere, în mod expres, drepturi opozabile persoanelor vizate în ceea ce privește prelucrarea datelor lor cu caracter personal; și

(c) să îndeplinească cerințele prevăzute la alineatul (2).

(2) Regulile corporatiste obligatorii menționate la alineatul (1) precizează cel puțin:

(a) structura și datele de contact ale grupului de întreprinderi sau ale grupului de întreprinderi implicate într-o activitate economică comună și ale fiecăruia dintre membrii săi;

(b) transferurile de date sau setul de transferuri, inclusiv categoriile de date cu caracter personal, tipul prelucrării și scopurile prelucrării, tipurile de persoane vizate afectate și identificarea țării terțe sau a țărilor terțe în cauză;

- (c) caracterul lor juridic obligatoriu, atât pe plan intern, cât și extern;
- (d) aplicarea principiilor generale în materie de protecție a datelor, în special limitarea scopului, reducerea la minimum a datelor, perioadele de stocare limitate, calitatea datelor, protecția datelor începând cu momentul conceperii și protecția implicită, temeiul juridic pentru prelucrare, prelucrarea categoriilor speciale de date cu caracter personal, măsurile de asigurare a securității datelor, precum și cerințele referitoare la transferurile ulterioare către organisme care nu fac obiectul regulilor corporatiste obligatorii;
- (e) drepturile persoanelor vizate în ceea ce privește prelucrarea și mijloacele de exercitare a acestor drepturi, inclusiv dreptul de a nu face obiectul unor decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, în conformitate cu [articolul 22](#), dreptul de a depune o plângere în fața autorității de supraveghere competente și în fața instanțelor competente ale statelor membre, în conformitate cu [articolul 79](#), precum și dreptul de a obține reparații și, după caz, despăgubiri pentru încălcarea regulilor corporatiste obligatorii;
- (f) acceptarea de către operator sau de persoana împuternicită de operator, care își are sediul pe teritoriul unui stat membru, a răspunderii pentru orice încălcare a regulilor corporatiste obligatorii de către orice membru în cauză care nu își are sediul în Uniune; operatorul sau persoana împuternicită de operator este exonerat(ă) de această răspundere, integral sau parțial, numai dacă dovedește că membrul respectiv nu a fost răspunzător de evenimentul care a cauzat prejudiciul;
- (g) modul în care informațiile privind regulile corporatiste obligatorii, în special privind dispozițiile menționate la literele (d), (e) și (f) de la prezentul alineat, sunt furnizate persoanelor vizate în completarea informațiilor menționate la [articolele 13 și 14](#);
- (h) sarcinile oricărui responsabil cu protecția datelor desemnat în conformitate cu [articolul 37](#) sau ale oricărei alte persoane sau entități însărcinate cu monitorizarea respectării regulilor corporatiste obligatorii în cadrul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, a activităților de formare și a gestionării plângerilor;
- (i) procedurile de formulare a plângerilor;
- (j) mecanismele din cadrul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, menite să asigure verificarea conformității cu regulile corporatiste obligatorii. Aceste mecanisme includ auditurile privind protecția datelor și metodele de asigurare a acțiunilor corective menite să protejeze drepturile persoanei vizate. Rezultatele acestor verificări ar trebui să fie comunicate persoanei sau entității menționate la litera (h) și consiliului de administrație al întreprinderii care exercită controlul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună și ar trebui să fie puse la dispoziția autorității de supraveghere competente, la cerere;
- (k) mecanismele de raportare și înregistrare a modificărilor aduse regulilor și de raportare a acestor modificări autorității de supraveghere;
- (l) mecanismul de cooperare cu autoritatea de supraveghere în vederea asigurării respectării regulilor de către orice membru al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, în special prin punerea la dispoziția autorității de supraveghere a rezultatelor verificărilor cu privire la măsurile menționate la punctul (j);

(m) mecanismele de raportare către autoritatea de supraveghere competentă a oricăror cerințe legale impuse unui membru al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună într-o țară terță care pot avea un efect advers considerabil asupra garanțiilor furnizate prin regulile corporatiste obligatorii; și

(n) formarea corespunzătoare în domeniul protecției datelor a personalului care are un acces permanent sau periodic la date cu caracter personal.

(3) Comisia poate preciza formatul și procedurile pentru schimbul de informații între operatori, persoanele împuternicite de operatori și autoritățile de supraveghere pentru regulile corporatiste obligatorii în sensul prezentului articol. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 93 [alineatul \(2\)](#).

Articolul 48 Transferurile sau divulgările de informații neautorizate de dreptul Uniunii Orice hotărâre a unei instanțe sau a unui tribunal și orice decizie a unei autorități administrative a unei țări terțe care impun unui operator sau persoanei împuternicite de operator să transfere sau să divulge date cu caracter personal poate fi recunoscută sau executată în orice fel numai dacă se bazează pe un acord internațional, cum ar fi un tratat de asistență judiciară reciprocă în vigoare între țara terță solicitantă și Uniune sau un stat membru, fără a se aduce atingere altor motive de transfer în temeiul prezentului capitol.

Articolul 49 Derogări pentru situații specifice (1) În absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 45 [alineatul \(3\)](#) sau a unor garanții adecvate în conformitate cu [articolul 46](#), inclusiv a regulilor corporatiste obligatorii, un transfer sau un set de transferuri de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc numai în una dintre condițiile următoare:

(a) persoana vizată și-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a fost informată asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizată ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecție și a unor garanții adecvate;

(b) transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;

(c) transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;

(d) transferul este necesar din considerente importante de interes public;

(e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;

(f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul;

(g) transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau al dreptului intern, are scopul de a furniza informații publicului și care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în măsura în care sunt îndeplinite condițiile cu privire la consultare prevăzute de dreptul Uniunii sau de dreptul intern în acel caz specific.

În cazul în care un transfer nu ar putea să se întemeieze pe o dispoziție prevăzută la [articolul 45](#) sau [46](#), inclusiv dispoziții privind reguli corporatiste obligatorii, și nu este aplicabilă niciuna dintre derogările

pentru situații specifice prevăzute la primul paragraf din prezentul alineat, un transfer către o țară terță sau o organizație internațională poate avea loc numai în cazul în care transferul nu este repetitiv, se referă doar la un număr limitat de persoane vizate, este necesar în scopul realizării intereselor legitime majore urmărite de operator asupra căruia nu prevalează interesele sau drepturile și libertățile persoanei vizate și operatorul a evaluat toate circumstanțele aferente transferului de date și, pe baza acestei evaluări, a prezentat garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal. Operatorul informează autoritatea de supraveghere cu privire la transfer. Operatorul, în plus față de furnizarea informațiilor menționate la [articolele 13 și 14](#), informează persoana vizată cu privire la transfer și la interesele legitime majore pe care le urmărește.

(2) Transferul în temeiul alineatului (1) primul paragraf litera (g) nu implică totalitatea datelor cu caracter personal sau ansamblul categoriilor de date cu caracter personal cuprinse în registru. Atunci când registrul urmează a fi consultat de către persoane care au un interes legitim, transferul se efectuează numai la cererea persoanelor respective sau în cazul în care acestea vor fi destinatarii.

(3) Alineatul (1) primul paragraf literele (a), (b) și (c) și paragraful al doilea nu se aplică în cazul activităților desfășurate de autoritățile publice în exercitarea competențelor lor publice.

(4) Interesul public prevăzut la alineatul (1) primul paragraf litera (d) este recunoscut în dreptul Uniunii sau în dreptul statului membru sub incidența căruia intră operatorul.

(5) În absența unei decizii privind caracterul adecvat al nivelului de protecție, dreptul Uniunii sau dreptul intern poate, din considerente importante de interes public, să stabilească în mod expres limite asupra transferului unor categorii specifice de date cu caracter personal către o țară terță sau o organizație internațională. Statele membre notifică aceste dispoziții Comisiei.

(6) Operatorul sau persoana împuternicită de operator consemnează evaluarea, precum și garanțiile adecvate prevăzute la paragraful al doilea al alineatului (1) din prezentul articol, în evidențele menționate la [articolul 30](#).

Articolul 50 Cooperarea internațională în domeniul protecției datelor cu caracter personal În ceea ce privește țările terțe și organizațiile internaționale, Comisia și autoritățile de supraveghere iau măsurile corespunzătoare pentru:

(a) elaborarea de mecanisme de cooperare internațională pentru a facilita asigurarea aplicării efective a legislației privind protecția datelor cu caracter personal;

(b) acordarea de asistență internațională reciprocă în asigurarea aplicării legislației din domeniul protecției datelor cu caracter personal, inclusiv prin notificare, transferul plângerilor, asistență în investigații și schimb de informații, sub rezerva unor garanții adecvate pentru protecția datelor cu caracter personal și a altor drepturi și libertăți fundamentale;

(c) implicarea părților interesate relevante în discuțiile și activitățile care au ca scop intensificarea cooperării internaționale în domeniul aplicării legislației privind protecția datelor cu caracter personal;

(d) promovarea schimbului reciproc și a documentației cu privire la legislația și practicile în materie de protecție a datelor cu caracter personal, inclusiv în ceea ce privește conflictele jurisdicționale cu țările terțe.

CAPITOLUL VI

Autorități de supraveghere independente

Secțiunea 1

Statutul independent

Articolul 51 Autoritatea de supraveghere (1) Fiecare stat membru se asigură că una sau mai multe autorități publice independente sunt responsabile de monitorizarea aplicării prezentului regulament, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea și în vederea facilitării liberei circulații a datelor cu caracter personal în cadrul Uniunii ("autoritatea de supraveghere").

(2) Fiecare autoritate de supraveghere contribuie la aplicarea coerentă a prezentului regulament în întreaga Uniune. În acest scop, autoritățile de supraveghere cooperează atât între ele, cât și cu Comisia, în conformitate cu capitolul VII.

(3) În cazul în care mai multe autorități de supraveghere sunt instituite într-un stat membru, acesta desemnează autoritatea de supraveghere care reprezintă autoritățile respective în cadrul comitetului și instituie un mecanism prin care să asigure respectarea de către celelalte autorități a normelor privind mecanismul pentru asigurarea coerenței prevăzut la [articolul 63](#).

(4) Fiecare stat membru notifică Comisiei dispozițiile de drept pe care le adoptă în temeiul prezentului capitol până la 25 mai 2018 și, fără întârziere, orice modificare ulterioară pe care o aduce acestor dispoziții.

Articolul 52 Independență (1) Fiecare autoritate de supraveghere beneficiază de independență deplină în îndeplinirea sarcinilor sale și exercitarea competențelor sale în conformitate cu prezentul regulament.

(2) Membrul sau membrii fiecărei autorități de supraveghere, în cadrul îndeplinirii sarcinilor și al exercitării competențelor sale (lor) în conformitate cu prezentul regulament, rămâne (rămân) independent (independenți) de orice influență externă directă sau indirectă și nici nu solicită, nici nu acceptă instrucțiuni de la o parte externă.

(3) Membrul sau membrii fiecărei autorități de supraveghere se abțin de la a întreprinde acțiuni incompatibile cu atribuțiile lor, iar pe durata mandatului, nu desfășoară activități incompatibile, remunerate sau nu.

(4) Fiecare stat membru se asigură că fiecare autoritate de supraveghere beneficiază de resurse umane, tehnice și financiare, de un sediu și de infrastructura necesară pentru îndeplinirea sarcinilor și exercitarea efectivă a competențelor sale, inclusiv a celor care urmează să fie aplicate în contextul asistenței reciproce, al cooperării și al participării în cadrul comitetului.

(5) Fiecare stat membru se asigură că fiecare autoritate de supraveghere își selectează personalul propriu și deține personal propriu aflat sub conducerea exclusivă a membrului sau membrilor autorității de supraveghere respective.

(6) Fiecare stat membru se asigură că fiecare autoritate de supraveghere face obiectul unui control financiar care nu aduce atingere independenței sale și că dispune de bugete anuale distincte, publice, care pot face parte din bugetul general de stat sau național.

Articolul 53 Condiții generale aplicabile membrilor autorității de supraveghere (1) Statele membre se asigură că fiecare membru al autorității lor de supraveghere este numit prin intermediul unei proceduri transparente:

- de parlament;
- de guvern;
- de șeful statului; sau
- de un organism independent împuternicit să facă numiri în temeiul dreptului intern.

(2) Fiecare membru în cauză are calificările, experiența și competențele necesare, în special în domeniul protecției datelor cu caracter personal, pentru a-și putea îndeplini atribuțiile și exercita competențele.

(3) Atribuțiile unui membru încetează în cazul expirării mandatului, în cazul demisiei sau pensionării din oficiu în conformitate cu dreptul intern relevant.

(4) Un membru poate fi demis doar în cazuri de abateri grave sau dacă nu mai îndeplinește condițiile necesare pentru îndeplinirea atribuțiilor sale.

Articolul 54 Norme privind instituirea autorității de supraveghere (1) Fiecare stat membru prevede, pe cale legislativă, următoarele:

- (a) instituirea fiecărei autorități de supraveghere;
- (b) calificările și condițiile de eligibilitate necesare pentru a fi numit în calitate de membru al fiecărei autorități de supraveghere;
- (c) normele și procedurile pentru numirea membrului sau a membrilor fiecărei autorități de supraveghere;
- (d) durata mandatului membrului sau membrilor fiecărei autorități de supraveghere, de minimum patru ani, cu excepția primei numiri după 24 mai 2016, din care o parte poate fi pe o perioadă mai scurtă în cazul în care acest lucru este necesar pentru a proteja independența autorității de supraveghere printr-o procedură de numiri eşalonate;
- (e) dacă și de câte ori este eligibil pentru reînnoire mandatul membrului sau membrilor fiecărei autorități de supraveghere;
- (f) condițiile care reglementează obligațiile membrului sau membrilor și ale personalului fiecărei autorități de supraveghere, interdicții privind acțiunile, ocupațiile și beneficiile incompatibile cu acestea în cursul mandatului și după încetarea acestuia, precum și normele care reglementează încetarea contractului de angajare.

(2) Membrul sau membrii și personalul fiecărei autorități de supraveghere au obligația, în conformitate cu dreptul Uniunii sau cu dreptul intern, de a respecta atât pe parcursul mandatului, cât și după încetarea acestuia, secretul profesional în ceea ce privește informațiile confidențiale de care au luat cunoștință în cursul îndeplinirii sarcinilor sau al exercitării competențelor lor. Pe durata mandatului lor, această obligație de păstrare a secretului profesional se aplică în special în ceea ce privește raportarea de către persoane fizice a încălcărilor prezentului regulament.

Secțiunea 2

Abilitări, sarcini și competențe

Articolul 55 Competența (1) Fiecare autoritate de supraveghere are competența să îndeplinească sarcinile și să exercite competențele care îi sunt conferite în conformitate cu prezentul regulament pe teritoriul statului membru de care aparține.

(2) În cazul în care prelucrarea este efectuată de autorități publice sau de organisme private care acționează pe baza articolului 6 alineatul (1) litera (c) sau (e), autoritatea de supraveghere din statul membru respectiv are competență. În astfel de cazuri, articolul 56 nu se aplică.

(3) Autoritățile de supraveghere nu sunt competente să supravegheze operațiunile de prelucrare ale instanțelor care acționează în exercițiul funcției lor judiciare.

Articolul 56 Competența autorității de supraveghere principale (1) Fără a aduce atingere [articolului 55](#), autoritatea de supraveghere a sediului principal sau a sediului unic al operatorului sau al persoanei împuternicite de operator este competentă să acționeze în calitate de autoritate de supraveghere principală pentru prelucrarea transfrontalieră efectuată de respectivul operator sau respectiva persoană împuternicită în cauză în conformitate cu procedura prevăzută la [articolul 60](#).

(2) Prin derogare de la alineatul (1), fiecare autoritate de supraveghere este competentă să trateze o plângere depusă în atenția sa sau o eventuală încălcare a prezentului regulament, în cazul în care obiectul acesteia se referă numai la un sediu aflat în statul său membru sau afectează în mod semnificativ persoane vizate numai în statul său membru.

(3) În cazurile menționate la alineatul (2) din prezentul articol, autoritatea de supraveghere informează fără întârziere autoritatea de supraveghere principală cu privire la această chestiune. În termen de trei săptămâni de la momentul informării, autoritatea de supraveghere principală decide dacă tratează sau nu cazul respectiv în conformitate cu procedura prevăzută la [articolul 60](#), luând în considerare dacă există sau nu un sediu al operatorului sau al persoanei împuternicite de operator pe teritoriul statului membru a cărui autoritate de supraveghere a informat-o.

(4) În cazul în care autoritatea de supraveghere principală decide să trateze cazul, se aplică procedura prevăzută la [articolul 60](#). Autoritatea de supraveghere care a informat autoritatea de supraveghere principală poate înainta un proiect de decizie acesteia din urmă. Autoritatea de supraveghere principală ține seama în cea mai mare măsură posibilă de proiectul respectiv atunci când pregătește proiectul de decizie prevăzut la articolul 60 [alineatul \(3\)](#).

(5) În cazul în care autoritatea de supraveghere principală decide să nu trateze cazul, autoritatea de supraveghere care a informat autoritatea de supraveghere principală tratează cazul în conformitate cu [articolele 61 și 62](#).

(6) Autoritatea de supraveghere principală este singurul interlocutor al operatorului sau al persoanei împuternicite de operator în ceea ce privește prelucrarea transfrontalieră efectuată de respectivul operator sau de respectiva persoană împuternicită de operator.

Articolul 57 Sarcini (1) Fără a aduce atingere altor sarcini stabilite în temeiul prezentului regulament, fiecare autoritate de supraveghere, pe teritoriul său:

- (a) monitorizează și asigură aplicarea prezentului regulament;
- (b) promovează acțiuni de sensibilizare și de înțelegere în rândul publicului a riscurilor, normelor, garanțiilor și drepturilor în materie de prelucrare. Se acordă atenție specială activităților care se adresează în mod specific copiilor;
- (c) oferă consiliere, în conformitate cu dreptul intern, parlamentului național, guvernului și altor instituții și organisme cu privire la măsurile legislative și administrative referitoare la protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea;
- (d) promovează acțiuni de sensibilizare a operatorilor și a persoanelor împuternicite de aceștia cu privire la obligațiile care le revin în temeiul prezentului regulament;
- (e) la cerere, furnizează informații oricărei persoane vizate în legătură cu exercitarea drepturilor sale în conformitate cu prezentul regulament și, dacă este cazul, cooperează cu autoritățile de supraveghere din alte state membre în acest scop;
- (f) tratează plângerile depuse de o persoană vizată, un organism, o organizație sau o asociație în conformitate cu [articolul 80](#) și investighează într-o măsură adecvată obiectul plângerii și informează reclamantul cu privire la evoluția și rezultatul investigației, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigații mai amănunțite sau coordonarea cu o altă autoritate de supraveghere;
- (g) cooperează, inclusiv prin schimb de informații, cu alte autorități de supraveghere și își oferă asistență reciprocă pentru a asigura coerența aplicării și respectării prezentului regulament;
- (h) desfășoară investigații privind aplicarea prezentului regulament, inclusiv pe baza unor informații primite de la o altă autoritate de supraveghere sau de la o altă autoritate publică;
- (i) monitorizează evoluțiile relevante, în măsura în care acestea au impact asupra protecției datelor cu caracter personal, în special evoluția tehnologiilor informației și comunicațiilor și a practicilor comerciale;
- (j) adoptă clauze contractuale standard menționate la articolul 28 [alineatul \(8\)](#) și la articolul 46 [alineatul \(2\) litera \(d\)](#);
- (k) întocmește și menține la zi o listă în legătură cu cerința privind evaluarea impactului asupra protecției datelor, în conformitate cu articolul 35 [alineatul \(4\)](#);
- (l) oferă consiliere cu privire la operațiunile de prelucrare menționate la articolul 36 [alineatul \(2\)](#);
- (m) încurajează elaborarea de coduri de conduită în conformitate cu articolul 40 [alineatul \(1\)](#), își dă avizul cu privire la acestea și le aprobă pe cele care oferă suficiente garanții, în conformitate cu articolul 40 [alineatul \(5\)](#);
- (n) încurajează stabilirea unor mecanisme de certificare, precum și a unor sigilii și mărci în domeniul protecției datelor în conformitate cu articolul 42 [alineatul \(1\)](#) și aprobă criteriile de certificare în conformitate cu articolul 42 [alineatul \(5\)](#);
- (o) acolo unde este cazul, efectuează o revizuire periodică a certificărilor acordate, în conformitate cu articolul 42 [alineatul \(7\)](#);
- (p) elaborează și publică cerințele de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu articolul 41 și a unui organism de certificare în conformitate cu articolul 43;

- (q) coordonează procedura de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu [articolul 41](#) și a unui organism de certificare în conformitate cu [articolul 43](#);
 - (r) autorizează clauzele și dispozițiile contractuale menționate la articolul 46 [alineatul \(3\)](#);
 - (s) aprobă regulile corporatiste obligatorii în conformitate cu [articolul 47](#);
 - (t) contribuie la activitățile comitetului;
 - (u) menține la zi evidențe interne privind încălcările prezentului regulament și măsurile luate, în special avertismentele emise și sancțiunile impuse în conformitate cu articolul 58 [alineatul \(2\)](#); și
 - (v) îndeplinește orice alte sarcini legate de protecția datelor cu caracter personal.
- (2) Fiecare autoritate de supraveghere facilitează depunerea plângerilor menționate la alineatul (1) litera (f) prin măsuri precum punerea la dispoziție a unui formular de depunere a plângerii care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.
- (3) Îndeplinirea sarcinilor fiecărei autorități de supraveghere este gratuită pentru persoana vizată și, după caz, pentru responsabilul cu protecția datelor.
- (4) În cazul în care cererile sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, autoritatea de supraveghere poate percepe o taxă rezonabilă, bazată pe costurile administrative, sau poate refuza să le trateze. Sarcina de a demonstra caracterul evident nefondat sau excesiv al cererii revine autorității de supraveghere.

Articolul 58 Competențe (1) Fiecare autoritate de supraveghere are toate următoarele competențe de investigare:

- (a) de a da dispoziții operatorului și persoanei împuternicite de operator și, după caz, reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informații pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale;
- (b) de a efectua investigații sub formă de audituri privind protecția datelor;
- (c) de a efectua o revizuire a certificărilor acordate în temeiul articolului 42 [alineatul \(7\)](#);
- (d) de a notifica operatorul sau persoana împuternicită de operator cu privire la presupusa încălcare a prezentului regulament;
- (e) de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale;
- (f) de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor, în conformitate cu dreptul Uniunii sau cu dreptul procesual intern.

(2) Fiecare autoritate de supraveghere are toate următoarele competențe corective:

- (a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la posibilitatea ca operațiunile de prelucrare prevăzute să încalce dispozițiile prezentului regulament;
- (b) de a emite avertismente adresate unui operator sau unei persoane împuternicite de operator în cazul în care operațiunile de prelucrare au încălcat dispozițiile prezentului regulament;
- (c) de a da dispoziții operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-și exercita drepturile în temeiul prezentului regulament;

(d) de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile prezentului regulament, specificând, după caz, modalitatea și termenul-limită pentru aceasta;

(e) de a obliga operatorul să informeze persoana vizată cu privire la o încălcare a protecției datelor cu caracter personal;

(f) de a impune o limitare temporară sau definitivă, inclusiv o interdicție asupra prelucrării;

(g) de a dispune rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării, în temeiul [articolelor 16, 17 și 18](#), precum și notificarea acestor acțiuni destinatarilor cărora le-au fost divulgate datele cu caracter personal, în conformitate cu articolul 17 [alineatul \(2\)](#) și cu [articolul 19](#);

(h) de a retrage o certificare sau de a obliga organismul de certificare să retragă o certificare eliberată în temeiul [articolul 42 și 43](#) sau de a obliga organismul de certificare să nu elibereze o certificare în cazul în care cerințele de certificare nu sunt sau nu mai sunt îndeplinite;

(i) de a impune amenzi administrative în conformitate cu [articolul 83](#), în completarea sau în locul măsurilor menționate la prezentul alineat, în funcție de circumstanțele fiecărui caz în parte;

(j) de a dispune suspendarea fluxurilor de date către un destinatar dintr-o țară terță sau către o organizație internațională.

(3) Fiecare autoritate de supraveghere are toate următoarele competențe de autorizare și de consiliere:

(a) de a oferi consiliere operatorului în conformitate cu procedura de consultare prealabilă menționată la [articolul 36](#);

(b) de a emite avize, din proprie inițiativă sau la cerere, parlamentului național, guvernului statului membru sau, în conformitate cu dreptul intern, altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal;

(c) de a autoriza prelucrarea menționată la articolul 36 [alineatul \(5\)](#), în cazul în care dreptul statului membru prevede o astfel de autorizare prealabilă;

(d) de a emite un aviz și de a aproba proiectele de coduri de conduită, în conformitate cu articolul 40 [alineatul \(5\)](#);

(e) de a acredita organismele de certificare în conformitate cu [articolul 43](#);

(f) de a emite certificări și de a aproba criteriile de certificare în conformitate cu articolul 42 [alineatul \(5\)](#);

(g) de a adopta clauzele standard în materie de protecție a datelor menționate la articolul 28 [alineatul \(8\)](#) și la articolul 46 [alineatul \(2\) litera \(d\)](#);

(h) de a autoriza clauzele contractuale menționate la articolul 46 [alineatul \(3\) litera \(a\)](#);

(i) de a autoriza acordurile administrative menționate la articolul 46 [alineatul \(3\) litera \(b\)](#); și

(j) de a aproba reguli corporatiste obligatorii în conformitate cu [articolul 47](#).

(4) Exercițarea competențelor conferite autorității de supraveghere în temeiul prezentului articol face obiectul unor garanții adecvate, inclusiv căi de atac judiciare eficiente și procese echitabile, prevăzute în dreptul Uniunii și în dreptul intern în conformitate cu [carta](#).

(5) Fiecare stat membru prevede, pe cale legislativă, faptul că autoritatea sa de supraveghere are competența de a aduce în fața autorităților judiciare cazurile de încălcare a prezentului regulament și, după caz, de a iniția sau de a se implica într-un alt mod în proceduri judiciare, în scopul de a asigura aplicarea dispozițiilor prezentului regulament.

(6) Fiecare stat membru poate să prevadă în dreptul său faptul că autoritatea sa de supraveghere are competențe suplimentare, în afara celor menționate la alineatele (1), (2) și (3). Exercițarea acestor competențe nu afectează modul de operare eficientă a capitolului VII.

Articolul 59 Rapoarte de activitate Fiecare autoritate de supraveghere întocmește un raport anual cu privire la activitățile sale, care poate include o listă a tipurilor de încălcări notificate și a tipurilor de măsuri luate în conformitate cu articolul 58 [alineatul \(2\)](#). Rapoartele se transmit parlamentului național, guvernului și altor autorități desemnate prin dreptul intern. Acestea se pun la dispoziția publicului, a Comisiei și a comitetului.

CAPITOLUL VII

Cooperare și coerență

Secțiunea 1

Cooperare

Articolul 60 Cooperarea dintre autoritatea de supraveghere principală și celelalte autorități de supraveghere vizate (1) Autoritatea de supraveghere principală cooperează cu celelalte autorități de supraveghere vizate, în conformitate cu prezentul articol, în încercarea de a ajunge la un consens. Autoritatea de supraveghere principală și autoritățile de supraveghere vizate își comunică reciproc toate informațiile relevante.

(2) Autoritatea de supraveghere principală poate solicita în orice moment altor autorități de supraveghere vizate să ofere asistență reciprocă în temeiul [articolului 61](#) și poate desfășura operațiuni comune în temeiul [articolului 62](#), în special în vederea efectuării de investigații sau a monitorizării punerii în aplicare a unei măsuri referitoare la un operator sau o persoană împuternicită de operator, stabilit(ă) în alt stat membru.

(3) Autoritatea de supraveghere principală comunică fără întârziere informațiile relevante referitoare la această chestiune celorlalte autorități de supraveghere vizate. Autoritatea de supraveghere principală transmite fără întârziere un proiect de decizie celorlalte autorități de supraveghere vizate, pentru a obține avizul lor, și ține seama în mod corespunzător de opiniile acestora.

(4) În cazul în care oricare dintre celelalte autorități de supraveghere vizate exprimă, în termen de patru săptămâni după ce a fost consultată în conformitate cu alineatul (3) din prezentul articol, o obiecție relevantă și motivată la proiectul de decizie, autoritatea de supraveghere principală, în cazul în care nu dă curs obiecției relevante și motivate sau consideră că obiecția nu este relevantă sau motivată, sesizează mecanismul pentru asigurarea coerenței menționat la [articolul 63](#).

(5) În cazul în care intenționează să dea curs obiecției relevante și motivate formulate, autoritatea de supraveghere principală transmite celorlalte autorități de supraveghere vizate un proiect revizuit de decizie pentru a obține avizul acestora. Acest proiect revizuit de decizie face obiectul procedurii menționate la alineatul (4) pe parcursul unei perioade de două săptămâni.

(6) În cazul în care niciuna dintre celelalte autorități de supraveghere vizate nu a formulat obiecții la proiectul de decizie transmis de autoritatea de supraveghere principală în termenul menționat la alineatele (4) și (5), se consideră că autoritatea de supraveghere principală și autoritățile de supraveghere vizate sunt de acord cu proiectul de decizie respectiv, care devine obligatoriu pentru acestea.

(7) Autoritatea de supraveghere principală adoptă decizia și o notifică sediului principal sau sediului unic al operatorului sau al persoanei împuternicite de operator, după caz, și informează celelalte autorități de supraveghere vizate și comitetul cu privire la decizia în cauză, incluzând un rezumat al elementelor și motivelor relevante. Autoritatea de supraveghere la care a fost depusă plângerea informează reclamantul cu privire la decizie.

(8) Prin derogare de la alineatul (7), în cazul în care o plângere este refuzată sau respinsă, autoritatea de supraveghere la care s-a depus plângerea adoptă decizia, o notifică reclamantului și informează operatorul cu privire la acest lucru.

(9) În cazul în care autoritatea de supraveghere principală și autoritățile de supraveghere vizate sunt de acord să refuze sau să respingă anumite părți ale unei plângeri și să dea curs altor părți ale plângerii respective, se adoptă o decizie separată pentru fiecare dintre aceste părți. Autoritatea de supraveghere principală adoptă decizia pentru partea care vizează acțiunile referitoare la operator, o notifică sediului principal sau sediului unic al operatorului sau al persoanei împuternicite de operator de pe teritoriul statului membru în cauză și informează reclamantul cu privire la acest lucru, în timp ce autoritatea de supraveghere a reclamantului adoptă decizia pentru partea care vizează refuzarea sau respingerea plângerii respective, o notifică reclamantului și informează operatorul sau persoana împuternicită de operator cu privire la acest lucru.

(10) În urma notificării deciziei autorității de supraveghere principale în temeiul alineatelor (7) și (9), operatorul sau persoana împuternicită de operator ia măsurile necesare pentru a se asigura că activitățile de prelucrare sunt în conformitate cu decizia în toate sediile sale din Uniune. Operatorul sau persoana împuternicită de operator notifică măsurile luate în vederea respectării deciziei autorității de supraveghere principale, care informează celelalte autorități de supraveghere vizate.

(11) În cazul în care, în circumstanțe excepționale, o autoritate de supraveghere vizată are motive să considere că există o nevoie urgentă de a acționa în vederea protejării intereselor persoanelor vizate, se aplică procedura de urgență prevăzută la [articolul 66](#).

(12) Autoritatea de supraveghere principală și celelalte autorități de supraveghere vizate își furnizează reciproc informațiile solicitate în temeiul prezentului articol, pe cale electronică, utilizând un formular standard.

Articolul 61 Asistență reciprocă (1) Autoritățile de supraveghere își furnizează reciproc informații relevante și asistență pentru a pune în aplicare prezentul regulament în mod coerent și instituie măsuri de cooperare eficiente între ele. Asistența reciprocă se referă, în special, la cereri de informații și măsuri de supraveghere, cum ar fi cereri privind autorizări și consultări prealabile, inspecții și investigații.

(2) Fiecare autoritate de supraveghere ia toate măsurile corespunzătoare necesare pentru a răspunde unei cereri a unei alte autorități de supraveghere, fără întârzieri nejustificate și cel târziu în termen de o

lună de la data primirii cererii. Aceste măsuri pot include, în special, transmiterea informațiilor relevante privind desfășurarea unei investigații.

(3) Cererile de asistență cuprind toate informațiile necesare, inclusiv scopul cererii și motivele care stau la baza acesteia. Informațiile care fac obiectul schimbului se utilizează numai în scopul în care au fost solicitate.

(4) Autoritatea de supraveghere solicitată nu poate refuza să dea curs cererii, cu excepția cazului în care:

(a) nu are competență privind obiectul cererii sau măsurile pe care este solicitată să le execute; sau

(b) a da curs cererii ar încălca prezentul regulament sau dreptul Uniunii sau dreptului intern sub incidența căruia intră autoritatea de supraveghere care a primit cererea.

(5) Autoritatea de supraveghere căreia i s-a adresat cererea informează autoritatea de supraveghere care a transmis cererea cu privire la rezultate sau, după caz, la progresele înregistrate ori măsurile întreprinse pentru a răspunde cererii. Autoritatea de supraveghere solicitată își motivează fiecare refuz de a da curs cererii în temeiul alineatului (4).

(6) Ca regulă, autoritățile de supraveghere solicitate furnizează informațiile solicitate de alte autorități de supraveghere pe cale electronică, utilizând un formular standard.

(7) Autoritățile de supraveghere solicitate nu percep nicio taxă pentru acțiunile întreprinse de acestea în temeiul unei cereri de asistență reciprocă. Autoritățile de supraveghere pot conveni asupra unor norme privind retribuțiile reciproce în cazul unor cheltuieli specifice rezultate în urma acordării de asistență reciprocă în situații excepționale.

(8) În cazul în care o autoritate de supraveghere nu furnizează informațiile menționate la alineatul (5) din prezentul articol în termen de o lună de la primirea cererii din partea altei autorități de supraveghere, aceasta din urmă poate adopta o măsură provizorie pe teritoriul propriului stat membru, în conformitate cu articolul 55 [alineatul \(1\)](#). În acest caz, necesitatea urgentă de a acționa în temeiul articolului 66 [alineatul \(1\)](#) este considerată a fi îndeplinită și necesită o decizie obligatorie urgentă din partea comitetului, în conformitate cu articolul 66 [alineatul \(2\)](#).

(9) Comisia, printr-un act de punere în aplicare, poate specifica forma și procedurile pentru asistența reciprocă menționată în prezentul articol, precum și modalitățile de schimb de informații pe cale electronică între autoritățile de supraveghere și între autoritățile de supraveghere și comitet, în special formularul standard menționat la alineatul (6) din prezentul articol. Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 93 [alineatul \(2\)](#).

Articolul 62 Operațiuni comune ale autorităților de supraveghere (1) După caz, autoritățile de supraveghere desfășoară operațiuni comune, inclusiv investigații comune și măsuri comune de aplicare a legii, în care sunt implicați membri sau personal din autoritățile de supraveghere ale altor state membre.

(2) În cazul în care operatorul sau persoana împuternicită de operator deține sedii în mai multe state membre sau dacă un număr semnificativ de persoane vizate din mai multe state membre sunt susceptibile de a fi afectate în mod semnificativ de operațiuni de prelucrare, o autoritate de supraveghere din fiecare dintre statele membre respective are dreptul de a participa la operațiunile

comune. Autoritatea de supraveghere care este competentă în conformitate cu articolul 56 [alineatul \(1\)](#) sau [alineatul \(4\)](#) invită autoritățile de supraveghere din fiecare dintre aceste state membre să ia parte la operațiunile comune respective și răspunde fără întârziere la cererea de participare a unei autorități de supraveghere.

(3) O autoritate de supraveghere poate, în conformitate cu dreptul intern și cu acordul autorității de supraveghere din statul membru de origine, să acorde competențe, inclusiv competențe de investigare, membrilor sau personalului autorității de supraveghere din statul membru de origine implicați în operațiuni comune sau, în măsura în care dreptul statului membru al autorității de supraveghere din statul membru de primire permite acest lucru, poate autoriza membrii sau personalul autorității de supraveghere din statul membru de origine să își exercite competențele de investigare în conformitate cu dreptul statului membru al acestei din urmă autorități. Astfel de competențe de investigare pot fi exercitate doar sub coordonarea și în prezența membrilor sau personalului autorității de supraveghere din statul membru de primire. Membrii sau personalul autorității de supraveghere din statul membru de origine sunt supuși dreptului intern sub incidența căruia intră autoritatea de supraveghere din statul membru de primire.

(4) În cazul în care, în conformitate cu alineatul (1), personalul unei autorități de supraveghere din statul membru de origine își desfășoară activitatea într-un alt stat membru, statul membru de primire își asumă responsabilitatea pentru acțiunile personalului respectiv, inclusiv răspunderea pentru eventualele prejudicii cauzate de membrii personalului respectiv în cursul operațiunilor acestora, în conformitate cu dreptul statului membru pe teritoriul căruia își desfășoară operațiunile.

(5) Statul membru pe teritoriul căruia s-au produs prejudiciile repară aceste prejudicii în condițiile aplicabile prejudiciilor cauzate de propriul său personal. Statul membru de origine al autorității de supraveghere al cărei personal a cauzat prejudicii unei persoane de pe teritoriul unui alt stat membru rambursează acestui alt stat membru totalitatea sumelor pe care le-a plătit persoanelor îndreptățite în numele acestora.

(6) Fără a aduce atingere exercitării drepturilor sale față de terțe părți și cu excepția alineatului (5), fiecare stat membru se abține, în cazul prevăzut la alineatul (1), de la a pretinde de la un alt stat membru rambursarea despăgubirilor pentru prejudiciile menționate la alineatul (4).

(7) În cazul în care este planificată o operațiune comună, iar o autoritate de supraveghere nu se conformează, în termen de o lună, obligației prevăzute în a doua teză a alineatului (2) din prezentul articol, celelalte autorități de supraveghere pot adopta o măsură provizorie pe teritoriul statului membru al respectivei autorități, în conformitate cu [articolul 55](#). În acest caz, necesitatea urgentă de a acționa în temeiul articolului 66 [alineatul \(1\)](#) este considerată a fi îndeplinită și necesită un aviz de urgență sau o decizie obligatorie urgentă din partea comitetului, în conformitate cu [articolul 66 alineatul \(2\)](#).

Secțiunea 2 Asigurarea coerenței

Articolul 63 Mecanismul pentru asigurarea coerenței Pentru a contribui la aplicarea coerentă a prezentului regulament în întreaga Uniune, autoritățile de supraveghere cooperează între ele și, după caz, cu Comisia prin mecanismul pentru asigurarea coerenței, astfel cum se prevede în prezenta secțiune.

Articolul 64 Avizul comitetului (1) Comitetul emite un aviz de fiecare dată când o autoritate de supraveghere competentă intenționează să adopte oricare dintre măsurile de mai jos. În acest scop, autoritatea de supraveghere competentă comunică proiectul de decizie comitetului, atunci când:

(a) vizează adoptarea unei liste de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor, în conformitate cu articolul 35 [alineatul \(4\)](#);

(b) în conformitate cu articolul 40 [alineatul \(7\)](#), se referă la conformitatea cu prezentul regulament a unui proiect de cod de conduită sau a unei modificări sau extinderi a unui cod de conduită;

(c) vizează aprobarea cerințelor pentru acreditarea unui organism în conformitate cu articolul 41 alineatul (3), a unui organism de certificare în conformitate cu articolul 43 alineatul (3) sau a criteriilor de certificare menționate la articolul 42 alineatul (5);

(d) vizează determinarea clauzelor standard în materie de protecție a datelor menționate la articolul 46 alineatul (2) [litera \(d\)](#) sau la articolul 28 [alineatul \(8\)](#);

(e) vizează autorizarea clauzelor contractuale menționate la articolul 46 alineatul (3) [litera \(a\)](#); sau

(f) vizează aprobarea regulilor corporatiste obligatorii în sensul [articolului 47](#).

(2) Orice autoritate de supraveghere, președintele comitetului sau Comisia poate solicita ca orice chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru să fie examinată de comitet în vederea obținerii unui aviz, în special în cazul în care o autoritate de supraveghere competentă nu respectă obligațiile privind asistența reciprocă în conformitate cu [articolul 61](#) sau privind operațiunile comune în conformitate cu [articolul 62](#).

(3) În cazurile menționate la alineatele (1) și (2), comitetul emite un aviz cu privire la chestiunea care îi este prezentată, cu condiția să nu fi emis deja un aviz cu privire la aceeași chestiune. Avizul respectiv este adoptat în termen de opt săptămâni cu majoritatea simplă a membrilor comitetului. Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea chestiunii. În ceea ce privește proiectul de decizie menționat la alineatul (1) transmis membrilor comitetului în conformitate cu alineatul (5), un membru care nu a emis obiecții într-un termen rezonabil indicat de președinte se consideră a fi de acord cu proiectul de decizie.

(4) Autoritățile de supraveghere și Comisia comunică pe cale electronică comitetului, fără întârzieri nejustificate, printr-un formular standard, orice informație relevantă, inclusiv, după caz, o sinteză a faptelor, proiectul de decizie, motivele care fac necesară adoptarea unei astfel de măsuri, precum și opiniile altor autorități de supraveghere vizate.

(5) Președintele comitetului informează pe cale electronică, fără întârzieri nejustificate:

(a) membrii comitetului și Comisia cu privire la orice informație relevantă care i-a fost comunicată, utilizând un formular standard. Secretariatul comitetului furnizează traduceri ale informațiilor relevante, acolo unde este necesar; și

(b) autoritatea de supraveghere menționată, după caz, la alineatele (1) și (2), și Comisia cu privire la aviz și îl publică.

(6) Autoritatea de supraveghere competentă menționată la alineatul (1) nu își adoptă proiectul de decizie menționat la alineatul (1) în termenul menționat la alineatul (3).

(7) Autoritatea de supraveghere competentă menționată la alineatul (1) ține seama pe deplin de avizul comitetului și comunică pe cale electronică președintelui comitetului, în termen de două săptămâni de la primirea avizului, dacă își va păstra sau își va modifica proiectul de decizie și, dacă este cazul, transmite proiectul de decizie modificat, utilizând un formular standard.

(8) În cazul în care autoritatea de supraveghere competentă menționată la alineatul (1) informează președintele comitetului, în termenul menționat la alineatul (7) din prezentul articol, că intenționează să nu se conformeze avizului comitetului, integral sau parțial, oferind motivele relevante, se aplică articolul 65 alineatul (1).

Articolul 65 Soluționarea litigiilor de către comitet (1) Pentru a asigura aplicarea corectă și coerentă a prezentului regulament în cazuri individuale, comitetul adoptă o decizie obligatorie în următoarele cazuri:

(a) atunci când, în unul dintre cazurile menționate la articolul 60 alineatul (4), o autoritate de supraveghere vizată a formulat o obiecție relevantă și motivată la un proiect de decizie a autorității de supraveghere principale și autoritatea de supraveghere principală nu a dat curs obiecției sau a respins o astfel de obiecție ca nefiind relevantă sau motivată. Decizia obligatorie se referă la toate chestiunile vizate de obiecția relevantă și motivată, în special la chestiunea dacă prezentul regulament a fost încălcat;

(b) în cazul în care există opinii divergente cu privire la care dintre autoritățile de supraveghere vizate deține competența pentru sediul principal;

(c) în cazul în care o autoritate de supraveghere competentă nu solicită avizul comitetului în cazurile menționate la articolul 64 [alineatul \(1\)](#) sau nu ține seama de avizul comitetului emis în temeiul [articolului 64](#). În acest caz, orice autoritate de supraveghere vizată sau Comisia poate comunica chestiunea comitetului.

(2) Decizia menționată la alineatul (1) se adoptă în termen de o lună de la prezentarea chestiunii, cu o majoritate de două treimi a membrilor comitetului. Acest termen poate fi prelungit cu o lună, ținându-se seama de complexitatea chestiunii. Decizia menționată la alineatul (1) se motivează și se adresează autorității de supraveghere principale și tuturor autorităților de supraveghere vizate, fiind obligatorie pentru acestea.

(3) În cazul în care comitetul nu a fost în măsură să adopte o decizie în termenele menționate la alineatul (2), acesta își adoptă decizia în termen de două săptămâni de la data expirării celei de a doua luni menționate la alineatul (2), cu o majoritate simplă a membrilor săi. În cazul în care membrii comitetului au opinii divergente în proporții egale, decizia se adoptă prin votul președintelui.

(4) Autoritățile de supraveghere vizate nu adoptă o decizie asupra chestiunii prezentate comitetului în conformitate cu alineatul (1) în termenele menționate la alineatele (2) și (3).

(5) Președintele comitetului notifică, fără întârzieri nejustificate, decizia menționată la alineatul (1) autorităților de supraveghere vizate. Comitetul informează Comisia cu privire la acest lucru. Decizia se publică pe site-ul comitetului, fără întârziere, după notificarea de către autoritatea de supraveghere a deciziei finale menționate la alineatul (6).

(6) Autoritatea de supraveghere principală sau, dacă este cazul, autoritatea de supraveghere la care s-a depus plângerea își adoptă decizia finală pe baza deciziei menționate la alineatul (1) din prezentul articol, fără întârziere nejustificată și în termen de cel mult o lună de la notificarea de către comitet a deciziei sale. Autoritatea de supraveghere principală sau, dacă este cazul, autoritatea de supraveghere la care s-a depus plângerea informează comitetul cu privire la data la care decizia sa finală este notificată operatorului sau persoanei împuternicite de operator și, respectiv, persoanei vizate. Decizia finală a autorităților de supraveghere vizate se adoptă în conformitate cu condițiile prevăzute la articolul 60 [alineatele \(7\), \(8\) și \(9\)](#). Decizia finală se referă la decizia menționată la alineatul (1) din prezentul articol și precizează faptul că decizia menționată la respectivul alineat va fi publicată pe site-ul al comitetului, în conformitate cu alineatul (5). La decizia finală se anexează decizia menționată la alineatul (1) din prezentul articol.

Articolul 66 Procedura de urgență (1) În circumstanțe excepționale, atunci când o autoritate de supraveghere vizată consideră că există o necesitate urgentă de a acționa în scopul protejării drepturilor și libertăților persoanelor vizate, aceasta poate, prin derogare de la mecanismul pentru asigurarea coerenței menționat la [articolele 63, 64 și 65](#) sau de la procedura menționată la [articolul 60](#), să adopte de îndată măsuri provizorii menite să producă efecte juridice pe propriul său teritoriu, cu o perioadă de valabilitate determinată, care să nu depășească trei luni. Autoritatea de supraveghere comunică fără întârziere aceste măsuri și motivele adoptării lor celorlalte autorități de supraveghere vizate, comitetului și Comisiei.

(2) În cazul în care o autoritate de supraveghere a adoptat o măsură în temeiul alineatului (1) și consideră că este necesară adoptarea de urgență a unor măsuri definitive, aceasta poate solicita un aviz de urgență sau o decizie obligatorie urgentă din partea comitetului, indicând motivele pentru această solicitare.

(3) Orice autoritate de supraveghere poate solicita un aviz de urgență sau o decizie obligatorie urgentă, după caz, din partea comitetului în cazul în care o autoritate de supraveghere competentă nu a luat o măsură adecvată într-o situație în care există o necesitate urgentă de a acționa pentru a proteja drepturile și libertățile persoanelor vizate, indicând motivele pentru solicitarea unui astfel de aviz sau a unei astfel de decizii, inclusiv pentru necesitatea urgentă de a acționa.

(4) Prin derogare de la articolul 64 [alineatul \(3\)](#) și de la articolul 65 [alineatul \(2\)](#), un aviz de urgență sau o decizie obligatorie urgentă menționat(ă) la alineatele (2) și (3) de la prezentul articol este adoptat(ă) în termen de două săptămâni cu majoritate simplă a membrilor comitetului.

Articolul 67 Schimb de informații Comisia poate adopta acte de punere în aplicare cu un domeniu de aplicare general pentru a defini modalitățile de realizare a schimbului electronic de informații între autoritățile de supraveghere, precum și între autoritățile de supraveghere și comitet, în special formularul standard menționat la [articolul 64](#).

Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 93 [alineatul \(2\)](#).

Secțiunea 3

Comitetul european pentru protecția datelor

Articolul 68 Comitetul european pentru protecția datelor (1) Comitetul european pentru protecția datelor ("comitetul") este instituit ca organ al Uniunii și are personalitate juridică.

(2) Comitetul este reprezentat de președintele său.

(3) Comitetul este alcătuit din șeful unei autorități de supraveghere din fiecare stat membru și din Autoritatea Europeană pentru Protecția Datelor sau reprezentanții respectivi ai acestora.

(4) În cazul în care într-un stat membru mai multe autorități de supraveghere sunt responsabile de monitorizarea aplicării dispozițiilor adoptate în temeiul prezentului regulament, se numește un reprezentant comun în conformitate cu dreptul intern al statului membru respectiv.

(5) Comisia are dreptul de a participa la activitățile și reuniunile comitetului fără a avea drept de vot. Comisia numește un reprezentant. Președintele comitetului comunică Comisiei activitățile comitetului.

(6) În cazurile menționate la [articolul 65](#), Autoritatea Europeană pentru Protecția Datelor deține drept de vot numai cu privire la deciziile care privesc principiile și normele aplicabile în ceea ce privește instituțiile, organismele, oficiile și agențiile Uniunii care corespund pe fond cu cele din prezentul regulament.

Articolul 69 Independență (1) Comitetul acționează independent în îndeplinirea sarcinilor sale sau în exercitarea competențelor sale în conformitate cu [articolele 70 și 71](#).

(2) Fără a aduce atingere solicitărilor din partea Comisiei menționate la articolul 70 alineatele (1) și (2), comitetul, în îndeplinirea sarcinilor sale sau în exercitarea competențelor sale, nu solicită și nu acceptă instrucțiuni de la nicio parte externă.

Articolul 70 Sarcinile comitetului (1) Comitetul asigură aplicarea coerentă a prezentului regulament. În acest scop, din proprie inițiativă sau, după caz, la solicitarea Comisiei, comitetul are, în special, următoarele sarcini:

(a) să monitorizeze și să asigure aplicarea corectă a prezentului regulament, în cazurile prevăzute la [articolele 64 și 65](#), fără a aduce atingere sarcinilor autorităților naționale de supraveghere;

(b) să ofere consiliere Comisiei cu privire la orice aspect legat de protecția datelor cu caracter personal în cadrul Uniunii, inclusiv cu privire la orice propunere de modificare a prezentului regulament;

(c) să ofere consiliere Comisiei cu privire la formatul și procedurile pentru schimbul de informații între operatori, persoanele împuternicite de operatori și autoritățile de supraveghere pentru regulile corporatiste obligatorii;

(d) să emită orientări, recomandări și bune practici privind procedurile de ștergere a linkurilor către datele cu caracter personal, a copiilor sau a reproducerilor acestora de care dispun serviciile de comunicații accesibile publicului, astfel cum se menționează la articolul 17 [alineatul \(2\)](#);

(e) să examineze, din proprie inițiativă, la cererea unuia dintre membrii săi sau la cererea Comisiei, orice chestiune referitoare la aplicarea prezentului regulament și să emită orientări, recomandări și bune practici pentru a încuraja aplicarea coerentă a prezentului regulament;

(f) să emită orientări, recomandări și bune practici în conformitate cu prezentul alineat litera (e) în vederea detalierii criteriilor și condițiilor pentru deciziile bazate pe crearea de profiluri menționate la articolul 22 [alineatul \(2\)](#);

(g) să emită orientări, recomandări și bune practici în conformitate cu litera (e) din prezentul alineat pentru stabilirea încălcării securității datelor cu caracter personal și stabilirii întârzierilor nejustificate menționate la articolul 33 [alineatele \(1\) și \(2\)](#), precum și pentru circumstanțele speciale în care un operator sau o persoană împuternicită de către operator are obligația de a notifica încălcarea securității datelor cu caracter personal;

(h) să emită orientări, recomandări și bune practici în conformitate cu litera (e) din prezentul alineat în ceea ce privește circumstanțele în care o încălcare a securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, menționate la articolul 34 [alineatul \(1\)](#);

(i) să emită orientări, recomandări și bune practici în conformitate cu litera (e) din prezentul alineat în scopul detalierii criteriilor și cerințelor aplicabile transferurilor de date cu caracter personal bazate pe regulile corporatiste obligatorii care trebuie respectate de operatori și cele care trebuie respectate de persoanele împuternicite de operatori, precum și cu privire la cerințe suplimentare necesare pentru a asigura protecția datelor cu caracter personal ale persoanelor vizate menționate la [articolul 47](#);

(j) să emită orientări, recomandări și bune practici în conformitate cu litera (e) din prezentul alineat în vederea detalierii criteriilor și cerințelor pentru transferurile de date cu caracter personal menționate la articolul 49 [alineatul \(1\)](#);

(k) să elaboreze orientări destinate autorităților de supraveghere, referitoare la aplicarea măsurilor menționate la articolul 58 [alineatele \(1\), \(2\) și \(3\)](#) și să stabilească amenzile administrative în conformitate cu articolul 83;

(l) să revizuiască aplicarea practică a orientărilor, recomandărilor și bunelor practici;

(m) să emită orientări, recomandări și bune practici în conformitate cu litera (e) din prezentul alineat în vederea stabilirii procedurilor comune de raportare de către persoanele fizice a încălcărilor prezentului regulament în conformitate cu articolul 54 [alineatul \(2\)](#);

(n) să încurajeze elaborarea de coduri de conduită și stabilirea unor mecanisme de certificare, precum și a unor sigilii și mărci în domeniul protecției datelor, în conformitate cu [articolele 40 și 42](#);

(o) să aprobe criteriile de certificare în temeiul articolului 42 alineatul (5) și să țină un registru public al mecanismelor de certificare și al sigiliilor și mărcilor în materie de protecție a datelor, în temeiul articolului 42 alineatul (8), și al operatorilor certificați sau al persoanelor împuternicite de operatori certificate, stabiliți (stabilite) în țări terțe, în temeiul articolului 42 alineatul (7);

(p) să aprobe cerințele menționate la articolul 43 alineatul (3), în vederea acreditării organismelor de certificare menționate la articolul 43;

(q) să prezinte Comisiei un aviz privind cerințele de certificare menționate la articolul 43 [alineatul \(8\)](#);

(r) să prezinte Comisiei un aviz privind pictogramele menționate la articolul 12 [alineatul \(7\)](#);

(s) să prezinte Comisiei un aviz pentru evaluarea caracterului adecvat al nivelului de protecție într-o țară terță sau o organizație internațională, inclusiv pentru a determina dacă o țară terță, un teritoriu, sau unul sau mai multe sectoare specificate din acea țară terță, sau o organizație internațională nu mai

asigură un nivel de protecție adecvat. În acest scop, Comisia pune la dispoziția comitetului toată documentația necesară, inclusiv corespondența purtată cu autoritățile publice ale țării terțe, în ceea ce privește acea țară terță, acel teritoriu sau acel sector, sau cu organizația internațională;

(t) să emită avize privind proiectele de decizii ale autorităților de supraveghere în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 64 [alineatul \(1\)](#) privind chestiunile prezentate în conformitate cu articolul 64 [alineatul \(2\)](#) și să emită decizii obligatorii în temeiul [articolului 65](#), inclusiv în cazurile menționate la [articolul 66](#);

(u) să promoveze cooperarea și schimbul eficient bilateral și multilateral de informații și bune practici între autoritățile de supraveghere;

(v) să promoveze programe comune de formare și să faciliteze schimburile de personal între autoritățile de supraveghere, precum și, după caz, cu autoritățile de supraveghere ale țărilor terțe sau organizațiilor internaționale;

(w) să promoveze schimbul de cunoștințe și de documente privind legislația și practicile în materie de protecție a datelor cu autoritățile de supraveghere a protecției datelor la nivel mondial;

(x) să emită avize privind codurile de conduită elaborate la nivelul Uniunii în temeiul articolului 40 [alineatul \(9\)](#); și

(y) să țină un registru electronic accesibil publicului cu deciziile luate de autoritățile de supraveghere și de instanțe cu privire la chestiuni tratate în cadrul mecanismului pentru asigurarea coerenței.

(2) În cazul în care Comisia consultă comitetul, aceasta poate indica un termen limită, ținând seama de caracterul urgent al chestiunii.

(3) Comitetul își transmite avizele, orientările, recomandările și bunele practici Comisiei și comitetului menționat la [articolul 93](#) și le face publice.

(4) Dacă este cazul, comitetul consultă părțile interesate și le oferă posibilitatea de a face observații într-un termen rezonabil. Fără a aduce atingere dispozițiilor [articolului 76](#), comitetul publică rezultatele procedurii de consultare.

Articolul 71 Rapoarte (1) Comitetul întocmește un raport anual privind protecția persoanelor fizice cu privire la prelucrare în Uniune și, dacă este relevant, în țări terțe și organizații internaționale. Raportul este pus la dispoziția publicului și transmis Parlamentului European, Consiliului și Comisiei.

(2) Raportul anual include o revizuire a aplicării practice a orientărilor, recomandărilor și bunelor practici menționate la articolul 70 alineatul (1) [litera \(l\)](#), precum și a deciziilor obligatorii menționate la [articolul 65](#).

Articolul 72 Procedura (1) Comitetul adoptă decizii prin majoritate simplă a membrilor săi, cu excepția cazului când se prevede altfel în prezentul regulament.

(2) Comitetul își adoptă propriul regulament de procedură cu o majoritate de două treimi a membrilor săi și își organizează propriile mecanisme de funcționare.

Articolul 73 Președintele (1) Comitetul alege un președinte și doi vicepreședinți din rândul membrilor săi, cu majoritate simplă.

(2) Mandatul președintelui și al vicepreședinților este de cinci ani și poate fi reînnoit o singură dată.

Articolul 74 Sarcinile președintelui (1) Președintele are următoarele sarcini:

(a) să convoace reuniunile comitetului și să stabilească ordinea de zi;

(b) să notifice deciziile adoptate de comitet, în conformitate cu [articolul 65](#), autorității de supraveghere principale și autorităților de supraveghere vizate;

(c) să asigure îndeplinirea la timp a sarcinilor comitetului, în special în ceea ce privește mecanismul pentru asigurarea coerenței menționat la [articolul 63](#).

(2) Comitetul stabilește în regulamentul său de procedură repartizarea sarcinilor între președinte și vicepreședinți.

Articolul 75 Secretariatul (1) Comitetul dispune de un secretariat, care este asigurat de Autoritatea Europeană pentru Protecția Datelor.

(2) Secretariatul își îndeplinește sarcinile exclusiv pe baza instrucțiunilor președintelui comitetului.

(3) Personalul Autorității Europene pentru Protecția Datelor implicat în îndeplinirea sarcinilor conferite comitetului în temeiul prezentului regulament face obiectul unor linii de raportare separate în raport cu personalul implicat în îndeplinirea sarcinilor conferite Autorității Europene pentru Protecția Datelor.

(4) Dacă este oportun, comitetul și Autoritatea Europeană pentru Protecția Datelor elaborează și publică un memorandum de înțelegere pentru punerea în aplicare a prezentului articol, care să stabilească condițiile cooperării și să se aplice personalului Autorității Europene pentru Protecția Datelor implicat în îndeplinirea sarcinilor conferite comitetului în temeiul prezentului regulament.

(5) Secretariatul oferă sprijin analitic, administrativ și logistic comitetului.

(6) Secretariatul este responsabil în special de următoarele:

(a) gestionarea curentă a activității comitetului;

(b) comunicarea dintre membrii comitetului, președintele acestuia și Comisie;

(c) comunicarea cu alte instituții și cu publicul;

(d) utilizarea mijloacelor electronice pentru comunicarea internă și externă;

(e) traducerea informațiilor relevante;

(f) pregătirea și monitorizarea acțiunilor ulterioare reuniunilor comitetului;

(g) pregătirea, redactarea și publicarea avizelor, deciziilor privind soluționarea litigiilor dintre autoritățile de supraveghere și a altor texte adoptate de comitet.

Articolul 76 Confidențialitate (1) Discuțiile din cadrul comitetului sunt confidențiale în cazul în care comitetul consideră că acest lucru este necesar în conformitate cu regulamentul său de procedură.

(2) Accesul la documentele prezentate membrilor comitetului, experților și reprezentanților părților terțe este reglementat prin Regulamentul (CE) [nr. 1049/2001](#) al Parlamentului European și al Consiliului.

CAPITOLUL VIII

Căi de atac, răspundere și sancțiuni

Articolul 77 Dreptul de a depune o plângere la o autoritate de supraveghere (1) Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prezentul regulament.

(2) Autoritatea de supraveghere la care s-a depus plângerea informează reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul [articolului 78](#).

Articolul 78 Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere (1)

Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană fizică sau juridică are dreptul de a exercita o cale de atac judiciară eficientă împotriva unei decizii obligatorii din punct de vedere juridic a unei autorități de supraveghere care o vizează.

(2) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care autoritatea de supraveghere care este competentă în temeiul articolelor 55 și 56 nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse în temeiul [articolului 77](#).

(3) Acțiunile introduse împotriva unei autorități de supraveghere sunt aduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere.

(4) În cazul în care acțiunile sunt introduse împotriva unei decizii a unei autorități de supraveghere care a fost precedată de un aviz sau o decizie a comitetului în cadrul mecanismului pentru asigurarea coerenței, autoritatea de supraveghere transmite curții avizul respectiv sau decizia respectivă.

Articolul 79 Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau unei persoane împuternicite de operator (1)

Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere în temeiul [articolului 77](#), fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal fără a se respecta prezentul regulament.

(2) Acțiunile introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în fața instanțelor din statul membru unde operatorul sau persoana împuternicită de operator își are un sediu. Alternativ, o astfel de acțiune poate fi prezentată în fața instanțelor din statul membru în care persoana vizată își are reședința obișnuită, cu excepția cazului în care operatorul sau persoana împuternicită de operator este o autoritate publică a unui stat membru ce acționează în exercitarea competențelor sale publice.

Articolul 80 Reprezentarea persoanelor vizate (1) Persoana vizată are dreptul de a mandata un organism, o organizație sau o asociație fără scop lucrativ, care au fost constituite în mod corespunzător în conformitate cu dreptul intern, ale căror obiective statutare sunt de interes public, care sunt active în domeniul protecției drepturilor și libertăților persoanelor vizate în ceea ce privește protecția datelor lor cu caracter personal, să depună plângerea în numele său, să exercite în numele său drepturile menționate la [articolele 77, 78 și 79](#), precum și să exercite dreptul de a primi despăgubiri menționat la [articolul 82](#) în numele persoanei vizate, dacă acest lucru este prevăzut în dreptul intern.

(2) Statele membre pot prevedea că orice organism, organizație sau asociație menționată la alineatul (1) din prezentul articol, independent de mandatul unei persoanei vizate, are dreptul de a depune în statul membru respectiv o plângere la autoritatea de supraveghere care este competentă în temeiul [articolului 77](#) și de a exercita drepturile menționate la [articolele 78 și 79](#), în cazul în care consideră că

drepturile unei persoane vizate în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării.

Articolul 81 Suspendarea procedurilor (1) În cazul în care o instanță competentă a unui stat membru are informații că pe rolul unei instanțe dintr-un alt stat membru se află o acțiune având același obiect în ceea ce privește activitățile de prelucrare ale aceluiași operator sau ale aceleași persoane împuternicite de operator, instanța respectivă contactează instanța din celălalt stat membru pentru a confirma existența unor astfel de acțiuni.

(2) Atunci când pe rolul unei instanțe dintr-un alt stat membru se află o acțiune având același obiect în ceea ce privește activitățile de prelucrare ale aceluiași operator sau ale aceleași persoane împuternicite de operator, orice altă instanță competentă decât instanța sesizată inițial poate suspenda acțiunea aflată la ea pe rol.

(3) În cazul în care o astfel de acțiune se judecă în primă instanță, orice instanță sesizată ulterior poate, de asemenea, la cererea uneia dintre părți, să-și decline competența, cu condiția ca respectiva acțiune să fie de competența primei instanțe sesizate și ca dreptul aplicabil acesteia să permită conexarea acțiunilor.

Articolul 82 Dreptul la despăgubiri și răspunderea (1) Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a prezentului regulament are dreptul să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.

(2) Orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă prezentul regulament. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligațiile din prezentul regulament care revin în mod specific persoanelor împuternicite de operator sau a acționat în afara sau în contradicție cu instrucțiunile legale ale operatorului.

(3) Operatorul sau persoana împuternicită de operator este exonerat(ă) de răspundere în temeiul alineatului (2) dacă dovedește că nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul.

(4) În cazul în care mai mulți operatori sau mai multe persoane împuternicite de operator, sau un operator și o persoană împuternicită de operator sunt implicați (implicate) în aceeași operațiune de prelucrare și răspund, în temeiul alineatelor (2) și (3), pentru orice prejudiciu cauzat de prelucrare, fiecare operator sau persoană împuternicită de operator este răspunzător (răspunzătoare) pentru întregul prejudiciu pentru a asigura despăgubirea efectivă a persoanei vizate.

(5) În cazul în care un operator sau o persoană împuternicită de operator a plătit, în conformitate cu alineatul (4), în totalitate despăgubirile pentru prejudiciul ocazionat, respectivul operator sau respectiva persoană împuternicită de operator are dreptul să solicite de la ceilalți operatori sau celelalte persoane împuternicite de operator implicate în aceeași operațiune de prelucrare recuperarea acelei părți din despăgubiri care corespunde părții lor de răspundere pentru prejudiciu, în conformitate cu condițiile stabilite la alineatul (2).

(6) Acțiunile în exercitarea dreptului de recuperare a despăgubirilor plătite se introduc la instanțele competente în temeiul dreptului statului membru menționat la articolul 79 [alineatul \(2\)](#).

Articolul 83 Condiții generale pentru impunerea amenzilor administrative (1) Fiecare autoritate de supraveghere asigură faptul că impunerea unor amenzi administrative în conformitate cu prezentul articol pentru încălcările prezentului regulament menționate la alineatele (4), (5) și (6) este, în fiecare caz, eficace, proporțională și disuasivă.

(2) În funcție de circumstanțele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menționate la articolul 58 alineatul (2) [literele \(a\) - \(h\)](#) și [\(j\)](#). Atunci când se ia decizia dacă să se impună o amendă administrativă și decizia cu privire la valoarea amenzii administrative în fiecare caz în parte, se acordă atenția cuvenită următoarelor aspecte:

(a) natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea;

(b) dacă încălcarea a fost comisă intenționat sau din neglijență;

(c) orice acțiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;

(d) gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ținându-se seama de măsurile tehnice și organizatorice implementate de aceștia în temeiul [articolelor 25 și 32](#);

(e) eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;

(f) gradul de cooperare cu autoritatea de supraveghere pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării;

(g) categoriile de date cu caracter personal afectate de încălcare;

(h) modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;

(i) în cazul în care măsurile menționate la articolul 58 [alineatul \(2\)](#) au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la același obiect, respectarea respectivelor măsuri;

(j) aderarea la coduri de conduită aprobate, în conformitate cu [articolul 40](#), sau la mecanisme de certificare aprobate, în conformitate cu [articolul 42](#); și

(k) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

(3) În cazul în care un operator sau o persoană împuternicită de operator încalcă în mod intenționat sau din neglijență, pentru aceeași operațiune de prelucrare sau pentru operațiuni de prelucrare conexe, mai multe dispoziții din prezentul regulament, quantumul total al amenzii administrative nu poate depăși suma prevăzută pentru cea mai gravă încălcare.

(4) Pentru încălcările dispozițiilor următoare, în conformitate cu alineatul (2), se aplică amenzi administrative de până la 10 000 000 EUR sau, în cazul unei întreprinderi, de până la 2% din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare:

(a) obligațiile operatorului și ale persoanei împuternicite de operator în conformitate cu [articolele 8, 11, 25-39, 42 și 43](#);

- (b) obligațiile organismului de certificare în conformitate cu [articolele 42 și 43](#);
- (c) obligațiile organismului de monitorizare în conformitate cu articolul 41 [alineatul \(4\)](#).
- (5) Pentru încălcările dispozițiilor următoare, în conformitate cu alineatul (2), se aplică amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4% din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare:
- (a) principiile de bază pentru prelucrare, inclusiv condițiile privind consimțământul, în conformitate cu [articolele 5, 6, 7 și 9](#);
- (b) drepturile persoanelor vizate în conformitate cu [articolele 12-22](#);
- (c) transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu [articolele 44-49](#);
- (d) orice obligații în temeiul legislației naționale adoptate în temeiul capitolului IX;
- (e) nerespectarea unui ordin sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării fluxurilor de date, emisă de către autoritatea de supraveghere în temeiul articolului 58 [alineatul \(2\)](#), sau neacordarea accesului, încălcând articolul 58 [alineatul \(1\)](#).
- (6) Pentru încălcarea unui ordin emis de autoritatea de supraveghere în conformitate cu articolul 58 [alineatul \(2\)](#) se aplică, în conformitate cu alineatul (2) din prezentul articol, amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4% din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare.
- (7) Fără a aduce atingere competențelor corective ale autorităților de supraveghere menționate la articolul 58 [alineatul \(2\)](#), fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi impuse amenzi administrative autorităților publice și organismelor publice stabilite în statul membru respectiv.
- (8) Exercițarea de către autoritatea de supraveghere a competențelor sale în temeiul prezentului articol are loc cu condiția existenței unor garanții procedurale adecvate în conformitate cu dreptul Uniunii și cu dreptul intern, inclusiv căi de atac judiciare eficiente și dreptul la un proces echitabil.
- (9) În cazul în care sistemul juridic al statului membru nu prevede amenzi administrative, prezentul articol poate fi aplicat astfel încât amenda să fie inițiată de autoritatea de supraveghere competentă și impusă de instanțele naționale competente, garantându-se, în același timp, faptul că aceste căi de atac sunt eficiente și au un efect echivalent cu cel al amenzilor administrative impuse de autoritățile de supraveghere. În orice caz, amenzile impuse trebuie să fie eficiente, proporționale și disuasive. Respectivele state membre informează Comisia cu privire la dispozițiile de drept intern pe care le adoptă în temeiul prezentului alineat până la 25 mai 2018, precum și, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară a acestora.

Articolul 84 Sancțiuni (1) Statele membre stabilesc normele privind alte sancțiunile aplicabile în caz de încălcare a prezentului regulament, în special pentru încălcări care nu fac obiectul unor amenzi administrative în temeiul [articolului 83](#), și iau toate măsurile necesare pentru a garanta faptul că acestea sunt puse în aplicare. Sancțiunile respective sunt eficiente, proporționale și disuasive.

(2) Fiecare stat membru informează Comisia cu privire la dispozițiile de drept intern pe care le adoptă în temeiul alineatului (1) până la 25 mai 2018, precum și, fără întârziere, cu privire la orice modificare ulterioară a acestora.

CAPITOLUL IX

Dispoziții referitoare la situații specifice de prelucrare

Articolul 85 Prelucrarea și libertatea de exprimare și de informare (1) Prin intermediul dreptului intern, statele membre asigură un echilibru între dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament și dreptul la libertatea de exprimare și de informare, inclusiv prelucrarea în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare.

(2) Pentru prelucrarea efectuată în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare, statele membre prevăd exonerări sau derogări de la dispozițiile capitolului II (principii), ale capitolului III (drepturile persoanei vizate), ale capitolului IV (operatorul și persoana împuternicită de operator), ale capitolului V (transferul datelor cu caracter personal către țări terțe sau organizații internaționale), ale capitolului VI (autorități de supraveghere independente), ale capitolului VII (cooperare și coerență) și ale capitolului IX (situații specifice de prelucrare a datelor) în cazul în care acestea sunt necesare pentru a asigura un echilibru între dreptul la protecția datelor cu caracter personal și libertatea de exprimare și de informare.

(3) Fiecare stat membru informează Comisia cu privire la dispozițiile de drept intern pe care le-a adoptat în temeiul alineatului (2) precum și, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară a acestora.

Articolul 86 Prelucrarea și accesul public la documente oficiale Datele cu caracter personal din documentele oficiale deținute de o autoritate publică sau de un organism public sau privat pentru îndeplinirea unei sarcini care servește interesului public pot fi divulgate de autoritatea sau organismul respectiv în conformitate cu dreptul Uniunii sau cu dreptul intern sub incidența căruia intră autoritatea sau organismul, pentru a stabili un echilibru între accesul public la documente oficiale și dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament.

Articolul 87 Prelucrarea unui număr de identificare național Statele membre pot detalia în continuare condițiile specifice de prelucrare a unui număr de identificare național sau a oricărui alt identificator cu aplicabilitate generală. În acest caz, numărul de identificare național sau orice alt identificator cu aplicabilitate generală este folosit numai în temeiul unor garanții corespunzătoare pentru drepturile și libertățile persoanei vizate în temeiul prezentului regulament.

Articolul 88 Prelucrarea în contextul ocupării unui loc de muncă (1) Prin lege sau prin acorduri colective, statele membre pot prevedea norme mai detaliate pentru a asigura protecția drepturilor și a libertăților cu privire la prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii, al egalității și diversității la locul de muncă, al asigurării sănătății și securității la locul de muncă, al protejării proprietății angajatorului sau a clientului, precum și în scopul exercitării și

beneficiarilor, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și pentru încetarea raporturilor de muncă.

(2) Aceste norme includ măsuri corespunzătoare și specifice pentru garantarea demnității umane, a intereselor legitime și a drepturilor fundamentale ale persoanelor vizate, în special în ceea ce privește transparența prelucrării, transferul de date cu caracter personal în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună și sistemele de monitorizare la locul de muncă.

(3) Fiecare stat membru informează Comisia cu privire la dispozițiile de drept intern pe care le adoptă în temeiul alineatului (1) până la 25 mai 2018, precum și, fără întârziere, cu privire la orice modificare ulterioară a acestora.

Articolul 89 Garanții și derogări privind prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice (1) Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice are loc cu condiția existenței unor garanții corespunzătoare, în conformitate cu prezentul regulament, pentru drepturile și libertățile persoanelor vizate. Respectivul asigură faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor. Respectivul măsuri pot include pseudonimizarea, cu condiția ca respectivul scopuri să fie îndeplinite în acest mod. Atunci când respectivul scopuri pot fi îndeplinite printr-o prelucrare ulterioară care nu permite sau nu mai permite identificarea persoanelor vizate, scopurile respective sunt îndeplinite în acest mod.

(2) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică ori în scopuri statistice, dreptul Uniunii sau dreptul intern poate să prevadă derogări de la drepturile menționate la [articolele 15, 16, 18 și 21](#), sub rezerva condițiilor și a garanțiilor prevăzute la alineatul (1) din prezentul articol, în măsura în care drepturile respective sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri.

(3) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare în interes public, dreptul Uniunii sau dreptul intern poate să prevadă derogări de la drepturile menționate la [articolele 15, 16, 18, 19, 20 și 21](#), sub rezerva condițiilor și a garanțiilor prevăzute la alineatul (1) din prezentul articol, în măsura în care drepturile respective sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri.

(4) În cazul în care prelucrarea menționată la alineatele (2) și (3) servește în același timp și altui scop, derogările se aplică numai prelucrării în scopurile menționate la alineatele respective.

Articolul 90 Obligații privind păstrarea confidențialității (1) Statele membre pot adopta norme specifice pentru a stabili competențele autorităților de supraveghere, prevăzute la articolul 58 alineatul (1) [literele \(e\)](#) și [\(f\)](#), în legătură cu operatori sau cu persoane împuternicite de operatori care, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organismele naționale competente, au obligația de a păstra secretul profesional sau alte obligații echivalente de confidențialitate, în cazul în care acest lucru este necesar și proporțional pentru a stabili un echilibru

între dreptul la protecția datelor cu caracter personal și obligația păstrării confidențialității. Respectivele norme se aplică doar în ceea ce privește datele cu caracter personal pe care operatorul sau persoana împuternicită de operator le-a primit în urma sau în contextul unei activități care intră sub incidența acestei obligații de păstrare a confidențialității.

(2) Fiecare stat membru notifică Comisiei normele adoptate în temeiul alineatului (1) până la 25 mai 2018, precum și, fără întârziere, orice modificare ulterioară a acestora.

Articolul 91 Normele existente în domeniul protecției datelor pentru biserici și asociații religioase (1)
În cazul în care, într-un stat membru, bisericile și asociațiile sau comunitățile religioase aplică, la data intrării în vigoare a prezentului regulament, un set cuprinzător de norme de protecție a persoanelor fizice cu privire la prelucrare, aceste norme pot continua să se aplice, cu condiția să fie aliniate la prezentul regulament.

(2) Bisericile și asociațiile religioase care aplică un set cuprinzător de norme în conformitate cu alineatul (1) din prezentul articol sunt supuse supravegherii unei autorități de supraveghere independente care poate fi specifică, cu condiția să îndeplinească condițiile stabilite în capitolul VI din prezentul regulament.

CAPITOLUL X

Acte delegate și acte de punere în aplicare

Articolul 92 Exercițarea delegării (1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute de prezentul articol.

(2) Delegarea de competențe prevăzută la articolul 12 [alineatul \(8\)](#) și la articolul 43 [alineatul \(8\)](#) se conferă Comisiei pe o perioadă nedeterminată de la 24 mai 2016.

(3) Delegarea de competențe menționată la articolul 12 [alineatul \(8\)](#) și la articolul 43 [alineatul \(8\)](#) poate fi revocată în orice moment de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificată în decizia respectivă. Decizia produce efecte din ziua următoare datei publicării acesteia în Jurnalul Oficial al Uniunii Europene sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere validității actelor delegate care sunt deja în vigoare.

(4) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(5) Un act delegat adoptat în conformitate cu articolul 12 [alineatul \(8\)](#) și cu articolul 43 [alineatul \(8\)](#) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecțiuni în termen de trei luni de la notificarea acestuia Parlamentului European și Consiliului, sau în cazul în care, înainte de expirarea termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecțiuni. Respectivul termen se prelungește cu trei luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 93 Procedura comitetului (1) Comisia este asistată de un comitet. Comitetul respectiv este un comitet în înțelesul Regulamentului (UE) [nr. 182/2011](#).

(2) În cazul în care se face trimitere la prezentul alineat, se aplică [articolul 5](#) din Regulamentul (UE) nr. 182/2011.

(3) În cazul în care se face trimitere la prezentul alineat, se aplică [articolul 8](#) din Regulamentul (UE) nr. 182/2011 coroborat cu [articolul 5](#) din respectivul regulament.

CAPITOLUL XI

Dispoziții finale

Articolul 94 Abrogarea Directivei 95/46/CE (1) Decizia 95/46/CE se abrogă cu efect de la 25 mai 2018.

(2) Trimiterile la directiva abrogată se interpretează ca trimiteri la prezentul regulament. Trimiterile la Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal instituit prin articolul 29 din Directiva 95/46/CE se interpretează ca trimiteri la Comitetul european pentru protecția datelor instituit prin prezentul regulament.

Articolul 95 Relația cu Directiva 2002/58/CE Prezentul regulament nu impune obligații suplimentare pentru persoanele fizice sau juridice în ceea ce privește prelucrarea în legătură cu furnizarea de servicii de comunicații electronice destinate publicului în rețelele de comunicații publice din Uniune, cu privire la aspectele pentru care acestora le revin obligații specifice cu același obiectiv prevăzut în Directiva 2002/58/CE.

Articolul 96 Relația cu acordurile încheiate anterior Acordurile internaționale care implică transferul de date cu caracter personal către țări terțe sau organizații internaționale, care au fost încheiate de statele membre înainte de 24 mai 2016 și care sunt în conformitate cu dreptul Uniunii aplicabil înainte de data respectivă, rămân în vigoare până când vor fi modificate, înlocuite sau revocate.

Articolul 97 Rapoartele Comisiei (1) Până la 25 mai 2020 și, ulterior, la fiecare patru ani, Comisia transmite Parlamentului European și Consiliului un raport privind evaluarea și revizuirea prezentului regulament. Rapoartele sunt făcute publice.

(2) În contextul evaluărilor și revizuirilor menționate la alineatul (1), Comisia examinează în special aplicarea și funcționarea:

(a) capitolului V privind transferul datelor cu caracter personal către țări terțe sau organizații internaționale, având în vedere în special deciziile adoptate în temeiul articolului 45 [alineatul \(3\)](#) din prezentul regulament și deciziile adoptate în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE;

(b) capitolul VII privind cooperarea și coerența.

(3) În scopul alineatului (1), Comisia poate solicita informații de la statele membre și de la autoritățile de supraveghere.

(4) La efectuarea evaluărilor și a revizuirilor menționate la alineatele (1) și (2), Comisia ia în considerare pozițiile și constatările Parlamentului European, ale Consiliului, precum și ale altor organisme sau surse relevante.

(5) Comisia transmite, dacă este necesar, propuneri corespunzătoare de modificare a prezentului regulament, în special ținând seama de evoluțiile din domeniul tehnologiei informației și având în vedere progresele societății informaționale.

Articolul 98 Revizuirea altor acte juridice ale Uniunii în materie de protecție a datelor Dacă este cazul, Comisia prezintă propuneri legislative în vederea modificării altor acte juridice ale Uniunii privind protecția datelor cu caracter personal, în vederea asigurării unei protecții uniforme și consecvente a

persoanelor fizice în ceea ce privește prelucrarea. Acest lucru privește în special normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea de către instituțiile, organismele, oficiile și agențiile Uniunii, precum și normele referitoare la libera circulație a acestor date.

Articolul 99 Intrare în vigoare și aplicare (1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene.

(2) Prezentul regulament se aplică de la 25 mai 2018.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 27 aprilie 2016.

Pentru Parlamentul European

Președintele

M. SCHULZ

Pentru Consiliu

Președintele

J.A. HENNIS-PLASSCHAERT