REGULAMENTUL NR. 679/2016
PRIVIND PROTECŢIA PERSOANELOR FIZICE ÎN CEEA CE PRIVEŞTE PRELUCRAREA DATELOR CU CARACTER PERSONAL ŞI PRIVIND LIBERA CIRCULAŢIE A ACESTOR DATE ŞI DE ABROGARE A DIRECTIVEI 95/46/CE (REGULAMENTUL GENERAL PRIVIND PROTECŢIA DATELOR) (TEXT CU RELEVANŢĂ PENTRU SEE)

GDPR

CAPITOLUL I
Dispoziţii generale

Articolul 1
Obiect şi obiective

(1) Prezentul regulament stabileşte normele referitoare la protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal, precum şi normele referitoare la libera circulaţie a datelor cu caracter personal.

(2) Prezentul regulament asigură protecţia drepturilor şi libertăţilor fundamentale ale persoanelor fizice şi în special a dreptului acestora la protecţia datelor cu caracter personal.

(3) Libera circulaţie a datelor cu caracter personal în interiorul Uniunii nu poate fi restricţionată sau interzisă din motive legate de protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal.

Articolul 2
Domeniul de aplicare material

(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parţial prin mijloace automatizate, precum şi prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă a datelor sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor.

(2) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:

(a) în cadrul unei activităţi care nu intră sub incidenţa dreptului Uniunii;

(b) de către statele membre atunci când desfăşoară activităţi care intră sub incidenţa capitolului 2 al titlului V din Tratatul UE;

(c) de către o persoană fizică în cadrul unei activităţi exclusiv personale sau domestice;

(d) de către autorităţile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracţiunilor, sau al executării sancţiunilor penale, inclusiv al protejării împotriva ameninţărilor la adresa siguranţei publice şi al prevenirii acestora.

(3) Pentru prelucrarea datelor cu caracter personal de către instituţiile, organele, oficiile şi agenţiile Uniunii, se aplică Regulamentul (CE) nr. 45/2001. Regulamentul (CE) nr. 45/2001 şi alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal se adaptează la principiile şi 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 menţionată.

Articolul 3
Domeniul de aplicare teritorial

(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal în cadrul activităţilor 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

activităţile 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 plăţi 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 internaţional public.

Articolul 4
Definiţii
În sensul prezentului regulament:
1. **"date cu caracter personal"** înseamnă orice informaţii 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 identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;
2. **"prelucrare"** înseamnă orice operaţiune sau set de operaţiuni 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 dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;
3. **"restricţionarea 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 performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele 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 informaţii suplimentare, cu condiţia ca aceste informaţii suplimentare să fie stocate separat şi să facă obiectul unor măsuri de natură tehnică şi organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;
6. **"sistem de evidenţă a datelor"** înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice;
7. **"operator"** înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi 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, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
9. **"destinatar"** înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile 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 autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării;
10. **"parte terţă"** înseamnă o persoană fizică sau juridică, autoritate publică, agenţie sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;
11. **"consimţământ"** al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită

de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

12. **"încălcarea securităţii datelor cu caracter personal"** înseamnă o încălcare a securităţii 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 moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective şi 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 asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;

16. **"sediu principal"** înseamnă:

(a) în cazul unui operator cu sedii în cel puţin două state membre, locul în care se află administraţia centrală a acestuia în Uniune, cu excepţia cazului în care deciziile privind scopurile şi mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are competenţa 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 puţin două state membre, locul în care se află administraţia centrală a acesteia în Uniune, sau, în cazul în care persoana împuternicită de operator nu are o administraţie centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activităţile principale de prelucrare, în contextul activităţilor unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligaţii 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 priveşte obligaţiile lor respective care le revin în temeiul prezentului regulament;

18. **"întreprindere"** înseamnă o persoană fizică sau juridică ce desfăşoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociaţii care desfăşoară în mod regulat o activitate economică;

19. **"grup de întreprinderi"** înseamnă o întreprindere care exercită controlul şi întreprinderile controlate de aceasta;

20. **"reguli corporatiste obligatorii"** înseamnă politicile în materie de protecţie 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 priveşte transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe ţări terţe 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 autorităţii de supraveghere respective;

(b) persoanele vizate care îşi au reşedinţa 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 activităţilor 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 puţin două state membre; sau

GDPR

(b) fie prelucrarea datelor cu caracter personal care are loc în contextul activităţilor 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 puţin două state membre;

24. **"obiecţie relevantă şi motivată"** înseamnă o obiecţie la un proiect de decizie în scopul de a stabili dacă există o încălcare a prezentului regulament sau dacă măsurile preconizate în ceea ce priveşte operatorul sau persoana împuternicită de operator respectă prezentul regulament, care demonstrează în mod clar importanţa riscurilor pe care le prezintă proiectul de decizie în ceea ce priveşte drepturile şi libertăţile fundamentale ale persoanelor vizate şi, după caz, libera circulaţie a datelor cu caracter personal în cadrul Uniunii;

25. **"serviciile societăţii informaţionale"** înseamnă un serviciu astfel cum este definit la articolul 1 alineatul (1) litera (b) din Directiva 98/34/CE a Parlamentului European şi a Consiliului;

26. **"organizaţie internaţională"** înseamnă o organizaţie şi organismele sale subordonate reglementate de dreptul internaţional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe ţări 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 şi transparent faţă de persoana vizată ("legalitate, echitate şi transparenţă");

(b) colectate în scopuri determinate, explicite şi legitime şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile iniţiale, în conformitate cu articolul 89 alineatul (1) ("limitări legate de scop");

(c) adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate ("reducerea la minimum a datelor");

(d) exacte şi, 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 şterse sau rectificate fără întârziere ("exactitate");

(e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte 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 ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic şi organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor şi
libertăţilor persoanei vizate ("limitări legate de stocare");

(f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("integritate şi confidenţialitate").

(2) Operatorul este responsabil de respectarea alineatului (1) şi poate demonstra această respectare ("responsabilitate").

Articolul 6
Legalitatea prelucrării

(1) Prelucrarea este legală numai dacă şi în măsura în care se aplică cel puţin una dintre următoarele condiţii:

(a) persoana vizată şi-a dat consimţământul 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 obligaţii 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 serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul;
(f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terţă, cu excepţia cazului în care prevalează interesele sau drepturile şi libertăţile 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 autorităţi publice în îndeplinirea atribuţiilor lor.
(2) Statele membre pot menţine sau introduce dispoziţii mai specifice de adaptare a aplicării normelor prezentului regulament în ceea ce priveşte prelucrarea în vederea respectării alineatului (1) literele (c) şi (e) prin definirea unor cerinţe specifice mai precise cu privire la prelucrare şi a altor măsuri de asigurare a unei prelucrări legale şi echitabile, inclusiv pentru alte situaţii concrete de prelucrare, astfel cum este prevăzut în capitolul IX.
(3) Temeiul pentru prelucrarea menţionată la alineatul (1) literele (c) şi (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 priveşte prelucrarea menţionată la alineatul (1) litera (e), este necesar pentru îndeplinirea unei sarcini efectuate în interes public sau în cadrul exercitării unei funcţii publice atribuite operatorului. Respectivul temei juridic poate conţine dispoziţii specifice privind adaptarea aplicării normelor prezentului regulament, printre altele: condiţiile generale care reglementează legalitatea prelucrării de către operator; tipurile de date care fac obiectul prelucrării; persoanele vizate; entităţile cărora le pot fi divulgate datele şi scopul pentru care respectivele date cu caracter personal pot fi divulgate; limitările legate de scop; perioadele de stocare; şi operaţiunile şi procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale şi echitabile cum sunt cele pentru alte situaţii concrete de prelucrare astfel cum sunt prevăzute în capitolul IX. Dreptul Uniunii sau dreptul intern urmăreşte un obiectiv de interes public şi este proporţional 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 consimţământul persoanei vizate sau pe dreptul Uniunii sau dreptul intern, care constituie o măsură necesară şi proporţională într-o societate democratică pentru a proteja obiectivele menţionate 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 iniţial, ia în considerare, printre altele:
(a) orice legătură dintre scopurile în care datele cu caracter personal au fost colectate şi scopurile prelucrării ulterioare preconizate;
(b) contextul în care datele cu caracter personal au fost colectate, în special în ceea ce priveşte relaţia dintre persoanele vizate şi 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 şi infracţiuni, în conformitate cu articolul 10;
(d) posibilele consecinţe asupra persoanelor vizate ale prelucrării ulterioare preconizate;
(e) existenţa unor garanţii adecvate, care pot include criptarea sau pseudonimizarea.

Articolul 7
Condiţii privind consimţământul
(1) În cazul în care prelucrarea se bazează pe consimţământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal.
(2) În cazul în care consimţământul persoanei vizate este dat în contextul unei declaraţii scrise care se referă şi la alte aspecte, cererea privind consimţământul trebuie să fie prezentată într-o formă care o diferenţiază în mod clar de celelalte aspecte, într-o formă inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu. Nicio parte a

GDPR

respectivei declaraţii care constituie o încălcare a prezentului regulament nu este obligatorie.
(3) Persoana vizată are dreptul să îşi retragă în orice moment consimţământul. Retragerea consimţământului nu afectează legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia. Înainte de acordarea consimţământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimţământului se face la fel de simplu ca acordarea acestuia.
(4) Atunci când se evaluează dacă consimţământul este dat în mod liber, se ţine seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiţionată sau nu de consimţământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

Articolul 8
Condiţii aplicabile în ceea ce priveşte consimţământul copiilor în legătură cu serviciile societăţii informaţionale
(1) În cazul în care se aplică articolul 6 alineatul (1) litera (a), în ceea ce priveşte oferirea de servicii ale societăţii informaţionale în mod direct unui
copil, prelucrarea datelor cu caracter personal ale unui copil este legală dacă copilul are cel puţin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă şi în măsura în care consimţământul respectiv este acordat sau autorizat de titularul răspunderii părinteşti asupra copilului.
Statele membre pot prevedea prin lege o vârstă inferioară în aceste scopuri, cu condiţia 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 părinteşti a acordat sau a autorizat consimţământul, ţinând 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 apartenenţa la sindicate şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viaţa sexuală sau orientarea sexuală ale unei persoane fizice.
(2) Alineatul (1) nu se aplică în următoarele situaţii:
(a) persoana vizată şi-a dat consimţământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepţia cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicţia prevăzută la alineatul (1) să nu poată fi ridicată prin consimţământul persoanei vizate;
(b) prelucrarea este necesară în scopul îndeplinirii obligaţiilor şi al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forţei de muncă şi al securităţii sociale şi protecţiei 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 garanţii adecvate pentru drepturile fundamentale şi 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-şi da consimţământul;
(d) prelucrarea este efectuată în cadrul activităţilor lor legitime şi cu garanţii adecvate de către o fundaţie, o asociaţie sau orice alt organism fără scop lucrativ şi cu specific politic, filozofic, religios sau sindical, cu condiţia ca prelucrarea să se refere numai la membrii sau la foştii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale şi ca datele cu caracter personal să nu fie comunicate terţilor fără consimţământul 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 instanţă sau ori de câte ori

instanţele acţionează în exerciţiul funcţiei lor judiciare;

(g) prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate;

(h) prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacităţii de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistenţă medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor şi serviciilor de sănătate sau de asistenţă socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical şi sub rezerva respectării condiţiilor şi garanţiilor prevăzute la alineatul (3);

(i) prelucrarea este necesară din motive de interes public în domeniul sănătăţii publice, cum ar fi protecţia împotriva ameninţărilor transfrontaliere grave la adresa sănătăţii sau asigurarea de standarde ridicate de calitate şi siguranţă a asistenţei medicale şi a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate şi specifice pentru protejarea drepturilor şi libertăţilor persoanei vizate, în special a secretului profesional; sau

(j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate.

(3) Datele cu caracter personal menţionate la alineatul (1) pot fi prelucrate în scopurile menţionate la alineatul (2) litera (h) în cazul în care datele respective sunt prelucrate de către un profesionist supus obligaţiei de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naţionale competente sau de o altă persoană supusă, de asemenea, unei obligaţii de confidenţialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naţionale competente.

(4) Statele membre pot menţine sau introduce condiţii suplimentare, inclusiv restricţii, în ceea ce priveşte prelucrarea de date genetice, date biometrice sau date privind sănătatea.

Articolul 10

Prelucrarea de date cu caracter personal referitoare la condamnări penale şi infracţiuni

Prelucrarea de date cu caracter personal referitoare la condamnări penale şi infracţiuni sau la măsuri de securitate conexe în temeiul articolului 6 alineatul

(1) se efectuează numai sub controlul unei autorităţi de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern care

prevede garanţii adecvate pentru drepturile şi libertăţile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ţine numai sub controlul unei autorităţi 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 obligaţia de a păstra, obţine sau prelucra informaţii suplimentare pentru a identifica persoana vizată în scopul unic al respectării prezentului regulament.

(2) Dacă, în cazurile menţionate 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 excepţia cazului în care persoana vizată, în scopul exercitării drepturilor sale în temeiul respectivelor articole, oferă informaţii suplimentare care permit identificarea sa.

GDPR

CAPITOLUL III
Drepturile persoanei vizate

Secţiunea 1
Transparenţă şi modalităţi

Articolul 12
Transparenţa informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor persoanei vizate

(1) Operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informaţii menţionate la articolele 13 şi 14 şi orice comunicări în temeiul
articolelor 15-22 şi 34 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, în special pentru orice informaţii adresate în mod specific unui copil. Informaţiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informaţiile pot fi furnizate verbal, cu condiţia ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

(2) Operatorul facilitează exercitarea drepturilor persoanei vizate în temeiul articolelor 15-22. În cazurile menţionate la articolul 11 alineatul (2), operatorul nu refuză să dea curs cererii persoanei vizate de a-şi exercita drepturile în conformitate cu articolele 15-22, cu excepţia cazului în care operatorul demonstrează că nu este în măsură să identifice persoana vizată.

(3) Operatorul furnizează persoanei vizate informaţii privind acţiunile întreprinse în urma unei cereri în temeiul articolelor 15-22, fără întârzieri nejustificate şi în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ţinându-se seama de complexitatea şi numărul cererilor. Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând şi motivele întârzierii. În cazul în care persoana vizată
introduce o cerere în format electronic, informaţiile sunt furnizate în format electronic acolo unde este posibil, cu excepţia 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 şi în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri şi la posibilitatea de a depune o plângere în faţa unei autorităţi de supraveghere şi de a introduce o cale de atac judiciară.

(5) Informaţiile furnizate în temeiul articolelor 13 şi 14 şi orice comunicare şi orice măsuri luate în temeiul articolelor 15-22 şi 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 ţinând cont de costurile administrative pentru furnizarea informaţiilor 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 menţionată la articolele 15-21, operatorul poate solicita furnizarea de informaţii suplimentare necesare pentru a confirma identitatea persoanei vizate.

(7) Informaţiile care urmează să fie furnizate persoanelor vizate în temeiul articolelor 13 şi 14 pot fi furnizate în combinaţie cu pictograme standardizate pentru a oferi într-un mod uşor vizibil, inteligibil şi 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 informaţiilor care urmează să fie prezentate de pictograme şi a procedurilor pentru furnizarea de pictograme standardizate.

GDPR

Secţiunea 2
Informare şi acces la date cu caracter personal

Articolul 13
Informaţii 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 obţinerii acestor date cu caracter personal, furnizează persoanei vizate toate informaţiile următoare:
(a) identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;
(b) datele de contact ale responsabilului cu protecţia datelor, după caz;
(c) scopurile în care sunt prelucrate datele cu caracter personal, precum şi 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 terţă;
(e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
(f) dacă este cazul, intenţia operatorului de a transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională şi existenţa sau absenţa unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menţionate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf, o trimitere la garanţiile adecvate sau corespunzătoare şi la mijloacele de a obţine o copie a acestora, în cazul în care acestea au fost puse la dispoziţie.
(2) În plus faţă de informaţiile menţionate la alineatul (1), în momentul în care datele cu caracter personal sunt obţinute, operatorul furnizează persoanei vizate următoarele informaţii suplimentare necesare pentru a asigura o prelucrare echitabilă şi 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) existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării sau a dreptului de a se opune prelucrării, precum şi 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), existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;
(d) dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;
(e) dacă furnizarea de date cu caracter personal reprezintă o obligaţie legală sau contractuală sau o obligaţie necesară pentru încheierea unui contract, precum şi dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii;
(f) existenţa unui proces decizional automatizat incluzând crearea de profiluri, menţionat la articolul 22 alineatele (1) şi (4), precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.
(3) În cazul în care operatorul intenţionează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informaţii privind scopul secundar respectiv şi orice informaţii suplimentare relevante, în conformitate cu alineatul (2).
(4) Alineatele (1), (2) şi (3) nu se aplică dacă şi în măsura în care persoana vizată deţine deja informaţiile respective.

Articolul 14
Informaţii care se furnizează în cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată
(1) În cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informaţii:

GDPR

(a) identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;
(b) datele de contact ale responsabilului cu protecţia datelor, după caz;
(c) scopurile în care sunt prelucrate datele cu caracter personal, precum şi 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, intenţia operatorului de a transfera date cu caracter personal către un destinatar dintr-o ţară terţă sau o organizaţie internaţională şi existenţa sau absenţa unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menţionate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf, o trimitere la garanţiile adecvate sau corespunzătoare şi la mijloacele de a obţine o copie a acestora, în cazul în care acestea au fost puse la dispoziţie.
(2) Pe lângă informaţiile menţionate la alineatul (1), operatorul furnizează persoanei vizate următoarele informaţii necesare pentru a asigura o prelucrare echitabilă şi transparentă în ceea ce priveşte 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 terţă;
(c) existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării şi a dreptului de a se opune prelucrării, precum şi 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), existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;
(e) dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;
(f) sursa din care provin datele cu caracter personal şi, dacă este cazul, dacă acestea provin din surse disponibile public;
(g) existenţa unui proces decizional automatizat incluzând crearea de profiluri, menţionat la articolul 22 alineatele (1) şi (4), precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.
(3) Operatorul furnizează informaţiile menţionate la alineatele (1) şi (2):
(a) într-un termen rezonabil după obţinerea datelor cu caracter personal, dar nu mai mare de o lună, ţinându-se seama de circumstanţele 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 intenţionează 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 intenţionează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obţinute, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informaţii privind scopul secundar respectiv şi orice informaţii suplimentare relevante, în conformitate cu alineatul (2).
(5) Alineatele (1)-(4) nu se aplică dacă şi în măsura în care:
(a) persoana vizată deţine deja informaţiile;
(b) furnizarea acestor informaţii se dovedeşte a fi imposibilă sau ar implica eforturi disproporţionate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, sub rezerva condiţiilor şi a garanţiilor prevăzute la articolul 89 alineatul (1), sau în măsura în care obligaţia menţionată la alineatul (1) din prezentul articol este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective In astfel de cazuri, operatorul ia măsuri adecvate pentru a proteja drepturile, libertăţile şi interesele legitime ale persoanei vizate, inclusiv punerea informaţiilor la dispoziţia publicului;
(c) obţinerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern sub

GDPR

incidenţa căruia intră operatorul şi 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 confidenţiale în temeiul unei obligaţii statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligaţii legale de a păstra secretul.

Articolul 15
Dreptul de acces al persoanei vizate
(1) Persoana vizată are dreptul de a obţine din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc
şi, în caz afirmativ, acces la datele respective şi la următoarele informaţii:
(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 ţări terţe sau organizaţii internaţionale;
(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) existenţa dreptului de a solicita operatorului rectificarea sau ştergerea datelor cu caracter personal ori restricţionarea 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 faţa unei autorităţi de supraveghere;
(g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informaţii disponibile privind sursa acestora;
(h) existenţa unui proces decizional automatizat incluzând crearea de profiluri, menţionat la articolul 22 alineatele
(1) şi (4), precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.
(2) În cazul în care datele cu caracter personal sunt transferate către o ţară terţă sau o organizaţie internaţională, persoana vizată are dreptul să fie informată cu privire la garanţiile 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 şi cu excepţia cazului în care persoana vizată solicită un alt format, informaţiile sunt furnizate într-un format electronic utilizat în mod curent.
(4) Dreptul de a obţine o copie menţionată la alineatul (3) nu aduce atingere drepturilor şi libertăţilor altora.

Secţiunea 3
Rectificare şi ştergere

Articolul 16
Dreptul la rectificare
Persoana vizată are dreptul de a obţine de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ţinându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obţine completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declaraţii suplimentare.

Articolul 17
Dreptul la ştergerea datelor ("dreptul de a fi uitat")
(1) Persoana vizată are dreptul de a obţine din partea operatorului ştergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar

GDPR

operatorul are obligaţia de a şterge 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 îşi retrage consimţământul pe baza căruia are loc prelucrarea, în conformitate cu articolul 6 alineatul (1) litera (a) sau cu articolul 9 alineatul (2) litera (a), şi nu există niciun alt temei juridic pentru prelucrarea;
(c) persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (1) şi nu există motive legitime care să prevaleze în ceea ce priveşte 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 şterse pentru respectarea unei obligaţii legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidenţa căruia se află operatorul;
(f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societăţii informaţionale menţionate la articolul 8 alineatul (1).
(2) În cazul în care operatorul a făcut publice datele cu caracter personal şi este obligat, în temeiul alineatului (1), să le şteargă, operatorul, ţinând seama de tehnologia disponibilă şi de costul implementării, ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ştergerea de către aceşti operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.
(3) Alineatele (1) şi (2a) nu se aplică în măsura în care prelucrarea este necesară:
(a) pentru exercitarea dreptului la liberă exprimare şi la informare;
(b) pentru respectarea unei obligaţii 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 autorităţi oficiale cu care este învestit operatorul;
(c) din motive de interes public în domeniul sănătăţii publice, în conformitate cu articolul 9 alineatul (2) literele (h) şi (i) şi cu articolul 9 alineatul (3);
(d) în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în măsura în care dreptul menţionat 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 instanţă.

Articolul 18
Dreptul la restricţionarea prelucrării
(1) Persoana vizată are dreptul de a obţine din partea operatorului restricţionarea 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 ştergerii datelor cu caracter personal, solicitând în schimb restricţionarea 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 instanţă; 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 restricţionată în temeiul alineatului (1), astfel de date cu caracter personal pot, cu excepţia stocării, să fie prelucrate numai cu consimţământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanţă sau pentru protecţia drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

GDPR

(3) O persoană vizată care a obţinut restricţionarea prelucrării în temeiul alineatului (1) este informată de către operator înainte de ridicarea restricţiei de prelucrare.

Articolul 19
Obligaţia de notificare privind rectificarea sau ştergerea datelor cu caracter personal sau restricţionarea prelucrării

Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ştergere a datelor cu caracter personal sau restricţionare a prelucrării efectuate în conformitate cu articolul 16, articolul 17 alineatul (1) şi articolul 18, cu excepţia cazului în care acest lucru se dovedeşte imposibil sau presupune eforturi disproporţionate. 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 şi pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent şi care poate fi citit automat şi 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 consimţământ 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); şi
(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) Exercitarea dreptului menţionat 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 autorităţi oficiale cu care este învestit operatorul.
(4) Dreptul menţionat la alineatul (1) nu aduce atingere drepturilor şi libertăţilor altora.

Secţiunea 4
Dreptul la o poziţie şi procesul decizional individual automatizat

Articolul 21
Dreptul la opoziţie

(1) În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situaţia 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 dispoziţii. Operatorul nu mai prelucrează datele cu caracter personal, cu excepţia cazului în care operatorul demonstrează că are motive legitime şi imperioase care justifică prelucrarea şi care prevalează asupra
intereselor, drepturilor şi libertăţilor persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanţă.
(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

GDPR

nu mai sunt prelucrate în acest scop.
(4) Cel târziu în momentul primei comunicări cu persoana vizată, dreptul menţionat la alineatele (1) şi (2) este adus în mod explicit în atenţia persoanei vizate şi este prezentat în mod clar şi separat de orice alte informaţii.
(5) În contextual utilizării serviciilor societăţii informaţionale şi în pofida Directivei 2002/58/CE, persoana vizată îşi poate exercita dreptul de a se opune prin mijloace automate care utilizează specificaţii tehnice.
(6) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare ştiinţifică sau istorică sau în scopuri statistice în conformitate cu articolul 89 alineatul (1), persoana vizată, din motive legate de situaţia sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepţia 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 şi un operator de date;
(b) este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului şi care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate; sau
(c) are la bază consimţământul explicit al persoanei vizate.
(3) În cazurile menţionate la alineatul (2) literele (a) şi (c), operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate, cel puţin dreptul acesteia de a obţine intervenţie umană din partea operatorului, de a-şi exprima punctul de vedere şi de a contesta decizia.
(4) Deciziile menţionate la alineatul (2) nu au la bază categoriile speciale de date cu caracter personal menţionate la articolul 9 alineatul (1), cu excepţia cazului în care se aplică articolul 9 alineatul (2) litera (a) sau (g) şi în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate.

Secţiunea 5
Restricţii

Articolul 23
Restricţii
(1) Dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricţiona printr-o măsură
legislativă domeniul de aplicare al obligaţiilor şi al drepturilor prevăzute la articolele 12-22 şi 34, precum şi la articolul 5 în măsura în care dispoziţiile acestuia corespund drepturilor şi obligaţiilor prevăzute la articolele 12-22, atunci când o astfel de restricţie respectă esenţa drepturilor şi libertăţilor fundamentale şi constituie o măsură necesară şi proporţională într-o societate democratică, pentru a asigura:
(a) securitatea naţională;
(b) apărarea;
(c) securitatea publică;
(d) prevenirea, investigarea, depistarea sau urmărirea penală a infracţiunilor sau executarea sancţiunilor penale, inclusiv protejarea împotriva ameninţărilor la adresa securităţii publice şi 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 şi fiscal şi în domeniul sănătăţii publice şi al securităţii sociale;
(f) protejarea independenţei judiciare şi a procedurilor judiciare;

GDPR

(g) prevenirea, investigarea, depistarea şi urmărirea penală a încălcării eticii în cazul profesiilor reglementate;
(h) funcţia de monitorizare, inspectare sau reglementare legată, chiar şi ocazional, de exercitarea autorităţii oficiale în cazurile menţionate la literele (a)-(e) şi (g);
(i) protecţia persoanei vizate sau a drepturilor şi libertăţilor altora;
(j) punerea în aplicare a pretenţiilor de drept civil.
(2) În special, orice măsură legislativă menţionată la alineatul (1) conţine dispoziţii specifice cel puţin, dacă este cazul, în ceea ce priveşte:
(a) scopurile prelucrării sau ale categoriilor de prelucrare;
(b) categoriile de date cu caracter personal;
(c) domeniul de aplicare al restricţiilor introduse;
(d) garanţiile pentru a preveni abuzurile sau accesul sau transferul ilegal;
(e) menţionarea operatorului sau a categoriilor de operatori;
(f) perioadele de stocare şi garanţiile aplicabile având în vedere natura, domeniul de aplicare şi scopurile prelucrării sau ale categoriilor de prelucrare;
(g) riscurile pentru drepturile şi libertăţilor persoanelor vizate; şi
(h) dreptul persoanelor vizate de a fi informate cu privire la restricţie, cu excepţia cazului în care acest lucru poate aduce atingere scopului restricţiei.

GDPR

CAPITOLUL IV
Operatorul şi persoana împuternicită de operator

Secţiunea 1
Obligaţii generale

Articolul 24
Responsabilitatea operatorului

(1) Ţinând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să
demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar.

(2) Atunci când sunt proporţionale în raport cu operaţiunile de prelucrare, măsurile menţionate la alineatul (1) includ punerea în aplicare de către operator a unor politici adecvate de protecţie a datelor.

(3) Aderarea la coduri de conduită aprobate, menţionate la articolul 40, sau la un mecan ism de certificare aprobat, menţionat la articolul 42, poate fi utilizată ca element care să demonstreze respectarea obligaţiilor de către operator.

Articolul 25
Asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit

(1) Având în vedere stadiul actual al tehnologiei, costurile implementării, şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât şi în cel al prelucrării în sine, pune în aplicare măsuri tehnice şi organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecţie a datelor, precum reducerea la minimum a datelor, şi să integreze garanţiile necesare în cadrul prelucrării, pentru a îndeplini cerinţele prezentului regulament şi a proteja drepturile persoanelor vizate.

(2) Operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligaţie se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare şi accesibilităţii lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenţia 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 cerinţelor prevăzute la alineatele (1) şi (2) ale prezentului articol.

Articolul 26
Operatori asociaţi

(4) În cazul în care doi sau mai mulţi operatori stabilesc în comun scopurile şi mijloacele de prelucrare, aceştia sunt operatori asociaţi. Ei stabilesc într-un mod transparent responsabilităţile fiecăruia în ceea ce priveşte îndeplinirea obligaţiilor care le revin în temeiul prezentului regulament, în special în ceea ce priveşte exercitarea drepturilor persoanelor vizate şi îndatoririle fiecăruia de
furnizare a informaţiilor prevăzute la articolele 13 şi 14, prin intermediul unui acord între ei, cu excepţia cazului şi în măsura în care responsabilităţile 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.

(5) Acordul menţionat la alineatul (1) reflectă în mod adecvat rolurile şi raporturile respective ale operatorilor asociaţi faţă de persoanele vizate. Esenţa acestui acord este făcută cunoscută persoanei vizate.

(6) Indiferent de clauzele acordului menţionat la alineatul (1), persoana vizată îşi poate exercita drepturile în temeiul prezentului regulament cu privire la şi în raport cu fiecare dintre operatori.

GDPR

Articolul 27

Reprezentanţii operatorilor sau ai persoanelor împuternicite de operatori care nu îşi 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) Obligaţia 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 şi infracţiuni menţionată la articolul 10, şi care este puţin susceptibilă de a genera un risc pentru drepturile şi libertăţile persoanelor, ţinând cont de natura, contextul, domeniul de aplicare şi scopurile prelucrării; sau

(b) unei autorităţi sau unui organism public.

(3) Reprezentantul îşi 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 şi servicii sau al căror comportament este monitorizat.

(4) Reprezentantul primeşte din partea operatorului sau a persoanei împuternicite de operator un mandat prin care autorităţile de supraveghere şi persoanele vizate, în special, se pot adresa reprezentantului, în plus faţă 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 acţiunilor în justiţie care ar putea fi introduse împotriva operatorului sau persoanei împuternicite de operator înseşi.

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 garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să respecte cerinţele prevăzute în prezentul regulament şi să asigure protecţia drepturilor persoanei vizate.

(2) Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizaţie scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizaţii 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 obiecţii faţă 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 şi care stabileşte obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate şi obligaţiile şi drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoană împuternicită de operator:

(a) prelucrează datele cu caracter personal numai pe baza unor instrucţiuni documentate din partea operatorului, inclusiv în ceea ce priveşte transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, cu excepţia cazului în care această obligaţie îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligaţie juridică operatorului înainte de prelucrare, cu excepţia 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 confidenţialitatea sau au o obligaţie statutară adecvată de confidenţialitate;

(c) adoptă toate măsurile necesare în conformitate cu articolul 32;

(d) respectă condiţiile menţionate la alineatele (2) şi (4) privind recrutarea unei alte persoane împuternicite de operator;

(e) ţinând seama de natura prelucrării, oferă asistenţă operatorului prin măsuri tehnice şi organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligaţiei operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute în capitolul III;
(f) ajută operatorul să asigure respectarea obligaţiilor prevăzute la articolele 32-36, ţinând seama de caracterul prelucrării şi informaţiile aflate la dispoziţia persoanei împuternicite de operator;
(g) la alegerea operatorului, şterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare şi elimină copiile existente, cu excepţia cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;
(h) pune la dispoziţia operatorului toate informaţiile necesare pentru a demonstra respectarea obligaţiilor prevăzute la prezentul articol, permite desfăşurarea auditurilor, inclusiv a inspecţiilor, efectuate de operator sau alt auditor mandatat şi contribuie la acestea.
În ceea ce priveşte primul paragraf litera (h), persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o
instrucţiune încalcă prezentul regulament sau alte dispoziţii din dreptul intern sau din dreptul Uniunii referitoare la protecţia datelor.
(4) În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activităţi de prelucrare specifice în numele operatorului, aceleaşi obligaţii privind protecţia datelor prevăzute în contractul sau în alt act juridic încheiat între operator şi 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 garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerinţele prezentului regulament. În cazul în care această a doua persoană împuternicită nu îşi respectă obligaţiile privind protecţia datelor, persoana împuternicită iniţială rămâne pe deplin răspunzătoare faţă de operator în ceea ce priveşte îndeplinirea obligaţiilor acestei a doua persoane împuternicite.
(5) Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, menţionat la articolul 40, sau la un mecanism de certificare aprobat, menţionat la articolul 42, poate fi utilizată ca element prin care să se demonstreze existenţa garanţiilor suficiente menţionate la alineatele (1) şi (4) din prezentul articol.
(6) Fără a aduce atingere unui contract individual încheiat între operator şi persoana împuternicită de operator, contractul sau celălalt act juridic menţionat la alineatele (3) şi (4) din prezentul articol se poate baza, integral sau parţial, pe clauze contractuale standard menţionate la alineatele (7) şi (8) din prezentul articol, inclusiv atunci când fac parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator în temeiul articolelor 42 şi 43.
(7) Comisia poate să prevadă clauze contractuale standard pentru aspectele menţionate la alineatele (3) şi (4) din prezentul articol şi în conformitate cu procedura de examinare menţionată la articolul 93 alineatul (2).
(8) O autoritate de supraveghere poate să adopte clauze contractuale standard pentru aspectele menţionate la alineatele (3) şi (4) din prezentul articol şi în conformitate cu mecanismul pentru asigurarea coerenţei menţionat la articolul 63.
(9) Contractul sau celălalt act juridic menţionat la alineatele (3) şi (4) se formulează în scris, inclusiv în format electronic.
(10) Fără a aduce atingere articolelor 82, 83 şi 84, în cazul în care o persoană împuternicită de operator încălcă prezentul regulament, prin stabilirea scopurilor şi mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce priveşte prelucrarea respectivă.

Articolul 29

Desfăşurarea activităţii de prelucrare sub autoritatea operatorului sau a persoanei împuternicite de operator

Persoana împuternicită de operator şi orice persoană care acţionează 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 excepţia cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru.

GDPR

Articolul 30
Evidenţele activităţilor de prelucrare

(1) Fiecare operator şi, după caz, reprezentantul acestuia păstrează o evidenţă a activităţilor de prelucrare desfăşurate sub responsabilitatea lor.

Respectiva evidenţă cuprinde toate următoarele informaţii:

(a) numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului cu protecţia datelor;

(b) scopurile prelucrării;

(c) o descriere a categoriilor de persoane vizate şi 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 ţări terţe sau organizaţii internaţionale;

(e) dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, în cazul transferurilor menţionate la articolul 49 alineatul (1) al doilea paragraf, documentaţia care dovedeşte existenţa unor garanţii 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 şi organizatorice de securitate menţionate la articolul 32 alineatul (1).

(2) Fiecare operator şi, după caz, persoana împuternicită de operator păstrează o evidenţă a tuturor categoriilor de activităţi de prelucrare desfăşurate în numele operatorului, care cuprind:

(a) numele şi datele de contact ale persoanei sau persoanelor împuternicite de operator şi ale fiecărui operator în numele căruia acţionează această persoană (aceste persoane), precum şi ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;

(b) categoriile de activităţi de prelucrare desfăşurate în numele fiecărui operator;

(c) dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, în cazul transferurilor prevăzute la articolul 49 alineatul (1) al doilea paragraf, documentaţia care dovedeşte existenţa unor garanţii adecvate;

(d) acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la articolul 32 alineatul (1).

(3) Evidenţele menţionate la alineatele (1) şi (2) se formulează în scris, inclusiv în format electronic.

(4) Operatorul sau persoana împuternicită de acesta, precum şi, după caz, reprezentantul operatorului sau al persoanei împuternicite de operator pun evidenţele la dispoziţia autorităţii de supraveghere, la cererea acesteia.

(5) Obligaţiile menţionate la alineatele 1 şi 2 nu se aplică unei întreprinderi sau organizaţii cu mai puţin de 250 de angajaţi, cu excepţia cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile şi libertăţile 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 şi infracţiuni, astfel cum se menţionează la articolul 10.

Articolul 31
Cooperarea cu autoritatea de supraveghere

Operatorul şi persoana împuternicită de operator şi, după caz, reprezentantul acestora cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor lor.

GDPR

Secţiunea 2
Securitatea datelor cu caracter personal

Articolul 32
Securitatea prelucrării
(1) Având în vedere stadiul actual al dezvoltării, costurile implementării şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscul
cu diferite grade de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul şi persoana împuternicită de acesta implementează măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:
(a) pseudonimizarea şi criptarea datelor cu caracter personal;
(b) capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare;
(c) capacitatea de a restabili disponibilitatea datelor cu caracter personal şi 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 şi aprecierea periodice ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.
(2) La evaluarea nivelului adecvat de securitate, se ţine 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, menţionat la articolul 40, sau la un mecanism de certificare aprobat, menţionat la articolul 42, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerinţelor prevăzute la alineatul (1) din prezentul articol.
(4) Operatorul şi persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator şi care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepţia cazului în care această obligaţie îi revine în temeiul dreptului Uniunii sau al dreptului intern.

Articolul 33
Notificarea autorităţii de supraveghere în cazul încălcării securităţii datelor cu caracter personal
(1) În cazul în care are loc o încălcare a securității datelor cu character personal, operatorul notifică acest lucru autorităţii de supraveghere competente în temeiul articolului 55, fără întârzieri nejustificate şi, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta, cu excepţia cazului în care este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice. În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoţită de o explicaţie motivată din partea autorității de supraveghere în cazul în care.
(2) Persoana împuternicită de operator înştiinţează operatorul fără întârzieri nejustificate după ce ia cunoştinţă de o încălcare a securităţii datelor cu caracter personal.
(3) Notificarea menţionată la alineatul (1) cel puţin:
(a) descrie caracterul încălcării securităţii datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile şi numărul aproximativ al persoanelor vizate în cauză, precum şi categoriile şi numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
(b) comunică numele şi datele de contact ale responsabilului cu protecţia datelor sau un alt punct de contact de unde se pot obţine mai multe informaţii;
(c) descrie consecinţele probabile ale încălcării securităţii datelor cu caracter personal;
(d) descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securităţii datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.
(4) Atunci când şi în măsura în care nu este posibil să se furnizeze informaţiile în acelaşi timp, acestea pot fi

furnizate în mai multe etape, fără întârzieri nejustificate.
(5) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securităţii datelor cu caracter personal, care cuprind o descriere a situaţiei de fapt în care a avut loc încălcarea securităţii datelor cu caracter personal, a efectelor acesteia şi a măsurilor de remediere întreprinse. Această documentaţie permite autorităţii de supraveghere să verifice conformitatea cu prezentul articol.

Articolul 34
Informarea persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal
(1) În cazul în care încălcarea securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile
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 şi simplu a caracterului încălcării securităţii datelor cu caracter personal, precum şi cel puţin informaţiile şi măsurile menţionate la articolul 33 alineatul (3) literele (b),
(c) şi (d).
(3) Informarea persoanei vizate menţionată la alineatul (1) nu este necesară în cazul în care oricare dintre următoarele condiţii este îndeplinită:
(a) operatorul a implementat măsuri de protecţie tehnice şi organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securităţii 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 şi libertăţile persoanelor vizate menţionat la alineatul (1) nu mai este susceptibil să se materializeze;
(c) ar necesita un efort disproporţionat. În această situaţie, 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 securităţii datelor cu caracter personal către persoana vizată, autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securităţii datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condiţiile menţionate la alineatul (3) sunt îndeplinite.

Secţiunea 3
Evaluarea impactului asupra protecţiei datelor şi consultarea prealabilă

Articolul 35
Evaluarea impactului asupra protecţiei datelor
(1) Având în vedere natura, domeniul de aplicare, contextul şi 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 şi libertăţile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal. O evaluare unică poate aborda un set de operaţiuni de prelucrare similare care prezintă riscuri ridicate similare.
(2) La realizarea unei evaluări a impactului asupra protecţiei datelor, operatorul solicită avizul responsabilului cu protecţia datelor, dacă acesta a fost desemnat.
(3) Evaluarea impactului asupra protecţiei datelor menţionată la alineatul (1) se impune mai ales în cazul:
(a) unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi 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, menţionată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale şi infracţiuni, menţionată la articolul 10; sau

GDPR

(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

(4) Autoritatea de supraveghere întocmeşte şi publică o listă a tipurilor de operaţiuni de prelucrare care fac obiectul cerinţei de efectuare a unei evaluări a impactului asupra protecţiei datelor, în conformitate cu alineatul (1). Autoritatea de supraveghere comunică aceste liste comitetului menţionat la articolul 68.

(5) Autoritatea de supraveghere poate, de asemenea, să stabilească şi să pună la dispoziţia publicului o listă a tipurilor de operaţiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecţiei datelor. Autoritatea de supraveghere comunică aceste liste comitetului.

(6) Înainte de adoptarea listelor menţionate la alineatele (4) şi (5), autoritatea de supraveghere competentă aplică mecanismul pentru asigurarea coerenţei menţionat la articolul 63 în cazul în care aceste liste implică activităţi 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 substanţial libera circulaţie a datelor cu caracter personal în cadrul Uniunii.

(7) Evaluarea conţine cel puţin:

(a) o descriere sistematică a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

(b) o evaluare a necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri;

(c) o evaluare a riscurilor pentru drepturile şi libertăţile persoanelor vizate menţionate la alineatul (1); şi

(d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor cu caracter personal şi să demonstreze conformitatea cu dispoziţiile prezentului regulament, luând în considerare drepturile şi interesele legitime ale persoanelor vizate şi ale altor persoane interesate.

(8) La evaluarea impactului operaţiunilor 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 menţionate la articolul 40, în special în vederea unei evaluări a impactului asupra protecţiei datelor.

(9) Operatorul solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanţilor acestora privind prelucrarea prevăzută, fără a aduce atingere protecţiei intereselor comerciale sau publice ori securităţii operaţiunilor 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 incidenţa căruia intră operatorul, iar dreptul respectiv reglementează operaţiunea de prelucrare specifică sau setul de operaţiuni specifice în cauză şi deja s-a efectuat o evaluare a impactului asupra protecţiei datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, alineatele (1)-(7) nu se aplică, cu excepţia cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfăşurării activităţilor de prelucrare.

(11) Acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecţiei datelor, cel puţin atunci când are loc o modificare a riscului reprezentat de operaţiunile de prelucrare.

Articolul 36

Consultarea prealabilă

(1) Operatorul consultă autoritatea de supraveghere înainte de prelucrarea atunci când evaluarea impactului asupra protecţiei datelor prevăzută la

articolul 35 indică faptul că prelucrarea ar genera un risc ridicat în absenţa unor măsuri luate de operator pentru atenuarea riscului.

(2) Atunci când consideră că prelucrarea prevăzută menţionată 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 şi, după caz, persoanei împuternicite de operator, în cel mult opt săptămâni de la primirea cererii de consultare, şi îşi poate utiliza oricare dintre competenţele menţionate la

articolul 58. Această perioadă poate fi prelungită cu şase săptămâni, ţinându- se seama de complexitatea prelucrării prevăzute. Autoritatea de supraveghere informează operatorul şi, după caz, persoana împuternicită de operator, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când autoritatea de supraveghere a obţinut informaţiile 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, responsabilităţile respective ale operatorului, ale operatorilor asociaţi şi ale persoanelor împuternicite de operator implicate în activităţile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;

(b) scopurile şi mijloacele prelucrării preconizate;

(c) măsurile şi garanţiile prevăzute pentru protecţia drepturilor şi libertăţilor persoanelor vizate, în conformitate cu prezentul regulament;

(d) dacă este cazul, datele de contact ale responsabilului cu protecţia datelor;

(e) evaluarea impactului asupra protecţiei datelor prevăzută la articolul 35; şi

(f) orice alte informaţii 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 naţional 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 şi să obţină 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 protecţia socială şi sănătatea publică.

Secţiunea 4
Responsabilul cu protecţia datelor

Articolul 37
Desemnarea responsabilului cu protecţia datelor

(1) Operatorul şi persoana împuternicită de operator desemnează un responsabil cu protecţia datelor ori de câte ori:

(a) prelucrarea este efectuată de o autoritate sau un organism public, cu excepţia instanţelor care acţionează în exerciţiul funcţiei lor jurisdicţionale;

(b) activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în operaţiuni de prelucrare care, prin natura, domeniul de aplicare şi/sau scopurile lor, necesită o monitorizare periodică şi sistematică a persoanelor vizate pe scară largă; sau

(c) activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date, menţionată la articolul 9, sau a unor date cu caracter personal privind condamnări penale şi infracţiuni, menţionată la articolul 10.

(2) Un grup de întreprinderi poate numi un responsabil cu protecţia datelor unic, cu condiţia ca responsabilul cu protecţia datelor să fie uşor 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 protecţia datelor unic pentru mai multe dintre aceste autorităţi sau organisme, luând în considerare structura organizatorică şi dimensiunea acestora.

(4) În alte cazuri decât cele menţionate la alineatul (1), operatorul sau persoana împuternicită de operator ori asociaţiile şi 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 protecţia datelor. Responsabilul cu protecţia datelor poate să acţioneze în favoarea unor astfel de asociaţii şi alte organisme care reprezintă operatori sau persoane împuternicite de operatori.

GDPR

(5) Responsabilul cu protecţia datelor este desemnat pe baza calităţilor profesionale şi, în special, a cunoştinţelor de specialitate în dreptul şi practicile din domeniul protecţiei datelor, precum şi pe baza capacităţii de a îndeplini sarcinile prevăzute la articolul 39.
(6) Responsabilul cu protecţia datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să îşi îndeplinească sarcinile în baza unui contract de servicii.
(7) Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecţia datelor şi le comunică autorităţii de supraveghere.

Articolul 38
Funcţia responsabilului cu protecţia datelor
(1) Operatorul şi persoana împuternicită de operator se asigură că responsabilul cu protecţia datelor este implicat în mod corespunzător şi în timp
util în toate aspectele legate de protecţia datelor cu caracter personal.
(2) Operatorul şi persoana împuternicită de operator sprijină responsabilul cu protecţia datelor în îndeplinirea sarcinilor menţionate la articolul 39, asigurându-i resursele necesare pentru executarea acestor sarcini, precum şi accesarea datelor cu caracter personal şi a operaţiunilor de prelucrare, şi pentru menţinerea cunoştinţelor sale de specialitate.
(3) Operatorul şi persoana împuternicită de operator se asigură că responsabilul cu protecţia datelor nu primeşte niciun fel de instrucţiuni în ceea ce priveşte îndeplinirea acestor sarcini. Acesta nu este demis sau sancţionat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. Responsabilul cu protecţia datelor răspunde direct în faţa celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.
(4) Persoanele vizate pot contacta responsabilul cu protecţia datelor cu privire la toate chestiunile legate de prelucrarea datelor lor şi la exercitarea drepturilor lor în temeiul prezentului regulament.
(5) Responsabilul cu protecţia datelor are obligaţia de a respecta secretul sau confidenţialitatea în ceea ce priveşte îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.
(6) Responsabilul cu protecţia datelor poate îndeplini şi alte sarcini şi atribuţii. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini şi atribuţii nu generează un conflict de interese.

Articolul 39
Sarcinile responsabilului cu protecţia datelor
(1) Responsabilul cu protecţia datelor are cel puţin următoarele sarcini:
(a) informarea şi consilierea operatorului, sau a persoanei împuternicite de operator, precum şi a angajaţilor care se ocupă de prelucrare cu privire la obligaţiile care le revin în temeiul prezentului regulament şi al altor dispoziţii de drept al Uniunii sau drept intern referitoare la protecţia datelor;
(b) monitorizarea respectării prezentului regulament, a altor dispoziţii de drept al Uniunii sau de drept intern referitoare la protecţia datelor şi a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce priveşte protecţia datelor cu caracter personal, inclusiv alocarea responsabilităţilor şi acţiunile de sensibilizare şi de formare a personalului implicat în operaţiunile de prelucrare, precum şi auditurile aferente;
(c) furnizarea de consiliere la cerere în ceea ce priveşte evaluarea impactului asupra protecţiei datelor şi monitorizarea funcţionării 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 menţionată la articolul 36, precum şi, dacă este cazul, consultarea cu privire la orice altă chestiune.
(2) În îndeplinirea sarcinilor sale, responsabilul cu protecţia datelor ţine seama în mod corespunzător de riscul asociat operaţiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul şi scopurile prelucrării.

GDPR

Secţiunea 5
Coduri de conduită şi certificare

Articolul 40
Coduri de conduită

(1) Statele membre, autorităţile de supraveghere, comitetul şi Comisia încurajează elaborarea de coduri de conduită menite să contribuie la buna aplicare a prezentului regulament, ţinând seama de caracteristicile specifice ale diverselor sectoare de prelucrare şi de nevoile specifice ale microîntreprinderilor şi ale întreprinderilor mici şi mijlocii.

(2) Asociaţiile şi 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 priveşte:

(a) prelucrarea în mod echitabil şi 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 şi a persoanelor vizate;

(f) exercitarea drepturilor persoanelor vizate;

(g) informarea şi protejarea copiilor şi modalitatea în care trebuie obţinut consimţământul titularilor răspunderii părinteşti asupra copiilor;

(h) măsurile şi procedurile menţionate la articolele 24 şi 25 şi măsurile de asigurare a securităţii prelucrării, menţionate la articolul 32;

(i) notificarea autorităţilor de supraveghere cu privire la încălcările securităţii datelor cu caracter personal şi informarea persoanelor vizate cu privire la aceste încălcări;

(j) transferul de date cu caracter personal către ţări terţe sau organizaţii internaţionale; sau

(k) proceduri extrajudiciare şi alte proceduri de soluţionare a litigiilor pentru soluţionarea litigiilor între operatori şi persoanele vizate în ceea ce priveşte prelucrarea, fără a aduce atingere drepturilor persoanelor vizate, în temeiul articolelor 77 şi 79.

(3) La codurile de conduită aprobate în temeiul alineatului (5) din prezentul articol şi 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 şi operatorii sau persoanele împuternicite de operatori care nu fac obiectul prezentului regulament în temeiul articolului 3, în scopul de a oferi garanţii adecvate în cadrul transferurilor de date cu caracter personal către ţări terţe sau organizaţii internaţionale în condiţiile menţionate la articolul 46 alineatul (2) litera (e). Aceşti operatori sau persoane împuternicite de operatori îşi asumă angajamente cu caracter obligatoriu şi executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, în scopul aplicării garanţiilor 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 menţionat la articolul 41 alineatul (1) să efectueze monitorizarea obligatorie a respectării dispoziţiilor acestuia de către operatorii sau persoanele împuternicite de operatori care se angajează să îl aplice, fără a aduce atingere sarcinilor şi competenţelor autorităţilor de supraveghere care sunt competente în temeiul articolului 55 sau 56.

(5) Asociaţiile şi alte organisme menţionate la alineatul (2) din prezentul articol care intenţionează să pregătească un cod de conduită sau să modifice sau să extindă un cod existent transmit proiectul de cod, de modificare sau de extindere autorităţii 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 şi îl aprobă în cazul în care se constată că acesta oferă garanţii 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 activităţile de prelucrare din mai multe state membre, autoritatea de supraveghere înregistrează şi publică codul.

GDPR

(7) În cazul în care un proiect de cod de conduită, de modificare sau de extindere are legătură cu activităţile de prelucrare din mai multe state membre, înainte de aprobare, autoritatea de supraveghere competentă în temeiul articolului 55 îl transmite, prin procedura menţionată la articolul 63, comitetului, care emite un aviz cu privire la conformitatea cu prezentul regulament a proiectului respectiv, sau, în situaţia menţionată la alineatul (3) din prezentul articol, oferă garanţii adecvate.

(8) În cazul în care avizul menţionat la alineatul (7) confirmă conformitatea cu prezentul regulament a proiectului de cod, de modificare sau de extindere sau în cazul în care, în situaţia menţionată la alineatul (3), oferă garanţii 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 şi extinderile aprobate într-un registru şi le pune la dispoziţia publicului prin mijloace corespunzătoare.

Articolul 41

Monitorizarea codurilor de conduită aprobate

(1) Fără a aduce atingere sarcinilor şi competenţelor autorităţii de supraveghere competente în temeiul articolelor 57 şi 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 şi care este acreditat în acest scop de autoritatea de supraveghere competentă.

(2) Un organism menţionat la alineatul (1) poate fi acreditat pentru monitorizarea respectării unui cod de conduită dacă:

(a) a demonstrat autorităţii de supraveghere competente, într-un mod satisfăcător, independenţa şi expertiza sa în legătură cu obiectul codului;

(b) a instituit proceduri care îi permit să evalueze eligibilitatea operatorilor şi a persoanelor împuternicite de operatori în vederea aplicării codului, să monitorizeze respectarea de către aceştia a dispoziţiilor codului şi să revizuiască periodic funcţionarea acestuia;

(c) a instituit proceduri şi 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 şi pentru asigurarea transparenţei acestor proceduri şi structuri pentru persoanele vizate şi pentru public; şi

(d) a demonstrat autorităţii de supraveghere competente, într-un mod satisfăcător, că sarcinile şi atribuţiile sale nu creează conflicte de interese.

(3) Autoritatea de supraveghere competentă transmite proiectul de criterii pentru acreditarea unui organism menţionat la alineatul (1) din prezentul articol comitetului, în conformitate cu mecanismul pentru asigurarea coerenţei menţionat la articolul 63.

(4) Fără a aduce atingere sarcinilor şi competenţelor autorităţii de supraveghere competente şi dispoziţiilor capitolului VIII, un organism menţionat la alineatul (1) din prezentul articol ia măsuri corespunzătoare, sub rezerva unor garanţii 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 şi la motivele care le-au determinat.

(5) Autoritatea de supraveghere competentă revocă acreditarea unui organism menţionat la alineatul (1) în cazul în care nu mai sunt îndeplinite condiţiile pentru acreditare sau măsurile luate de organismul în cauză încalcă prezentul regulament.

(6) Prezentul articol nu se aplică prelucrării efectuate de autorităţi şi organisme publice.

GDPR

Articolul 42

Certificare

(1) Statele membre, autorităţile de supraveghere, comitetul şi Comisia încurajează, în special la nivelul Uniunii, instituirea de mecanisme de

certificare în domeniul protecţiei datelor, precum şi de sigilii şi mărci în acest domeniu, care să permită demonstrarea faptului că operaţiunile de prelucrare efectuate de operatori şi de persoanele împuternicite de operatori respectă prezentul regulament. Sunt luate în considerare necesităţile specifice ale microîntreprinderilor şi ale întreprinderilor mici şi mijlocii.

(2) Mecanismele de certificare din domeniul protecţiei datelor, sigiliile sau mărcile aprobate în temeiul alineatului (5) din prezentul articol sunt instituite nu numai pentru a fi respectate de operatorii sau de persoanele împuternicite de operatori care fac obiectul prezentului regulament, ci şi pentru a demonstra existenţa unor garanţii adecvate oferite de operatorii sau de persoanele împuternicite de operatori care nu fac obiectul prezentului regulament, în temeiul articolului 3, în cadrul transferurilor de date cu caracter personal către ţări terţe sau organizaţii internaţionale în condiţiile menţionate la articolul 46 alineatul (2) litera (f) . Aceşti operatori sau persoane împuternicite de operatori îşi asumă angajamente cu caracter obligatoriu şi executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, în scopul aplicării garanţiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.

(3) Certificarea este voluntară şi disponibilă prin intermediul unui proces transparent.

(4) Certificarea în conformitate cu prezentul articol nu reduce responsabilitatea operatorului sau a persoanei împuternicite de operator de a respecta prezentul regulament şi nu aduce atingere sarcinilor şi competenţelor autorităţilor de supraveghere care sunt competente în temeiul articolului 55 sau 56.

(5) Organismele de certificare menţionate 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, şi anume sigiliul european privind protecţia datelor.

(6) Operatorul sau persoana împuternicită de operator care supune activităţile sale de prelucrare mecanismului de certificare oferă organismului de certificare menţionat la articolul 43 sau, după caz, autorităţii de supraveghere competente, toate informaţiile necesare pentru desfăşurarea procedurii de certificare, precum şi accesul la activităţile de prelucrare respective.

(7) Certificarea este eliberată unui operator sau unei persoane împuternicite de operator pentru o perioadă maximă de trei ani şi poate fi reînnoită în aceleaşi condiţii, cu condiţia ca cerinţele relevante să fie îndeplinite în continuare. Certificarea este retrasă, după caz, de către organismele de certificare menţionate la articolul 43 sau de către autoritatea de supraveghere competentă în cazul în care nu mai sunt îndeplinite cerinţele pentru certificare.

(8) Comitetul regrupează toate mecanismele de certificare şi sigiliile şi mărcile de protecţie a datelor într-un registru şi le pune la dispoziţia publicului prin orice mijloc corespunzător.

Articolul 43

Organisme de certificare

(1) Fără a aduce atingere sarcinilor şi competenţelor autorităţii de supraveghere competente, prevăzute la articolele 57 şi 58, organismele de

certificare care dispun de un nivel adecvat de competenţă în domeniul protecţiei datelor, după ce informează autoritatea de supraveghere pentru a-i permite să îşi exercite competenţele în temeiul articolului 58 alineatul (2) litera (h), emit şi reînnoiesc certificarea. Statele membre se asigură că aceste organisme de certificare sunt acreditate de către una sau amândouă dintre următoarele entităţi:

(a) autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56;

(b) organismul naţional de acreditare desemnat în conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European şi al Consiliului în conformitate cu standardul EN-ISO/IEC 17065/2012 şi cu cerinţele suplimentare stabilite de autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56.

GDPR

(2) Un organism de certificare menţionat la alineatul (1) este acreditat în conformitate cu alineatul respectiv numai dacă:

(a) a demonstrat autorităţii de supraveghere competente, într-un mod satisfăcător, independenţa şi expertiza sa în legătură cu obiectul certificării;

(b) s-a angajat să respecte criteriile menţionate la articolul 42 alineatul (5) şi 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 şi retragerea certificării, a sigiliilor şi mărcilor din domeniul protecţiei datelor;

(d) a instituit proceduri şi 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 şi pentru asigurarea transparenţei acestor proceduri şi structuri pentru persoanele vizate şi pentru public; şi

(e) a demonstrat autorităţii de supraveghere competente, într-un mod satisfăcător, că sarcinile şi atribuţiile sale nu creează conflicte de interese.

(3) Acreditarea organismelor de certificare menţionate la alineatele (1) şi (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 cerinţe le completează pe cele prevăzute în Regulamentul (CE) nr. 765/2008 şi normele tehnice care descriu metodele şi procedurile organismelor de certificare.

(4) Organismele de certificare menţionate la alineatul (1) sunt responsabile cu realizarea unei evaluări adecvate în vederea certificării sau retragerii acestei certificări, fără a aduce atingere responsabilităţii operatorului sau a persoanei împuternicite de operator de a respecta prezentul regulament. Acreditarea se eliberează pentru o perioadă maximă de cinci ani şi poate fi reînnoită în aceleaşi condiţii, cu condiţia ca organismul de certificare să îndeplinească cerinţele prevăzute în prezentul articol.

(5) Organismele de certificare menţionate la alineatul (1) transmite autorităţilor de supraveghere competente motivele acordării sau retragerii certificării solicitate.

(6) Cerinţele menţionate la alineatul (3) din prezentul articol şi criteriile menţionate la articolul 42 alineatul (5) se publică de către autoritatea de supraveghere într-o formă uşor de accesat. Autorităţile de supraveghere transmit, de asemenea, aceste cerinţe şi criterii comitetului. Comitetul regrupează toate mecanismele de certificare şi sigiliile de protecţie a datelor într-un registru şi le pune la dispoziţia publicului prin orice mijloc corespunzător.

(7) Fără a aduce atingere dispoziţiilor capitolului VIII, autoritatea de supraveghere competentă sau organismul naţional 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 condiţiile 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 cerinţelor care trebuie luate în considerare pentru mecanismele de certificare din domeniul protecţiei datelor, menţionate la articolul 42 alineatul (1).

(9) Comisia poate adopta acte de punere în aplicare pentru a stabili standarde tehnice pentru mecanismele de certificare şi pentru sigiliile şi mărcile din domeniul protecţiei datelor, precum şi mecanisme de promovare şi recunoaştere a acelor mecanisme de certificare, sigilii şi mărci. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menţionată la articolul 93 alineatul (2).

CAPITOLUL V
Transferurile de date cu caracter personal către ţări terţe sau organizaţii internaţionale

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 ţară terţă sau către o organizaţie internaţională pot fi transferate doar dacă, sub rezerva celorlalte dispoziţii ale prezentului regulament, condiţiile prevăzute în prezentul capitol sunt respectate de operator şi de persoana

împuternicită de operator, inclusiv în ceea ce priveşte transferurile ulterioare de date cu caracter personal din ţara terţă sau de la organizaţia internaţională către o altă ţară terţă sau către o altă organizaţie internaţională. Toate dispoziţiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecţie a persoanelor fizice garantat prin prezentul regulament nu este subminat.

Articolul 45

Transferuri în temeiul unei decizii privind caracterul adecvat al nivelului de protecţie

(1) Transferul de date cu caracter personal către o ţară terţă sau o organizaţie internaţională se poate realiza atunci când Comisia a decis că ţara terţă, un teritoriu ori unul sau mai multe sectoare specificate din acea ţară terţă sau organizaţia internaţională în cauză asigură un nivel de protecţie adecvat. Transferurile realizate în aceste condiţii nu necesită autorizări speciale.

(2) Atunci când evaluează caracterul adecvat al nivelului de protecţie, Comisia ţine seama, în special, de următoarele elemente:

(a) statul de drept, respectarea drepturilor omului şi a libertăţilor fundamentale, legislaţia relevantă, atât generală, cât şi sectorială, inclusiv privind securitatea publică, apărarea, securitatea naţională şi dreptul penal, precum şi accesul autorităţilor publice la datele cu caracter personal, precum şi punerea în aplicare a acestei legislaţii, normele de protecţie a datelor, normele profesionale şi măsurile de securitate, inclusiv normele privind transferul ulterior de date cu caracter personal către o altă ţară terţă sau organizaţie internaţională, care sunt respectate în ţara terţă respectivă sau în organizaţia internaţională respectivă, jurisprudenţa, precum şi existenţa unor drepturi efective şi opozabile ale persoanelor vizate şi a unor reparaţii efective pe cale administrativă şi judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate;

(b) existenţa şi funcţionarea eficientă a uneia sau mai multor autorităţi de supraveghere independente în ţara terţă sau sub jurisdicţia cărora intră o organizaţie internaţională, cu responsabilitate pentru asigurarea şi impunerea respectării normelor de protecţie a datelor, incluzând competenţe adecvate de asigurare a respectării aplicării, pentru acordarea de asistenţă şi consiliere persoanelor vizate cu privire la exercitarea drepturilor acestora şi pentru cooperarea cu autorităţile de supraveghere din statele membre; şi

(c) angajamentele internaţionale la care a aderat ţara terţă sau organizaţia internaţională în cauză sau alte obligaţii care decurg din convenţii sau

instrumente obligatorii din punct de vedere juridic, precum şi din participarea acesteia la sisteme multilaterale sau regionale, mai ales în domeniul protecţiei datelor cu caracter personal.

(3) Comisia, după ce evaluează caracterul adecvat al nivelului de protecţie, poate decide, printr-un act de punere în aplicare, că o ţară terţă, un teritoriu sau unul sau mai multe sectoare specificate dintr-o ţară terţă sau o organizaţie internaţională asigură un nivel de protecţie adecvat în sensul alineatului (2) din prezentul articol. Actul de punere în aplicare prevede un mecanism de revizuire periodică, cel puţin o dată la patru ani, care ia în considerare toate evoluţiile relevante din ţara terţă sau organizaţia internaţională. Actul de punere în aplicare menţionează aplicarea geografică şi sectorială, şi, după caz, identifică autoritatea sau autorităţile de supraveghere menţionate la alineatul (2) litera (b) din prezentul articol. Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 93 alineatul (2).

(4) Comisia monitorizează continuu evoluţiile din ţările terţe şi de la nivelul organizaţiilor internaţionale care ar putea afecta funcţionarea deciziilor adoptate în temeiul alineatului (3) din prezentul articol şi a deciziilor adoptate în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE.

(5) În cazul în care informaţiile disponibile dezvăluie, în special în urma revizuirii menţionate la alineatul (3) din prezentul articol, că o ţară terţă, un teritoriu sau un sector specificat din acea ţară terţă sau o organizaţie internaţională nu mai asigură un nivel de protecţie 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 menţionată la alineatul (3) din prezentul articol fără efect retroactiv. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menţionată la articolul 93 alineatul (2).

Din motive imperioase de urgenţă, Comisia adoptă acte de punere în aplicare imediat aplicabile în conformitate cu procedura menţionată la articolul 93 alineatul (3).

GDPR

(6) Comisia iniţiază consultări cu ţara terţă sau organizaţia internaţională în vederea remedierii situaţiei 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 ţara terţă, un teritoriu sau unul sau mai multe sectoare specificate din acea ţară terţă sau către organizaţia internaţională în cauză în conformitate cu articolele 46-49.
(8) Comisia publică în Jurnalul Oficial al Uniunii Europene şi pe site-ul său o listă a ţărilor terţe, a teritoriilor şi sectoarelor specificate dintr-o ţară terţă şi a organizaţiilor internaţionale în cazul cărora a decis că nivelul de protecţie 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 garanţii adecvate
(1) În absenţa unei decizii în temeiul articolului 45 alineatul (3), operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională numai dacă operatorul sau persoana împuternicită de operator a oferit garanţii adecvate şi cu condiţia să existe drepturi opozabile şi căi de atac eficiente pentru persoanele vizate.
(2) Garanţiile adecvate menţionate la alineatul 1 pot fi furnizate fără să fie nevoie de nicio autorizaţie specifică din partea unei autorităţi de supraveghere, prin:
(a) un instrument obligatoriu din punct de vedere juridic şi executoriu între autorităţile sau organismele publice;
(b) reguli corporatiste obligatorii în conformitate cu articolul 47;
(c) clauze standard de protecţie a datelor adoptate de Comisie în conformitate cu procedura de examinare menţionată la articolul 93 alineatul (2);
(d) clauze standard de protecţie a datelor adoptate de o autoritate de supraveghere şi aprobate de Comisie în conformitate cu procedura de examinare menţionată la articolul 93 alineatul (2);
(e) un cod de conduită aprobat în conformitate cu articolul 40, însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a persoanei împuternicite de operator din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau
(f) un mecanism de certificare aprobat în conformitate cu articolul 42, însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a persoanei împuternicite de operator din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate.
(3) Sub rezerva autorizării din partea autorităţii de supraveghere competente, garanţiile adecvate menţionate la alineatul (1) pot fi furnizate de asemenea, în special, prin:
(a) clauze contractuale între operator sau persoana împuternicită de operator şi operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din ţara terţă sau organizaţia internaţională; sau
(b) dispoziţii care urmează să fie incluse în acordurile administrative dintre autorităţile sau organismele publice, care includ drepturi opozabile şi efective pentru persoanele vizate.
(4) Autoritatea de supraveghere aplică mecanismul pentru asigurarea coerenţei menţionat la articolul 63, în cazurile menţionate la alineatul (3) din prezentul articol.
(5) Autorizaţiile 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.

GDPR

Articolul 47

Reguli corporatiste obligatorii

(1) În conformitate cu mecanismul pentru asigurarea coerenţei prevăzut la articolul 63, autoritatea de supraveghere competentă aprobă reguli
corporatiste obligatorii, cu condiţia ca acestea:

(a) să fie obligatorii din punct de vedere juridic şi să se aplice fiecărui membru vizat al grupului de întreprinderi sau al grupului de întreprinderi
implicate într-o activitate economică comună, inclusiv angajaţilor acestuia, precum şi să fie puse în aplicare de membrii în cauză;

(b) să confere, în mod expres, drepturi opozabile persoanelor vizate în ceea ce priveşte prelucrarea datelor lor cu caracter personal; şi

(c) să îndeplinească cerinţele prevăzute la alineatul (2).

(2) Regulile corporatiste obligatorii menţionate la alineatul (1) precizează cel puţin:

(a) structura şi datele de contact ale grupului de întreprinderi sau ale grupului de întreprinderi implicate într-o activitate economică comună şi ale fiecăruia dintre membrii săi;

(b) transferurile de date sau setul de transferuri, inclusiv categoriile de date cu caracter personal, tipul prelucrării şi scopurile prelucrării, tipurile de persoane vizate afectate şi identificarea ţării terţe sau a ţărilor terţe în cauză;

(c) caracterul lor juridic obligatoriu, atât pe plan intern, cât şi extern;

(d) aplicarea principiilor generale în materie de protecţie a datelor, în special limitarea scopului, reducerea la minimum a datelor, perioadele de stocare limitate, calitatea datelor, protecţia datelor începând cu momentul conceperii şi protecţia implicită, temeiul juridic pentru prelucrare, prelucrarea categoriilor speciale de date cu caracter personal, măsurile de asigurare a securităţii datelor, precum şi cerinţele referitoare la transferurile ulterioare către organisme care nu fac obiectul regulilor corporatiste obligatorii;

(e) drepturile persoanelor vizate în ceea ce priveşte prelucrarea şi 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 faţa autorităţii de supraveghere competente şi în faţa instanţelor competente ale
statelor membre, în conformitate cu articolul 79, precum şi dreptul de a obţine reparaţii şi, după caz, despăgubiri pentru încălcarea regulilor corporatiste obligatorii;

(f) acceptarea de către operator sau de persoana împuternicită de operator, care îşi are sediul pe teritoriul unui stat membru, a răspunderii pentru orice încălcare a regulilor corporatiste obligatorii de către orice membru în cauză care nu îşi are sediul în Uniune; operatorul sau persoana împuternicită de operator este exonerat(ă) de această răspundere, integral sau parţial, numai dacă dovedeşte că membrul respectiv nu a fost răspunzător de evenimentul care a cauzat prejudiciul;

(g) modul în care informaţiile privind regulile corporatiste obligatorii, în special privind dispoziţiile menţionate la literele (d), (e) şi (f) de la prezentul alineat, sunt furnizate persoanelor vizate în completarea informaţiilor menţionate la articolele 13 şi 14;

(h) sarcinile oricărui responsabil cu protecţia datelor desemnat în conformitate cu articolul 37 sau ale oricărei alte persoane sau entităţi însărcinate cu monitorizarea respectării regulilor corporatiste obligatorii în cadrul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, a activităţilor de formare şi 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 conformităţii cu regulile corporatiste obligatorii. Aceste mecanisme includ auditurile privind protecţia datelor şi metodele de asigurare a acţiunilor corective menite să protejeze drepturile persoanei vizate. Rezultatele acestor verificări ar trebui să fie comunicate persoanei sau entităţii menţionate la litera

(h) şi consiliului de administraţie al întreprinderii care exercită controlul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună şi ar trebui să fie puse la dispoziţia autorităţii de

GDPR

supraveghere competente, la cerere;
(k) mecanismele de raportare şi înregistrare a modificărilor aduse regulilor şi de raportare a acestor modificări autorităţii 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 dispoziţia autorităţii de supraveghere a rezultatelor verificărilor cu privire la măsurile menţionate la punctul (j);
(m) mecanismele de raportare către autoritatea de supraveghere competentă a oricăror cerinţe legale impuse unui membru al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună într-o ţară terţă care pot avea un efect advers considerabil asupra garanţiilor furnizate prin regulile corporatiste obligatorii; şi
(n) formarea corespunzătoare în domeniul protecţiei datelor a personalului care are un acces permanent sau periodic la date cu caracter personal.
(3) Comisia poate preciza formatul şi procedurile pentru schimbul de informaţii între operatori, persoanele împuternicite de operatori şi autorităţile 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 informaţii neautorizate de dreptul Uniunii Orice hotărâre a unei instanţe sau a unui tribunal şi orice decizie a unei autorităţi administrative a unei ţări terţe 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 internaţional, cum ar fi un tratat de asistenţă judiciară reciprocă în vigoare între ţara terţă solicitantă şi Uniune sau un stat membru, fără a se aduce atingere altor motive de transfer în temeiul prezentului capitol.

Articolul 49
Derogări pentru situaţii specifice
(1) În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie în conformitate cu articolul 45 alineatul (3) sau a unor garanţii 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 ţară terţă sau o organizaţie internaţională poate avea loc numai în una dintre condiţiile următoare:
(a) persoana vizată şi-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 protecţie şi a unor garanţii adecvate;
(b) transferul este necesar pentru executarea unui contract între persoana vizată şi 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 şi 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 instanţă;
(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-şi exprima acordul;
(g) transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau al dreptului intern, are scopul de a furniza informaţii publicului şi 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 condiţiile cu privire la consultare prevăzute de dreptul Uniunii sau de dreptul intern în acel caz specific.

GDPR

În cazul în care un transfer nu ar putea să se întemeieze pe o dispoziţie prevăzută la articolul 45 sau 46, inclusiv dispoziţii privind reguli corporatiste obligatorii, şi nu este aplicabilă niciuna dintre derogările pentru situaţii specifice prevăzute la primul paragraf din prezentul alineat, un transfer către o ţară terţă sau o organizaţie internaţională 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 şi libertăţile persoanei vizate şi operatorul a evaluat toate circumstanţele aferente transferului de date şi, pe baza acestei evaluări, a prezentat garanţii corespunzătoare în ceea ce priveşte protecţia datelor cu caracter personal. Operatorul informează autoritatea de supraveghere cu privire la transfer. Operatorul, în plus faţă de furnizarea informaţiilor menţionate la articolele 13 şi 14, informează persoana vizată cu privire la transfer şi la interesele legitime majore pe care le urmăreşte.

(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) şi (c) şi paragraful al doilea nu se aplică în cazul activităţilor desfăşurate de autorităţile publice în exercitarea competenţelor lor publice.

(4) Interesul public prevăzut la alineatul (1) primul paragraf litera (d) este recunoscut în dreptul Uniunii sau în dreptul statului membru sub incidenţa căruia intră operatorul.

(5) În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie, 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 ţară terţă sau o organizaţie internaţională. Statele membre notifică aceste dispoziţii Comisiei.

(6) Operatorul sau persoana împuternicită de operator consemnează evaluarea, precum şi garanţiile adecvate prevăzute la paragraful al doilea al alineatului (1) din prezentul articol, în evidenţele menţionate la articolul 30.

Articolul 50

Cooperarea internaţională în domeniul protecţiei datelor cu caracter personal În ceea ce priveşte ţările terţe şi organizaţiile internaţionale, Comisia şi autorităţile de supraveghere iau măsurile corespunzătoare pentru:

(a) elaborarea de mecanisme de cooperare internaţională pentru a facilita asigurarea aplicării efective a legislaţiei privind protecţia datelor cu caracter personal;

(b) acordarea de asistenţă internaţională reciprocă în asigurarea aplicării legislaţiei din domeniul protecţiei datelor cu caracter personal, inclusiv prin notificare, transferul plângerilor, asistenţă în investigaţii şi schimb de informaţii, sub rezerva unor garanţii adecvate pentru protecţia datelor cu caracter personal şi a altor drepturi şi libertăţi fundamentale;

(c) implicarea părţilor interesate relevante în discuţiile şi activităţile care au ca scop intensificarea cooperării internaţionale în domeniul aplicării legislaţiei privind protecţia datelor cu caracter personal;

(d) promovarea schimbului reciproc şi a documentaţiei cu privire la legislaţia şi practicile în materie de protecţie a datelor cu caracter personal, inclusiv în ceea ce priveşte conflictele jurisdicţionale cu ţările terţe.

CAPITOLUL VI
Autorităţi de supraveghere independente

Secţiunea 1
Statutul independent

Articolul 51

Autoritatea de supraveghere

(1) Fiecare stat membru se asigură că una sau mai multe autorităţi publice independente sunt responsabile de monitorizarea aplicării prezentului

regulament, în vederea protejării drepturilor şi libertăţilor fundamentale ale persoanelor fizice în ceea ce priveşte prelucrarea şi în vederea facilitării liberei circulaţii 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, autorităţile de supraveghere cooperează atât între ele, cât şi cu Comisia, în conformitate cu capitolul VII.
(3) În cazul în care mai multe autorităţi de supraveghere sunt instituite într- un stat membru, acesta desemnează autoritatea de supraveghere care reprezintă autorităţile respective în cadrul comitetului şi instituie un mecanism prin care să asigure respectarea de către celelalte autorităţi a normelor privind mecanismul pentru asigurarea coerenţei prevăzut la articolul 63.
(4) Fiecare stat membru notifică Comisiei dispoziţiile de drept pe care le adoptă în temeiul prezentului capitol până la 25 mai 2018 şi, fără întârziere, orice modificare ulterioară pe care o aduce acestor dispoziţii.

Articolul 52
Independenţă
(1) Fiecare autoritate de supraveghere beneficiază de independenţă deplină în
îndeplinirea sarcinilor sale şi exercitarea competenţelor sale în conformitate cu prezentul regulament.
(2) Membrul sau membrii fiecărei autorităţi de supraveghere, în cadrul îndeplinirii sarcinilor şi al exercitării competenţelor sale (lor) în conformitate cu prezentul regulament, rămâne (rămân) independent (independenţi) de orice
influenţă externă directă sau indirectă şi nici nu solicită, nici nu acceptă instrucţiuni de la o parte externă.
(3) Membrul sau membrii fiecărei autorităţi de supraveghere se abţin de la a întreprinde acţiuni incompatibile cu atribuţiile lor, iar pe durata mandatului, nu desfăşoară activităţi incompatibile, remunerate sau nu.
(4) Fiecare stat membru se asigură că fiecare autoritate de supraveghere beneficiază de resurse umane, tehnice şi financiare, de un sediu şi de infrastructura necesară pentru îndeplinirea sarcinilor şi exercitarea efectivă a competenţelor sale, inclusiv a celor care urmează să fie aplicate în contextul asistenţei reciproce, al cooperării şi al participării în cadrul comitetului.
(5) Fiecare stat membru se asigură că fiecare autoritate de supraveghere îşi selectează personalul propriu şi deţine personal propriu aflat sub conducerea exclusivă a membrului sau membrilor autorităţii de supraveghere respective.
(6) Fiecare stat membru se asigură că fiecare autoritate de supraveghere face obiectul unui control financiar care nu aduce atingere independenţei sale şi că dispune de bugete anuale distincte, publice, care pot face parte din bugetul general de stat sau naţional.

Articolul 53
Condiţii generale aplicabile membrilor autorităţii de supraveghere
(1) Statele membre se asigură că fiecare membru al autorităţii lor de supraveghere este numit prin intermediul unei proceduri transparente:
- de parlament;
- de guvern;
- de şeful statului; sau
- de un organism independent împuternicit să facă numiri în temeiul dreptului intern.

(2) Fiecare membru în cauză are calificările, experienţa şi competenţele necesare, în special în domeniul protecţiei datelor cu caracter personal, pentru a-şi putea îndeplini atribuţiile şi exercita competenţele.
(3) Atribuţiile 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 îndeplineşte condiţiile necesare pentru îndeplinirea atribuţiilor sale.

GDPR

Articolul 54
Norme privind instituirea autorităţii de supraveghere
(1) Fiecare stat membru prevede, pe cale legislativă, următoarele:
(a) instituirea fiecărei autorităţi de supraveghere;
(b) calificările şi condiţiile de eligibilitate necesare pentru a fi numit în calitate de membru al fiecărei autorităţi de supraveghere;
(c) normele şi procedurile pentru numirea membrului sau a membrilor fiecărei autorităţi de supraveghere;
(d) durata mandatului membrului sau membrilor fiecărei autorităţi de supraveghere, de minimum patru ani, cu excepţia 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 independenţa autorităţii de supraveghere printr-o procedură de numiri eşalonate;
(e) dacă şi de câte ori este eligibil pentru reînnoire mandatul membrului sau membrilor fiecărei autorităţi de supraveghere;
(f) condiţiile care reglementează obligaţiile membrului sau membrilor şi ale personalului fiecărei autorităţi de supraveghere, interdicţii privind acţiunile, ocupaţiile şi beneficiile incompatibile cu acestea în cursul mandatului şi după încetarea acestuia, precum şi normele care reglementează încetarea contractului de angajare.
(2) Membrul sau membrii şi personalul fiecărei autorităţi de supraveghere au obligaţia, în conformitate cu dreptul Uniunii sau cu dreptul intern, de a respecta atât pe parcursul mandatului, cât şi după încetarea acestuia, secretul profesional în ceea ce priveşte informaţiile confidenţiale de care au luat cunoştinţă în cursul îndeplinirii sarcinilor sau al exercitării competenţelor lor. Pe durata mandatului lor, această obligaţie de păstrare a secretului profesional se aplică în special în ceea ce priveşte raportarea de către persoane fizice a încălcărilor prezentului regulament.

Secţiunea 2
Abilitări, sarcini şi competenţe

Articolul 55
Competenţa
(1) Fiecare autoritate de supraveghere are competenţa să îndeplinească sarcinile şi să exercite competenţele care îi sunt conferite în conformitate cu
prezentul regulament pe teritoriul statului membru de care aparţine.
(2) În cazul în care prelucrarea este efectuată de autorităţi publice sau de organisme private care acţionează 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) Autorităţile de supraveghere nu sunt competente să supravegheze operaţiunile de prelucrare ale instanţelor care acţionează în exerciţiul funcţiei lor judiciare.

Articolul 56
Competenţa autorităţii 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 acţioneze 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 atenţia 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 menţionate 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 ţine seama în cea mai mare măsură posibilă de proiectul respectiv atunci când pregăteşte 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 şi 62.
(6) Autoritatea de supraveghere principală este singurul interlocutor al operatorului sau al persoanei împuternicite de operator în ceea ce priveşte 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 şi asigură aplicarea prezentului regulament;
(b) promovează acţiuni de sensibilizare şi de înţelegere în rândul publicului a riscurilor, normelor, garanţiilor şi drepturilor în materie de prelucrare. Se acordă atenţie specială activităţilor care se adresează în mod specific copiilor;
(c) oferă consiliere, în conformitate cu dreptul intern, parlamentului naţional, guvernului şi altor instituţii şi organisme cu privire la măsurile legislative şi administrative referitoare la protecţia drepturilor şi libertăţilor persoanelor fizice în ceea ce priveşte prelucrarea;
(d) promovează acţiuni de sensibilizare a operatorilor şi a persoanelor împuternicite de aceştia cu privire la obligaţiile care le revin în temeiul prezentului regulament;
(e) la cerere, furnizează informaţii oricărei persoane vizate în legătură cu exercitarea drepturilor sale în conformitate cu prezentul regulament şi, dacă este cazul, cooperează cu autorităţile de supraveghere din alte state membre în acest scop;
(f) tratează plângerile depuse de o persoană vizată, un organism, o organizaţie sau o asociaţie în conformitate cu articolul 80 şi investighează într- o măsură adecvată obiectul plângerii şi informează reclamantul cu privire la evoluţia şi rezultatul investigaţiei, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigaţii mai amănunţite sau coordonarea cu o altă autoritate de supraveghere;
(g) cooperează, inclusiv prin schimb de informaţii, cu alte autorităţi de supraveghere şi îşi oferă asistenţă reciprocă pentru a asigura coerenţa aplicării şi respectării prezentului regulament;
(h) desfăşoară investigaţii privind aplicarea prezentului regulament, inclusiv pe baza unor informaţii primite de la o altă autoritate de supraveghere sau de la o altă autoritate publică;
(i) monitorizează evoluţiile relevante, în măsura în care acestea au impact asupra protecţiei datelor cu caracter personal, în special evoluţia tehnologiilor informaţiei şi comunicaţiilor şi a practicilor comerciale;
(j) adoptă clauze contractuale standard menţionate la articolul 28 alineatul
(8) şi la articolul 46 alineatul (2) litera (d);
(k) întocmeşte şi menţine la zi o listă în legătură cu cerinţa privind evaluarea impactului asupra protecţiei datelor, în conformitate cu articolul 35 alineatul (4);
(l) oferă consiliere cu privire la operaţiunile de prelucrare menţionate la articolul 36 alineatul (2);
(m) încurajează elaborarea de coduri de conduită în conformitate cu articolul 40 alineatul (1), îşi dă avizul cu privire la acestea şi le aprobă pe cele care oferă suficiente garanţii, în conformitate cu articolul 40 alineatul (5);
(n) încurajează stabilirea unor mecanisme de certificare, precum şi a unor sigilii şi mărci în domeniul protecţiei datelor în conformitate cu articolul 42 alineatul (1) şi 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 şi publică criteriile de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu articolul 41 şi 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 şi a unui organism de certificare în conformitate cu articolul 43;
(r) autorizează clauzele şi dispoziţiile contractuale menţionate la articolul 46 alineatul (3);
(s) aprobă regulile corporatiste obligatorii în conformitate cu articolul 47;
(t) contribuie la activităţile comitetului;
(u) menţine la zi evidenţe interne privind încălcările prezentului regulament şi măsurile luate, în special avertismentele emise şi sancţiunile impuse în conformitate cu articolul 58 alineatul (2); şi
(v) îndeplineşte orice alte sarcini legate de protecţia datelor cu caracter personal.
(2) Fiecare autoritate de supraveghere facilitează depunerea plângerilor menţionate la alineatul (1) litera (f) prin măsuri precum punerea la dispoziţie 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 autorităţi de supraveghere este gratuită pentru persoana vizată şi, după caz, pentru responsabilul cu protecţia 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 autorităţii de supraveghere.

Articolul 58
Competenţe
(1) Fiecare autoritate de supraveghere are toate următoarele competenţe de investigare:
(a) de a da dispoziţii operatorului şi persoanei împuternicite de operator şi, după caz, reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informaţii pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale;
(b) de a efectua investigaţii sub formă de audituri privind protecţia 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 obţine, din partea operatorului şi a persoanei împuternicite de operator, accesul la toate datele cu caracter personal şi la toate informaţiile necesare pentru îndeplinirea sarcinilor sale;
(f) de a obţine accesul la oricare dintre incintele operatorului şi ale persoanei împuternicite de operator, inclusiv la orice echipamente şi mijloace de prelucrare a datelor, în conformitate cu dreptul Uniunii sau cu dreptul procesual intern.
(2) Fiecare autoritate de supraveghere are toate următoarele competenţe corective:
(a) de a emite avertizări în atenţia unui operator sau a unei persoane împuternicite de operator cu privire la posibilitatea ca operaţiunile de prelucrare prevăzute să încalce dispoziţiile prezentului regulament;
(b) de a emite mustrări adresate unui operator sau unei persoane împuternicite de operator în cazul în care operaţiunile de prelucrare au încălcat dispoziţiile prezentului regulament;
(c) de a da dispoziţii operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-şi exercita drepturile în temeiul prezentului regulament;
(d) de a da dispoziţii operatorului sau persoanei împuternicite de operator să asigure conformitatea operaţiunilor de prelucrare cu dispoziţiile prezentului regulament, specificând, după caz, modalitatea şi termenul-limită pentru aceasta;
(e) de a obliga operatorul să informeze persoana vizată cu privire la o încălcare a protecţiei datelor cu caracter personal;
(f) de a impune o limitare temporară sau definitivă, inclusiv o interdicţie asupra prelucrării;

GDPR

(g) de a dispune rectificarea sau ştergerea datelor cu caracter personal sau restricţionarea prelucrării, în temeiul articolelor 16, 17 şi 18, precum şi notificarea acestor acţiuni destinatarilor cărora le-au fost divulgate datele cu caracter personal, în conformitate cu articolul 17 alineatul (2) şi cu articolul 19;
(h) de a retrage o certificare sau de a obliga organismul de certificare să retragă o certificare eliberată în temeiul articolul 42 şi 43 sau de a obliga organismul de certificare să nu elibereze o certificare în cazul în care cerinţele 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 menţionate la prezentul alineat, în funcţie de circumstanţele fiecărui caz în parte;
(j) de a dispune suspendarea fluxurilor de date către un destinatar dintr-o ţară terţă sau către o organizaţie internaţională.
(3) Fiecare autoritate de supraveghere are toate următoarele competenţe de autorizare şi de consiliere:
(a) de a oferi consiliere operatorului în conformitate cu procedura de consultare prealabilă menţionată la articolul 36;
(b) de a emite avize, din proprie iniţiativă sau la cerere, parlamentului naţional, guvernului statului membru sau, în conformitate cu dreptul intern, altor instituţii şi organisme, precum şi publicului, cu privire la orice aspect legat de protecţia datelor cu caracter personal;
(c) de a autoriza prelucrarea menţionată la articolul 36 alineatul (5), în cazul în care dreptul statului membru prevede o astfel de autorizare prealabilă;
(d) de a emite un aviz şi 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 şi de a aproba criterii de certificare în conformitate cu articolul 42 alineatul (5);
(g) de a adopta clauzele standard în materie de protecţie a datelor menţionate la articolul 28 alineatul (8) şi la articolul 46 alineatul (2) litera (d);
(h) de a autoriza clauzele contractuale menţionate la articolul 46 alineatul (3) litera (a);
(i) de a autoriza acordurile administrative menţionate la articolul 46 alineatul
(3) litera (b); şi
(j) de a aproba reguli corporatiste obligatorii în conformitate cu articolul 47.
(4) Exercitarea competenţelor conferite autorităţii de supraveghere în temeiul prezentului articol face obiectul unor garanţii adecvate, inclusiv căi de atac judiciare eficiente şi procese echitabile, prevăzute în dreptul Uniunii şi în dreptul intern în conformitate cu carta.
(5) Fiecare stat membru prevede, pe cale legislativă, faptul că autoritatea sa de supraveghere are competenţa de a aduce în faţa autorităţilor judiciare cazurile de încălcare a prezentului regulament şi, după caz, de a iniţia sau de a se implica într-un alt mod în proceduri judiciare, în scopul de a asigura aplicarea dispoziţiilor prezentului regulament.
(6) Fiecare stat membru poate să prevadă în dreptul său faptul că autoritatea sa de supraveghere are competenţe suplimentare, în afara celor menţionate la alineatele (1), (2) şi (3). Exercitarea acestor competenţe nu afectează modul de operare eficientă a capitolului VII.

Articolul 59
Rapoarte de activitate
Fiecare autoritate de supraveghere întocmeşte un raport anual cu privire la activităţile sale, care poate include o listă a tipurilor de încălcări notificate şi a tipurilor de măsuri luate în conformitate cu articolul 58 alineatul (2). Rapoartele se transmit parlamentului naţional, guvernului şi altor autorităţi desemnate prin dreptul intern. Acestea se pun la dispoziţia publicului, a Comisiei şi a comitetului.

GDPR

CAPITOLUL VII
Cooperare şi coerenţă

Secţiunea 1
Cooperare

Articolul 60
Cooperarea dintre autoritatea de supraveghere principală şi celelalte autorităţi de supraveghere vizate

(1) Autoritatea de supraveghere principală cooperează cu celelalte autorităţi de supraveghere vizate, în conformitate cu prezentul articol, în încercarea de a ajunge la un consens. Autoritatea de supraveghere principală şi autorităţile de
supraveghere vizate îşi comunică reciproc toate informaţiile relevante.

(2) Autoritatea de supraveghere principală poate solicita în orice moment altor autorităţi de supraveghere vizate să ofere asistenţă reciprocă în temeiul articolului 61 şi poate desfăşura operaţiuni comune în temeiul articolului 62, în special în vederea efectuării de investigaţii 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 informaţiile relevante referitoare la această chestiune celorlalte autorităţi de supraveghere vizate. Autoritatea de supraveghere principală transmite fără întârziere un proiect de decizie celorlalte autorităţi de supraveghere vizate, pentru a obţine avizul lor, şi ţine seama în mod corespunzător de opiniile acestora.

(4) În cazul în care oricare dintre celelalte autorităţi de supraveghere vizate exprimă, în termen de patru săptămâni după ce a fost consultată în conformitate cu alineatul (3) din prezentul articol, o obiecţie relevantă şi motivată la proiectul de decizie, autoritatea de supraveghere principală, în cazul în care nu dă curs obiecţiei relevante şi motivate sau consideră că obiecţia nu este relevantă sau motivată, sesizează mecanismul pentru asigurarea coerenţei menţionat la articolul 63.

(5) În cazul în care intenţionează să dea curs obiecţiei relevante şi motivate formulate, autoritatea de supraveghere principală transmite celorlalte autorităţi de supraveghere vizate un proiect revizuit de decizie pentru a obţine avizul acestora. Acest proiect revizuit de decizie face obiectul procedurii menţionate la alineatul (4) pe parcursul unei perioade de două săptămâni.

(6) În cazul în care niciuna dintre celelalte autorităţi de supraveghere vizate nu a formulat obiecţii la proiectul de decizie transmis de autoritatea de supraveghere principală în termenul menţionat la alineatele (4) şi (5), se consideră că autoritatea de supraveghere principală şi autorităţile de supraveghere vizate sunt de acord cu proiectul de decizie respectiv, care devine obligatoriu pentru acestea.

(7) Autoritatea de supraveghere principală adoptă decizia şi o notifică sediului principal sau sediului unic al operatorului sau al persoanei împuternicite de operator, după caz, şi informează celelalte autorităţi de supraveghere vizate şi comitetul cu privire la decizia în cauză, incluzând un rezumat al elementelor şi 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 şi informează operatorul cu privire la acest lucru.

(9) În cazul în care autoritatea de supraveghere principală şi autorităţile de supraveghere vizate sunt de acord să refuze sau să respingă anumite părţi ale unei plângeri şi să dea curs altor părţi ale plângerii respective, se adoptă o decizie separată pentru fiecare dintre aceste părţi. Autoritatea de supraveghere principală adoptă decizia pentru partea care vizează acţiunile 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 şi 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 şi informează operatorul sau persoana împuternicită de operator cu privire la acest lucru.

(10) În urma notificării deciziei autorităţii de supraveghere principale în temeiul alineatelor (7) şi (9), operatorul

sau persoana împuternicită de operator ia măsurile necesare pentru a se asigura că activităţile 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 autorităţii de supraveghere principale, care informează celelalte autorităţi de supraveghere vizate.

(11) În cazul în care, în circumstanţe excepţionale, o autoritate de supraveghere vizată are motive să considere că există o nevoie urgentă de a acţiona în vederea protejării intereselor persoanelor vizate, se aplică procedura de urgenţă prevăzută la articolul 66.

(12) Autoritatea de supraveghere principală şi celelalte autorităţi de supraveghere vizate îşi furnizează reciproc informaţiile solicitate în temeiul prezentului articol, pe cale electronică, utilizând un formular standard.

Articolul 61

Asistenţă reciprocă

(1) Autorităţile de supraveghere îşi furnizează reciproc informaţii relevante şi asistenţă pentru a pune în aplicare prezentul regulament în mod coerent şi instituie măsuri de cooperare eficace între ele. Asistenţa reciprocă se referă, în special, la cereri de informaţii şi măsuri de supraveghere, cum ar fi cereri privind autorizări şi consultări prealabile, inspecţii şi investigaţii.

(2) Fiecare autoritate de supraveghere ia toate măsurile corespunzătoare necesare pentru a răspunde unei cererii a unei alte autorităţi de supraveghere, fără întârzieri nejustificate şi cel târziu în termen de o lună de la data primirii cererii. Aceste măsuri pot include, în special, transmiterea informaţiilor relevante privind desfăşurarea unei investigaţii.

(3) Cererile de asistenţă cuprind toate informaţiile necesare, inclusiv scopul cererii şi motivele care stau la baza acesteia. Informaţiile 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 excepţia cazului în care:

(a) nu are competenţă 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 incidenţa 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 îşi motivează fiecare refuz de a da curs cererii în temeiul alineatului (4).

(6) Ca regulă, autorităţile de supraveghere solicitate furnizează informaţiile solicitate de alte autorităţi de supraveghere pe cale electronică, utilizând un formular standard.

(7) Autorităţile de supraveghere solicitate nu percep nicio taxă pentru acţiunile întreprinse de acestea în temeiul unei cereri de asistenţă reciprocă. Autorităţile de supraveghere pot conveni asupra unor norme privind retribuţiile reciproce în cazul unor cheltuieli specifice rezultate în urma acordării de asistenţă reciprocă în situaţii excepţionale.

(8) În cazul în care o autoritate de supraveghere nu furnizează informaţiile menţionate la alineatul (5) din prezentul articol în termen de o lună de la primirea cererii din partea altei autorităţi 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 acţiona în temeiul articolului 66 alineatul (1) este considerată a fi îndeplinită şi 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 şi procedurile pentru asistenţa reciprocă menţionată în prezentul articol, precum şi modalităţile de schimb de informaţii pe cale electronică între autorităţile de supraveghere şi între autorităţile de supraveghere şi comitet, în special formularul standard menţionat la alineatul (6) din prezentul articol. Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menţionată la articolul 93 alineatul (2).

Articolul 62

Operaţiuni comune ale autorităţilor de supraveghere

(1) După caz, autorităţile de supraveghere desfăşoară operaţiuni comune, inclusiv investigaţii comune şi măsuri

comune de aplicare a legii, în care sunt implicaţi membri sau personal din autorităţile de supraveghere ale altor state membre.

(2) În cazul în care operatorul sau persoana împuternicită de operator deţine 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 operaţiuni de prelucrare, o autoritate de supraveghere din fiecare dintre statele membre respective are dreptul de a participa la operaţiunile comune. Autoritatea de supraveghere care este competentă în conformitate cu articolul 56 alineatul (1) sau alineatul (4) invită autorităţile de supraveghere din fiecare dintre aceste state membre să ia parte la operaţiunile comune respective şi răspunde fără întârziere la cererea de participare a unei autorităţi de supraveghere.

(3) O autoritate de supraveghere poate, în conformitate cu dreptul intern şi cu acordul autorităţii de supraveghere din statul membru de origine, să acorde competenţe, inclusiv competenţe de investigare, membrilor sau personalului autorităţii de supraveghere din statul membru de origine implicaţi în operaţiuni comune sau, în măsura în care dreptul statului membru al autorităţii de supraveghere din statul membru de primire permite acest lucru, poate autoriza membrii sau personalul autorităţii de supraveghere din statul membru de origine să îşi exercite competenţele de investigare în conformitate cu dreptul statului membru al acestei din urmă autorităţi. Astfel de competenţe de

investigare pot fi exercitate doar sub coordonarea şi în prezenţa membrilor sau personalului autorităţii de supraveghere din statul membru de primire. Membrii sau personalul autorităţii de supraveghere din statul membru de origine sunt supuşi dreptului intern sub incidenţa căruia intră autoritatea de supraveghere din statul membru de primire.

(4) În cazul în care, în conformitate cu alineatul (1), personalul unei autorităţi de supraveghere din statul membru de origine îşi desfăşoară activitatea într-un alt stat membru, statul membru de primire îşi asumă responsabilitatea pentru acţiunile personalului respectiv, inclusiv răspunderea pentru eventualele prejudicii cauzate de membrii personalului respectiv în cursul operaţiunilor acestora, în conformitate cu dreptul statului membru pe teritoriul căruia îşi desfăşoară operaţiunile.

(5) Statul membru pe teritoriul căruia s-au produs prejudiciile repară aceste prejudicii în condiţiile aplicabile prejudiciilor cauzate de propriul său personal. Statul membru de origine al autorităţii 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 îndreptăţite în numele acestora.

(6) Fără a aduce atingere exercitării drepturilor sale faţă de terţe părţi şi cu excepţia alineatului (5), fiecare stat membru se abţine, în cazul prevăzut la alineatul (1), de la a pretinde de la un alt stat membru rambursarea despăgubirilor pentru prejudiciile menţionate la alineatul (4).

(7) În cazul în care este planificată o operaţiune comună, iar o autoritate de supraveghere nu se conformează, în termen de o lună, obligaţiei prevăzute în a doua teză a alineatului (2) din prezentul articol, celelalte autorităţi de supraveghere pot adopta o măsură provizorie pe teritoriul statului membru al respectivei autorităţi, în conformitate cu articolul 55. În acest caz, necesitatea urgentă de a acţiona în temeiul articolului 66 alineatul (1) este considerată a fi îndeplinită şi necesită un aviz de urgenţă sau o decizie obligatorie urgentă din partea comitetului, în conformitate cu articolul 66 alineatul (2).

Secţiunea 2
Asigurarea coerenţei

Articolul 63

Mecanismul pentru asigurarea coerenţei

Pentru a contribui la aplicarea coerentă a prezentului regulament în întreaga Uniune, autorităţile de supraveghere cooperează între ele şi, după caz, cu Comisia prin mecanismul pentru asigurarea coerenţei, astfel cum se prevede în prezenta secţiune.

GDPR

Articolul 64
Avizul comitetului

(1) Comitetul emite un aviz de fiecare dată când o autoritate de supraveghere competentă intenţionează 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 operaţiuni de prelucrare care fac obiectul cerinţei de efectuare a unei evaluări a impactului asupra protecţiei 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 protecţie a datelor menţionate la articolul 46 alineatul (2) litera (d) sau la articolul 28 alineatul (8);

(e) vizează autorizarea clauzelor contractuale menţionate la articolul 46 alineatul (3) litera (a); sau

(f) vizează aprobarea regulilor corporatiste obligatorii în sensul articolului 47.

(2) Orice autoritate de supraveghere, preşedintele comitetului sau Comisia po ate 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 obţinerii unui aviz, în special în cazul în care o autoritate de supraveghere competentă nu respectă obligaţiile privind asistenţa reciprocă în conformitate cu articolul 61 sau privind operaţiunile comune în conformitate cu articolul 62.

(3) În cazurile menţionate la alineatele (1) şi (2), comitetul emite un aviz cu privire la chestiunea care îi este prezentată, cu condiţia să nu fi emis deja un aviz cu privire la aceeaşi chestiune. Avizul respectiv este adoptat în termen de opt săptămâni cu majoritatea simplă a membrilor comitetului. Această perioadă poate fi prelungită cu şase săptămâni, ţinându-se seama de complexitatea chestiunii. În ceea ce priveşte proiectul de decizie menţionat la alineatul (1) transmis membrilor comitetului în conformitate cu alineatul (5), un membru care nu a emis obiecţii într-un termen rezonabil indicat de preşedinte se consideră a fi de acord cu proiectul de decizie.

(4) Autorităţile de supraveghere şi Comisia comunică pe cale electronică comitetului, fără întârzieri nejustificate, printr-un formular standard, orice informaţie relevantă, inclusiv, după caz, o sinteză a faptelor, proiectul de decizie, motivele care fac necesară adoptarea unei astfel de măsuri, precum şi opiniile altor autorităţi de supraveghere vizate.

(5) Preşedintele comitetului informează pe cale electronică, fără întârzieri nejustificate:

(a) membrii comitetului şi Comisia cu privire la orice informaţie relevantă care i-a fost comunicată, utilizând un formular standard. Secretariatul comitetului furnizează traduceri ale informaţiilor relevante, acolo unde este necesar; şi

(b) autoritatea de supraveghere menţionată, după caz, la alineatele (1) şi (2), şi Comisia cu privire la aviz şi îl publică.

(6) Autoritatea de supraveghere competentă nu îşi adoptă proiectul de decizie menţionat la alineatul (1) în termenul menţionat la alineatul (3).

(7) Autoritatea de supraveghere menţionată la alineatul (1) ţine seama pe deplin de avizul comitetului şi comunică pe cale electronică preşedintelui comitetului, în termen de două săptămâni de la primirea avizului, dacă îşi va păstra sau îşi va modifica proiectul de decizie şi, dacă este cazul, transmite proiectul de decizie modificat, utilizând un formular standard.

(8) În cazul în care autoritatea de supraveghere vizată informează preşedintele comitetului, în termenul menţionat la alineatul (7) din prezentul articol, că intenţionează să nu se conformeze avizului comitetului, integral sau parţial, oferind motivele relevante, se aplică articolul 65 alineatul (1).

Articolul 65
Soluţionarea litigiilor de către comitet

(1) Pentru a asigura aplicarea corectă şi coerentă a prezentului regulament în cazuri individuale, comitetul adoptă o

decizie obligatorie în următoarele cazuri:
(a) atunci când, în unul dintre cazurile menţionate la articolul 60 alineatul (4), o autoritate de supraveghere vizată a formulat o obiecţie relevantă şi motivată la un proiect de decizie a autorităţii principale sau autoritatea principală a respins o astfel de obiecţie ca nefiind relevantă sau motivată. Decizia obligatorie se referă la toate chestiunile vizate de obiecţia relevantă şi motivată, în special la chestiunea dacă prezentul regulament a fost încălcat;
(b) în cazul în care există opinii divergente cu privire la care dintre autorităţile de supraveghere vizate deţine competenţa pentru sediul principal;
(c) în cazul în care o autoritate de supraveghere competentă nu solicită avizul comitetului în cazurile menţionate la articolul 64 alineatul (1) sau nu ţine 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 menţionată 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, ţinându-se seama de complexitatea chestiunii. Decizia menţionată la alineatul (1) se motivează şi se adresează autorităţii de supraveghere principale şi tuturor autorităţilor de supraveghere vizate, fiind obligatorie pentru acestea.
(3) În cazul în care comitetul nu a fost în măsură să adopte o decizie în termenele menţionate la alineatul (2), acesta îşi adoptă decizia în termen de două săptămâni de la data expirării celei de a doua luni menţionate la alineatul (2), cu o majoritate simplă a membrilor săi. În cazul în care membrii comitetului au opinii divergente în proporţii egale, decizia se adoptă prin votul preşedintelui.
(4) Autorităţile de supraveghere vizate nu adoptă o decizie asupra chestiunii prezentate comitetului în conformitate cu alineatul (1) în termenele menţionate la alineatele (2) şi (3).
(5) Preşedintele comitetului notifică, fără întârzieri nejustificate, decizia menţionată la alineatul (1) autorităţilor 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 menţionate la alineatul (6).
(6) Autoritatea de supraveghere principală sau, dacă este cazul, autoritatea de supraveghere la care s-a depus plângerea îşi adoptă decizia finală pe baza deciziei menţionate la alineatul (1) din prezentul articol, fără întârziere nejustificată şi 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 şi, respectiv, persoanei vizate. Decizia finală a autorităţilor de supraveghere vizate se adoptă în conformitate cu condiţiile prevăzute la articolul 60 alineatele (7), (8) şi (9). Decizia finală se referă la decizia menţionată la alineatul (1) din prezentul articol şi precizează faptul că decizia menţionată la respectivul alineat va fi publicată pe site-ul al comitetului, în conformitate cu alineatul (5). La decizia finală se anexează decizia menţionată la alineatul (1) din prezentul articol.

Articolul 66
Procedura de urgenţă
(1) În circumstanţe excepţionale, atunci când o autoritate de supraveghere vizată consideră că există o necesitate urgentă de a acţiona în scopul protejării drepturilor şi libertăţilor persoanelor vizate, aceasta poate, prin derogare de la mecanismul pentru asigurarea coerenţei menţionat la articolele 63, 64 şi 65 sau de la procedura menţionată 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 depăşească trei luni. Autoritatea de supraveghere comunică fără întârziere aceste măsuri şi motivele adoptării lor celorlalte autorităţi de supraveghere vizate, comitetului şi Comisiei.
(2) În cazul în care o autoritate de supraveghere a adoptat o măsură în temeiul alineatului (1) şi consideră că este necesară adoptarea de urgenţă a unor măsuri definitive, aceasta poate solicita un aviz de urgenţă sau o decizie obligatorie urgentă din partea comitetului, indicând motivele pentru această solicitare.
(3) Orice autoritate de supraveghere poate solicita un aviz de urgenţă 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

situaţie în care există o necesitate urgentă de a acţiona pentru a proteja drepturile şi libertăţile persoanelor vizate, indicând motivele pentru solicitarea unui astfel de aviz sau a unei astfel de decizii, inclusiv pentru necesitatea urgentă de a acţiona.
(4) Prin derogare de la articolul 64 alineatul (3) şi de la articolul 65 alineatul (2), un aviz de urgenţă sau o decizie obligatorie urgentă menţionat(ă) la alineatele (2) şi (3) de la prezentul articol este adoptat(ă) în termen de două săptămâni cu majoritate simplă a membrilor comitetului.

Articolul 67
Schimb de informaţii
Comisia poate adopta acte de punere în aplicare cu un domeniu de aplicare general pentru a defini modalităţile de realizare a schimbului electronic de
informaţii între autorităţile de supraveghere, precum şi între autorităţile de supraveghere şi comitet, în special formularul standard menţionat la articolul 64.
Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menţionată la articolul 93 alineatul (2).

Secţiunea 3
Comitetul european pentru protecţia datelor

Articolul 68
Comitetul european pentru protecţia datelor
(1) Comitetul european pentru protecţia datelor ("comitetul") este instituit ca organ al Uniunii şi are personalitate juridică.
(2) Comitetul este reprezentat de preşedintele său.
(3) Comitetul este alcătuit din şeful unei autorităţi de supraveghere din fiecare stat membru şi din Autoritatea Europeană pentru Protecţia Datelor sau reprezentanţii respectivi ai acestora.
(4) În cazul în care într-un stat membru mai multe autorităţi de supraveghere sunt responsabile de monitorizarea aplicării dispoziţiilor adoptate în temeiul prezentului regulament, se numeşte un reprezentant comun în conformitate cu dreptul intern al statului membru respectiv.
(5) Comisia are dreptul de a participa la activităţile şi reuniunile comitetului fără a avea drept de vot. Comisia numeşte un reprezentant. Preşedintele comitetului comunică Comisiei activităţile comitetului.
(6) În cazurile menţionate la articolul 65, Autoritatea Europeană pentru Protecţia Datelor deţine drept de vot numai cu privire la deciziile care privesc principiile şi normele aplicabile în ceea ce priveşte instituţiile, organismele, oficiile şi agenţiile Uniunii care corespund pe fond cu cele din prezentul regulament.

Articolul 69
Independenţă
(1) Comitetul acţionează independent în îndeplinirea sarcinilor sale sau în exercitarea competenţelor sale în conformitate cu articolele 70 şi 71.
(2) Fără a aduce atingere solicitărilor din partea Comisiei menţionate la articolul 70 alineatul (1) litera (b) şi la articolul 70 alineatul (2), comitetul, în îndeplinirea sarcinilor sale sau în exercitarea competenţelor sale, nu solicită şi nu acceptă instrucţiuni de la nicio parte externă.

Articolul 70
Sarcinile comitetului
(1) Comitetul asigură aplicarea coerentă a prezentului regulament. În acest scop, din proprie iniţiativă sau, după caz, la solicitarea Comisiei, comitetul are,
în special, următoarele sarcini:
(a) să monitorizeze şi să asigure aplicarea corectă a prezentului regulament, în cazurile prevăzute la articolele 64 şi

GDPR

65, fără a aduce atingere sarcinilor autorităţilor naţionale de supraveghere;
(b) să ofere consiliere Comisiei cu privire la orice aspect legat de protecţia 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 şi procedurile pentru schimbul de informaţii între operatori, persoanele împuternicite de operatori şi autorităţile de supraveghere pentru regulile corporatiste obligatorii;
(d) să emită orientări, recomandări şi bune practici privind procedurile de ştergere a linkurilor către datele cu caracter personal, a copiilor sau a reproducerilor acestora de care dispun serviciile de comunicaţii accesibile publicului, astfel cum se menţionează la articolul 17 alineatul (2);
(e) să examineze, din proprie iniţiativă, la cererea unuia dintre membrii săi sau la cererea Comisiei, orice chestiune referitoare la aplicarea prezentului regulament şi să emită orientări, recomandări şi bune practici pentru a încuraja aplicarea coerentă a prezentului regulament;
(f) să emită orientări, recomandări şi bune practici în conformitate cu prezentul alineat litera (e) în vederea detalierii criteriilor şi condiţiilor pentru deciziile bazate pe crearea de profiluri menţionate la articolul 22 alineatul (2);
(g) să emită orientări, recomandări şi bune practici în conformitate cu litera
(e) din prezentul alineat pentru stabilirea încălcării securităţii datelor cu caracter personal şi stabilirii întârzierilor nejustificate menţionate la articolul 33 alineatele (1) şi (2), precum şi pentru circumstanţele speciale în care un operator sau o persoană împuternicită de către operator are obligaţia de a notifica încălcarea securităţii datelor cu caracter personal;
(h) să emită orientări, recomandări şi bune practici în conformitate cu litera
(e) din prezentul alineat în ceea ce priveşte circumstanţele în care o încălcare a securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, menţionate la articolul 34 alineatul (1);
(i) să emită orientări, recomandări şi bune practici în conformitate cu litera
(e) din prezentul alineat în scopul detalierii criteriilor şi cerinţelor aplicabile transferurilor de date cu caracter personal bazate pe regulile corporatiste obligatorii care trebuie respectate de operatori şi cele care trebuie respectate de persoanele împuternicite de operatori, precum şi cu privire la cerinţe suplimentare necesare pentru a asigura protecţia datelor cu caracter personal ale persoanelor vizate menţionate la articolul 47;
(j) să emită orientări, recomandări şi bune practici în conformitate cu litera
(e) din prezentul alineat în vederea detalierii criteriilor şi cerinţelor pentru transferurile de date cu caracter personal menţionate la articolul 49 alineatul (1);
(k) să elaboreze orientări destinate autorităţilor de supraveghere, referitoare la aplicarea măsurilor menţionate la articolul 58 alineatele (1), (2) şi (3) şi să stabilească amenzile administrative în conformitate cu articolul 83;
(l) să revizuiască aplicarea practică a orientărilor, recomandărilor şi bunelor practici menţionate la literele (e) şi (f);
(m) să emită orientări, recomandări şi 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 şi stabilirea unor mecanisme de certificare, precum şi a unor sigilii şi mărci în domeniul protecţiei datelor, în conformitate cu articolele 40 şi 42;
(o) să efectueze acreditarea organismelor de certificare şi revizuirea periodică a acreditării în conformitate cu articolul 43 şi să ţină un registru public al organismelor acreditate, în conformitate cu articolul 43 alineatul (6), şi al operatorilor acreditaţi sau al persoanelor împuternicite de operator acreditate, stabiliţi (stabilite) în ţări terţe, în conformitate cu articolul 42 alineatul (7);
(p) să precizeze cerinţele menţionate la articolul 43 alineatul (3), în vederea acreditării organismelor de certificare prevăzute la articolul 42;
(q) să prezinte Comisiei un aviz privind cerinţele de certificare menţionate la articolul 43 alineatul (8);
(r) să prezinte Comisiei un aviz privind pictogramele menţionate la articolul 12 alineatul (7);
(s) să prezinte Comisiei un aviz pentru evaluarea caracterului adecvat al nivelului de protecţie într-o ţară terţă sau o organizaţie internaţională, inclusiv pentru a determina dacă o ţară terţă, un teritoriu, sau unul sau mai multe sectoare specificate din acea ţară terţă, sau o organizaţie internaţională nu mai asigură un nivel de protecţie adecvat.

GDPR

În acest scop, Comisia pune la dispoziţia comitetului toată documentaţia necesară, inclusiv corespondenţa purtată cu autorităţile publice ale ţării terţe, în ceea ce priveşte acea ţară terţă, acel teritoriu sau acel sector, sau cu organizaţia internaţională;

(t) să emită avize privind proiectele de decizii ale autorităţilor de supraveghere în conformitate cu mecanismul pentru asigurarea coerenţei menţionat la articolul 64 alineatul (1) privind chestiunile prezentate în conformitate cu articolul 64 alineatul (2) şi să emită decizii obligatorii în temeiul articolului 65, inclusiv în cazurile menţionate la articolul 66;

(u) să promoveze cooperarea şi schimbul eficient bilateral şi multilateral de informaţii şi bune practici între autorităţile de supraveghere;

(v) să promoveze programe comune de formare şi să faciliteze schimburile de personal între autorităţile de supraveghere, precum şi, după caz, cu autorităţile de supraveghere ale ţărilor terţe sau organizaţiilor internaţionale;

(w) să promoveze schimbul de cunoştinţe şi de documente privind legislaţia şi practicile în materie de protecţie a datelor cu autorităţile de supraveghere a protecţiei datelor la nivel mondial;

(x) să emită avize privind codurile de conduită elaborate la nivelul Uniunii în temeiul articolului 40 alineatul (9); şi

(y) să ţină un registru electronic accesibil publicului cu deciziile luate de autorităţile de supraveghere şi de instanţe cu privire la chestiuni tratate în cadrul mecanismului pentru asigurarea coerenţei.

(2) În cazul în care Comisia consultă comitetul, aceasta poate indica un termen limită, ţinând seama de caracterul urgent al chestiunii.

(3) Comitetul îşi transmite avizele, orientările, recomandările şi bunele practici Comisiei şi comitetului menţionat la articolul 93 şi le face publice.

(4) Dacă este cazul, comitetul consultă părţile interesate şi le oferă posibilitatea de a face observaţii într-un termen rezonabil. Fără a aduce atingere dispoziţiilor articolului 76, comitetul publică rezultatele procedurii de consultare.

Articolul 71
Rapoarte

(1) Comitetul întocmeşte un raport anual privind protecţia persoanelor fizice cu privire la prelucrare în Uniune şi, dacă este relevant, în ţări terţe şi organizaţii
internaţionale. Raportul este pus la dispoziţia publicului şi transmis Parlamentului European, Consiliului şi Comisiei.

(2) Raportul anual include o revizuire a aplicării practice a orientărilor, recomandărilor şi bunelor practici menţionate la articolul 70 alineatul (1) litera (l), precum şi a deciziilor obligatorii menţionate la articolul 65.

Articolul 72
Procedura

(1) Comitetul adoptă decizii prin majoritate simplă a membrilor săi, cu excepţia cazului când se prevede altfel în prezentul regulament.

(2) Comitetul îşi adoptă propriul regulament de procedură cu o majoritate de două treimi a membrilor săi şi îşi organizează propriile mecanisme de funcţionare.

Articolul 73
Preşedintele

(1) Comitetul alege un preşedinte şi doi vicepreşedinţi din rândul membrilor săi, cu majoritate simplă.

(2) Mandatul preşedintelui şi al vicepreşedinţilor este de cinci ani şi poate fi reînnoit o singură dată.

Articolul 74
Sarcinile preşedintelui

(1) Preşedintele are următoarele sarcini:

(a) să convoace reuniunile comitetului şi să stabilească ordinea de zi;

(b) să notifice deciziile adoptate de comitet, în conformitate cu articolul 65, autorităţii de supraveghere principale şi

GDPR

autorităţilor de supraveghere vizate;
(c) să asigure îndeplinirea la timp a sarcinilor comitetului, în special în ceea ce priveşte mecanismul pentru asigurarea coerenţei menţionat la articolul 63.
(2) Comitetul stabileşte în regulamentul său de procedură repartizarea sarcinilor între preşedinte şi vicepreşedinţi.

Articolul 75
Secretariatul
(1) Comitetul dispune de un secretariat, care este asigurat de Autoritatea Europeană pentru Protecţia Datelor.
(2) Secretariatul îşi îndeplineşte sarcinile exclusiv pe baza instrucţiunilor preşedintelui comitetului.
(3) Personalul Autorităţii Europene pentru Protecţia 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 Autorităţii Europene pentru Protecţia Datelor.
(4) Dacă este oportun, comitetul şi Autoritatea Europeană pentru Protecţia Datelor elaborează şi publică un memorandum de înţelegere pentru punerea în aplicare a prezentului articol, care să stabilească condiţiile cooperării şi să se aplice personalului Autorităţii Europene pentru Protecţia Datelor implicat în îndeplinirea sarcinilor conferite comitetului în temeiul prezentului regulament.
(5) Secretariatul oferă sprijin analitic, administrativ şi logistic comitetului.
(6) Secretariatul este responsabil în special de următoarele:
(a) gestionarea curentă a activităţii comitetului;
(b) comunicarea dintre membrii comitetului, preşedintele acestuia şi Comisie;
(c) comunicarea cu alte instituţii şi cu publicul;
(d) utilizarea mijloacelor electronice pentru comunicarea internă şi externă;
(e) traducerea informaţiilor relevante;
(f) pregătirea şi monitorizarea acţiunilor ulterioare reuniunilor comitetului;
(g) pregătirea, redactarea şi publicarea avizelor, deciziilor privind soluţionarea litigiilor dintre autorităţile de supraveghere şi a altor texte adoptate de comitet.

Articolul 76
Confidenţialitate
(1) Discuţiile din cadrul comitetului sunt confidenţiale 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, experţilor şi reprezentanţilor părţilor terţe este reglementat prin Regulamentul (CE) nr. 1049/2001 al Parlamentului European şi al Consiliului.

CAPITOLUL VIII
Căi de atac, răspundere şi sancţiuni

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 îşi are reşedinţa obişnuită, 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 evoluţia şi rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul articolului 78.

GDPR

Articolul 78

Dreptul la o cale de atac judiciară eficientă împotriva unei autorităţi 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 autorităţi 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 şi 56 nu tratează o plângere sau nu
informează persoana vizată în termen de trei luni cu privire la progresele sau la soluţionarea plângerii depuse în temeiul articolului 77.

(3) Acţiunile introduse împotriva unei autorităţi de supraveghere sunt aduse în faţa instanţelor din statul membru în care este stabilită autoritatea de supraveghere.

(4) În cazul în care acţiunile sunt introduse împotriva unei decizii a unei autorităţi de supraveghere care a fost precedată de un aviz sau o decizie a comitetului în cadrul mecanismului pentru asigurarea coerenţei, autoritatea de supraveghere transmite curţii 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 dispo nibile, 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) Acţiunile introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în faţa instanţelor din statul membru unde operatorul sau persoana împuternicită de operator îşi are un sediu. Alternativ, o astfel de acţiune poate fi prezentată în faţa instanţelor din statul membru în care persoana vizată îşi are reşedinţa obişnuită, cu excepţia cazului în care operatorul sau persoana împuternicită de operator este o autoritate publică a unui stat membru ce acţionează în exercitarea competenţelor sale publice.

Articolul 80

Reprezentarea persoanelor vizate

(1) Persoana vizată are dreptul de a mandata un organism, o organizaţie sau o asociaţie 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 protecţiei drepturilor şi libertăţilor persoanelor vizate în ceea ce priveşte protecţia datelor lor cu caracter personal, să depună plângerea în numele său, să exercite în numele său drepturile menţionate la articolele 77, 78 şi 79, precum şi să exercite dreptul de a primi despăgubiri menţionat la articolul 82 în numele persoanei vizate, dacă acest lucru este prevăzut în dreptul intern.

(2) Statele membre pot prevedea că orice organism, organizaţie sau asociaţie menţionată 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 şi de a exercita drepturile menţionate la articolele 78 şi 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 instanţă competentă a unui stat membru are informaţii că pe rolul unei instanţe dintr-un alt stat membru se află o acţiune având acelaşi obiect în ceea ce priveşte activităţile de prelucrare ale aceluiaşi operator sau

ale aceleaşi persoane împuternicite de operator, instanţa respectivă contactează instanţa din celălalt stat membru pentru a confirma existenţa unor astfel de acţiuni.
(2) Atunci când pe rolul unei instanţe dintr-un alt stat membru se află o acţiune având acelaşi obiect în ceea ce priveşte activităţile de prelucrare ale aceluiaşi operator sau ale aceleaşi persoane împuternicite de operator, orice altă instanţă competentă decât instanţa sesizată iniţial poate suspenda acţiunea aflată la ea pe rol.
(3) În cazul în care o astfel de acţiune se judecă în primă instanţă, orice
instanţă sesizată ulterior poate, de asemenea, la cererea uneia dintre părţi, să- şi decline competenţa, cu condiţia ca respectiva acţiune să fie de competenţa primei instanţe sesizate şi ca dreptul aplicabil acesteia să permită conexarea acţiunilor.

Articolul 82
Dreptul la despăgubiri şi răspunderea
(1) Orice persoană care a suferit un prejudiciu materialesau moral ca urmare a unei încălcări a prezentului regulament are dreptul să obţină despăgubiri de la
operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.
(2) Orice operator implicat în operaţiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operaţiunile 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 obligaţiile din prezentul regulament care revin în mod specific persoanelor împuternicite de operator sau a acţionat în afara sau în contradicţie cu instrucţiunile legale ale operatorului.
(3) Operatorul sau persoana împuternicită de operator este exonerat(ă) de răspundere în temeiul alineatului (2) dacă dovedeşte că nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul.
(4) În cazul în care mai mulţi operatori sau mai multe persoane împuternicite de operator, sau un operator şi o persoană împuternicită de operator sunt implicaţi (implicate) în aceeaşi operaţiune de prelucrare şi răspund, în temeiul alineatelor (2) şi (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 ceilalţi operatori sau celelalte persoane împuternicite de operator implicate în aceeaşi operaţiune
de prelucrare recuperarea acelei părţi din despăgubiri care corespunde părţii lor de răspundere pentru prejudiciu, în conformitate cu condiţiile stabilite la alineatul (2).
(6) Acţiunile în exercitarea dreptului de recuperare a despăgubirilor plătite se
introduc la instanţele competente în temeiul dreptului statului membru menţionat la articolul 79 alineatul (2).

Articolul 83
Condiţii 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 menţionate la alineatele (4), (5) şi, (6) este, în fiecare caz, eficace, proporţională şi disuasivă.
(2) În funcţie de circumstanţele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menţionate la articolul 58 alineatul (2) literele (a) - (h) şi (j). Atunci când se ia decizia dacă să se impună o amendă administrativă şi decizia cu privire la valoarea amenzii administrative în fiecare caz în parte, se acordă atenţia cuvenită următoarelor aspecte:
(a) natura, gravitatea şi durata încălcării, ţinându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum şi de numărul persoanelor vizate afectate şi de nivelul prejudiciilor suferite de acestea;
(b) dacă încălcarea a fost comisă intenţionat sau din neglijenţă;
(c) orice acţiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit

GDPR

de persoana vizată;
(d) gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ţinându-se seama de măsurile tehnice şi organizatorice implementate de aceştia în temeiul articolelor 25 şi 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 şi 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 cunoştinţa autorităţii de supraveghere, în special dacă şi în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;
(i) în cazul în care măsurile menţionate la articolul 58 alineatul (2) au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la acelaşi 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; şi
(k) orice alt factor agravant sau atenuant aplicabil circumstanţelor 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 intenţionat sau din neglijenţă, pentru aceeaşi operaţiune de prelucrare sau pentru operaţiuni de prelucrare conexe, mai multe dispoziţii din prezentul regulament, cuantumul total al amenzii administrative nu poate depăşi suma prevăzută pentru cea mai gravă încălcare.
(4) Pentru încălcările dispoziţiilor 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 exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare:
(a) obligaţiile operatorului şi ale persoanei împuternicite de operator în conformitate cu articolele 8, 11, 25-39, 42 şi 43;
(b) obligaţiile organismului de certificare în conformitate cu articolele 42 şi 43;
(c) obligaţiile organismului de monitorizare în conformitate cu articolul 41 alineatul (4).
(5) Pentru încălcările dispoziţiilor 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 exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare:
(a) principiile de bază pentru prelucrare, inclusiv condiţiile privind consimţământul, în conformitate cu articolele 5, 6, 7 şi 9;
(b) drepturile persoanelor vizate în conformitate cu articolele 12-22;
(c) transferurile de date cu caracter personal către un destinatar dintr-o ţară terţă sau o organizaţie internaţională, în conformitate cu articolele 44-49;
(d) orice obligaţii în temeiul legislaţiei naţionale 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 exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare.
(7) Fără a aduce atingere competenţelor corective ale autorităţilor de supraveghere menţionate la articolul 58 alineatul (2), fiecare stat membru poate prevedea norme prin care să se stabilească dacă şi în ce măsură pot fi impuse amenzi administrative autorităţilor publice şi organismelor publice stabilite în statul membru respectiv.
(8) Exercitarea de către autoritatea de supraveghere a competenţelor sale în temeiul prezentului articol are loc cu condiţia existenţei unor garanţii procedurale adecvate în conformitate cu dreptul Uniunii şi cu dreptul intern, inclusiv căi de atac judiciare eficiente şi dreptul la un proces echitabil.

GDPR

(9) În cazul în care sistemul juridic al statului membru nu prevede amenzi administrative, prezentul articol poate fi aplicat astfel încât amenda să fie iniţiată de autoritatea de supraveghere competentă şi impusă de instanţele naţionale competente, garantându-se, în acelaşi timp, faptul că aceste căi de atac sunt eficiente şi au un efect echivalent cu cel al amenzilor administrative impuse de autorităţile de supraveghere. În orice caz, amenzile impuse trebuie
să fie eficace, proporţionale şi disuasive. Respectivele state membre informează Comisia cu privire la dispoziţiile de drept intern pe care le adoptă în temeiul prezentului alineat până la 25 mai 2018, precum şi, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară a acestora.

Articolul 84
Sancţiuni

(1) Statele membre stabilesc normele privind alte sancţiunile aplicabile în caz de încălcare a prezentului regulament, în special pentru încălcări care nu fac
obiectul unor amenzi administrative în temeiul articolului 83, şi iau toate măsurile necesare pentru a garanta faptul că acestea sunt puse în aplicare.
Sancţiunile respective sunt eficace, proporţionale şi disuasive.

(2) Fiecare stat membru informează Comisia cu privire la dispoziţiile de drept intern pe care le adoptă în temeiul alineatului (1) până la 25 mai 2018, precum şi, fără întârziere, cu privire la orice modificare ulterioară a acestora.

CAPITOLUL IX
Dispoziţii referitoare la situaţii specifice de prelucrare

Articolul 85
Prelucrarea şi libertatea de exprimare şi de informare

(1) Prin intermediul dreptului intern, statele membre asigură un echilibru între dreptul la protecţia datelor cu caracter personal în temeiul prezentului regulament şi dreptul la libertatea de exprimare şi 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 dispoziţiile capitolului II (principii), ale capitolului III (drepturile persoanei vizate), ale capitolului IV (operatorul şi persoana împuternicită de operator), ale capitolului V (transferul datelor cu caracter personal către ţări terţe sau organizaţii internaţionale), ale capitolului VI (autorităţi de supraveghere independente), ale capitolului VII (cooperare şi coerenţă) şi ale capitolului IX (situaţii specifice de prelucrare a datelor) în cazul în care acestea sunt necesare pentru a asigura un echilibru între dreptul la protecţia datelor cu caracter personal şi libertatea de exprimare şi de informare.

(3) Fiecare stat membru informează Comisia cu privire la dispoziţiile de drept intern pe care le-a adoptat în temeiul alineatului (2) precum şi, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară a acestora.

Articolul 86
Prelucrarea şi accesul public la documente oficiale

Datele cu caracter personal din documentele oficiale deţinute de o autoritate publică sau de un organism public sau privat pentru îndeplinirea unei sarcini care serveşte interesului public pot fi divulgate de autoritatea sau organismul respectiv în conformitate cu dreptul Uniunii sau cu dreptul intern sub incidenţa căruia intră autoritatea sau organismul, pentru a stabili un echilibru între accesul public la documente oficiale şi dreptul la protecţia datelor cu caracter personal în temeiul prezentului regulament.

Articolul 87
Prelucrarea unui număr de identificare naţional

Statele membre pot detalia în continuare condiţiile specifice de prelucrare a unui număr de identificare naţional sau

a oricărui alt identificator cu aplicabilitate generală. În acest caz, numărul de identificare naţional sau orice alt identificator cu aplicabilitate generală este folosit numai în temeiul unor garanţii corespunzătoare pentru drepturile şi libertăţile 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 protecţia drepturilor şi a libertăţilor cu privire la prelucrarea datelor cu caracter personal ale angajaţilor în contextul ocupării
unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligaţiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării şi organizării muncii, al egalităţii şi diversităţii la locul de muncă, al asigurării sănătăţii şi securităţii la
locul de muncă, al protejării proprietăţii angajatorului sau a clientului, precum şi în scopul exercitării şi beneficierii, în mod individual sau colectiv, de drepturile şi beneficiile legate de ocuparea unui loc de muncă, precum şi pentru încetarea raporturilor de muncă.

(2) Aceste norme includ măsuri corespunzătoare şi specifice pentru garantarea demnităţii umane, a intereselor legitime şi a drepturilor fundamentale ale persoanelor vizate, în special în ceea ce priveşte transparenţa 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 şi sistemele de monitorizare la locul de muncă.

(3) Fiecare stat membru informează Comisia cu privire la dispoziţiile de drept intern pe care le adoptă în temeiul alineatului (1) până la 25 mai 2018, precum şi, fără întârziere, cu privire la orice modificare ulterioară a acestora.

Articolul 89

Garanţii şi derogări privind prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice

(1) Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice are loc cu condiţia existenţei unor
garanţii corespunzătoare, în conformitate cu prezentul regulament, pentru drepturile şi libertăţile persoanelor vizate. Respectivele garanţii asigură faptul că au fost instituite măsuri tehnice şi organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor.
Respectivele măsuri pot include pseudonimizarea, cu condiţia ca respectivele scopuri să fie îndeplinite în acest mod. Atunci când respectivele 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 ştiinţifică sau istorică ori în scopuri statistice, dreptul Uniunii sau dreptul intern poate să prevadă derogări de la drepturile menţionate la articolele 15, 16, 18 şi 21, sub rezerva condiţiilor şi a garanţiilor 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 menţionate la articolele 15, 16, 18, 19, 20 şi 21, sub rezerva condiţiilor şi a garanţiilor 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 menţionată la alineatele (2) şi (3) serveşte în acelaşi timp şi altui scop, derogările se aplică numai prelucrării în scopurile menţionate la alineatele respective.

GDPR

Articolul 90

Obligaţii privind păstrarea confidenţialităţii

(1) Statele membre pot adopta norme specifice pentru a stabili competenţele autorităţilor de supraveghere, prevăzute la articolul 58 alineatul (1) literele (e) şi (f), în legătură cu operatori sau cu persoane împuternicite de operatori care,

în temeiul dreptului Uniunii sau al dreptului internsau în temeiul normelor stabilite de organismele naţionale competente, au obligaţia de a păstra secretul profesional sau alte obligaţii echivalente de confidenţialitate, în cazul în care acest lucru este necesar şi proporţional pentru a stabili un echilibru între dreptul la protecţia datelor cu caracter personal şi obligaţia păstrării confidenţialităţii. Respectivele norme se aplică doar în ceea ce priveşte datele cu caracter personal pe care operatorul sau persoana împuternicită de operator le-a primit în urma sau în contextul unei activităţi care intră sub

incidenţa acestei obligaţii de păstrare a confidenţialităţii.

(2) Fiecare stat membru notifică Comisiei normele adoptate în temeiul alineatului (1) până la 25 mai 2018, precum şi, fără întârziere, orice modificare ulterioară a acestora.

Articolul 91

Normele existente în domeniul protecţiei datelor pentru biserici şi asociaţii religioase

(1) În cazul în care, într-un stat membru, bisericile şi asociaţiile sau comunităţile religioase aplică, la data intrării în vigoare a prezentului

regulament, un set cuprinzător de norme de protecţie a persoanelor fizice cu privire la prelucrare, aceste norme pot continua să se aplice, cu condiţia să fie aliniate la prezentul regulament.

(2) Bisericile şi asociaţiile religioase care aplică un set cuprinzător de norme în conformitate cu alineatul (1) din prezentul articol sunt supuse supravegherii unei autorităţi de supraveghere independente care poate fi specifică, cu condiţia să îndeplinească condiţiile stabilite în capitolul VI din prezentul regulament.

CA ITOLUL X

Acte delegate şi acte de punere în aplicare

Articolul 92

Exercitarea delegării

(1) Competenţa de a adopta acte delegate este conferită Comisiei în condiţiile prevăzute de prezentul articol.

(2) Delegarea de competenţe prevăzută la articolul 12 alineatul (8) şi la articolul 43 alineatul (8) se conferă Comisiei pe o perioadă nedeterminată de la 24 mai 2016.

(3) Delegarea de competenţe menţionată la articolul 12 alineatul (8) şi 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 competenţe 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 menţionată în decizie. Decizia nu aduce atingere validităţii actelor delegate care sunt deja în vigoare.

(4) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European şi Consiliului.

(5) Un act delegat adoptat în conformitate cu articolul 12 alineatul (8) şi cu articolul 43 alineatul (8) intră în vigoare numai în cazul în care nici Parlamentul European şi nici Consiliul nu au formulat obiecţiuni în termen de trei luni de la notificarea acestuia Parlamentului European şi Consiliului, sau în cazul în care, înainte de expirarea termenului respectiv, Parlamentul European şi Consiliul au informat Comisia că nu vor formula obiecţiuni. Respectivul termen se prelungeşte cu trei luni la iniţiativa Parlamentului European sau a Consiliului.

Articolul 93

Procedura comitetului

(1) Comisia este asistată de un comitet. Comitetul respectiv este un comitet în înţelesul 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
Dispoziţii 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 protecţia persoanelor în ceea ce priveşte prelucrarea datelor cu caracter personal instituit prin articolul 29 din Directiva 95/46/CE se interpretează ca trimiteri la Comitetul european pentru protecţia datelor instituit prin prezentul regulament.

Articolul 95
Relaţia cu Directiva 2002/58/CE
Prezentul regulament nu impune obligaţii suplimentare pentru persoanele fizice sau juridice în ceea ce priveşte prelucrarea în legătură cu furnizarea de servicii de comunicaţii electronice destinate publicului în reţelele de comunicaţii publice din Uniune, cu privire la aspectele pentru care acestora le revin obligaţii specifice cu acelaşi obiectiv prevăzut în Directiva 2002/58/CE.

Articolul 96
Relaţia cu acordurile încheiate anterior
Acordurile internaţionale care implică transferul de date cu caracter personal către ţări terţe sau organizaţii internaţionale, care au fost încheiate de statele membre înainte de 24 mai 2016 şi 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 şi, ulterior, la fiecare patru ani, Comisia transmite Parlamentului European şi Consiliului un raport privind evaluarea şi revizuirea
prezentului regulament. Rapoartele sunt făcute publice.
(2) În contextul evaluărilor şi revizuirilor menţionate la alineatul (1), Comisia examinează în special aplicarea şi funcţionarea:
(a) capitolului V privind transferul datelor cu caracter personal către ţări terţe sau organizaţii internaţionale, având în vedere în special deciziile adoptate în temeiul articolului 45 alineatul (3) din prezentul regulament şi deciziile adoptate în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE;
(b) capitolul VII privind cooperarea şi coerenţa.
(3) În scopul alineatului (1), Comisia poate solicita informaţii de la statele membre şi de la autorităţile de supraveghere.
(4) La efectuarea evaluărilor şi a revizuirilor menţionate la alineatele (1) şi (2), Comisia ia în considerare poziţiile şi constatările Parlamentului European, ale Consiliului, precum şi ale altor organisme sau surse relevante.
(5) Comisia transmite, dacă este necesar, propuneri corespunzătoare de modificare a prezentului regulament, în special ţinând seama de evoluţiile din domeniul tehnologiei informaţiei şi având în vedere progresele societăţii informaţionale.

GDPR

Articolul 98

Revizuirea altor acte juridice ale Uniunii în materie de protecţie a datelor Dacă este cazul, Comisia prezintă propuneri legislative în vederea modificării altor acte juridice ale Uniunii privind protecţia datelor cu caracter personal, în vederea asigurării unei protecţii uniforme şi consecvente a persoanelor fizice în ceea ce priveşte prelucrarea. Acest lucru priveşte în special normele referitoare la protecţia persoanelor fizice în ceea ce priveşte prelucrarea de către instituţiile, organismele, oficiile şi agenţiile Uniunii, precum şi normele referitoare la libera circulaţie a acestor date.

Articolul 99

Intrare în vigoare şi 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 şi se aplică direct în toate statele membre.

Adoptat la Bruxelles, 27 aprilie 2016.
Pentru Parlamentul European Preşedintele
M. SCHULZ

Pentru Consiliu Preşedintele
J.A. HENNIS-PLASSCHAERT

GDPR