

# 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 privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)

## **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 [\(19\)](#);

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) literele (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) literele (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. Retragerea 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. Retragerea 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 prelucrez 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 prelucreze 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 prelucrează 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 retrage 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 ștergă, 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 (2a) 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 opoziție și procesul decizional individual automatizat

## **Articolul 21**

### Dreptul la opoziție

(1) În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situația particulară în care se află, prelucrării în temeiul articolului 6 alineatul (1) litera (e) sau (f) sau al articolului 6 alineatul (1) 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 literele (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 libertăților 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. Respectivăle 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. Respectivă 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 încălcă 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 operator și, după caz, persoana împuternicită 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 ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;

(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 lor.

#### 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 susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată din partea autorității de supraveghere în cazul în care.

(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 acesteia 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 înaintea 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 întâzierii. 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, menționată la articolul 9, sau a unor date cu caracter personal privind 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 criterii 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 condițiile 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

împuțernicite 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 împuțernicite de operatori care fac obiectul prezentului regulament, ci și pentru a demonstra existența unor garanții adecvate oferite de operatorii sau de persoanele împuțernicite 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 împuțernicite 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 împuțernicite 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 împuțernicită 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 împuțernicite de operator pentru o perioadă maximă de trei ani și poate fi reînnoită în aceleași condiții, cu condiția ca cerințele 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 cerințele pentru certificare.

(8) Comitetul regroupează 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 [\(20\)](#) 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) 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) 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 criteriilor 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 conformitate cu alineatul (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. Comitetul regrupează toate mecanismele de certificare și sigiliile de protecție a datelor într-un registru și le pune la dispoziția publicului prin orice mijloc corespunzător.

(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 reparații 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 acesteia 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 revizuirii 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 eșalonate;
- (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 literei (c) sau (e) de la articolul 6 alineatul (1), este autoritatea de supraveghere din statul membru respectiv. În astfel de cazuri, nu se aplică articolul 56.

(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 criteriile 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 mustrări 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 articolului 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 cartă.

(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 retribuiile 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 criteriilor pentru acreditarea unui organism în conformitate cu articolul 41 alineatul (3) sau a unui organism de certificare în conformitate cu articolul 43 alineatul (3);

(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 nu își adoptă proiectul de decizie menționat la alineatul (1) în termenul menționat la alineatul (3).

(7) Autoritatea de supraveghere 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 vizată 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 principale sau autoritatea principală 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 autorităților 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 alineatul (1) litera (b) și la articolul 70 alineatul (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 menționate la literele (e) și (f);
- (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 efectueze acreditarea organismelor de certificare și revizuirea periodică a acreditării în conformitate cu articolul 43 și să țină un registru public al organismelor acreditate, în conformitate cu articolul 43 alineatul (6), și al operatorilor acreditați sau al persoanelor împuternicite de operator acreditate, stabiliți (stabilite) în țări terțe, în conformitate cu articolul 42 alineatul (7);
- (p) să precizeze cerințele menționate la articolul 43 alineatul (3), în vederea acreditării organismelor de certificare prevăzute la articolul 42;
- (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 [\(21\)](#).

#### **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 aceleiași 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 aceleiași 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, amenziile 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, cuantumul 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. Respectiv 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**

### Sanțiuni

(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 beneficierii, 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 garanții 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 aliniată 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**

Exercitarea 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