

Jurnalul Oficial al Uniunii Europene

L 119



Ediția în limba română

Legislație

Anul 59

4 mai 2016

Cuprins

I Acte legislative

REGULAMENTE

- ★ **Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) ⁽¹⁾** 1

DIRECTIVE

- ★ **Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului** 89
- ★ **Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave** 132

⁽¹⁾ Text cu relevanță pentru SEE

RO

Actele ale căror titluri sunt tipărite cu caractere drepte sunt acte de gestionare curentă adoptate în cadrul politicii agricole și care au, în general, o perioadă de valabilitate limitată.

Titlurile celorlalte acte sunt tipărite cu caractere aldine și sunt precedate de un asterisc.

I

(Acte legislative)

REGULAMENTE

REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 27 aprilie 2016

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

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European ⁽¹⁾,

având în vedere avizul Comitetului Regiunilor ⁽²⁾,

hotărând în conformitate cu procedura legislativă ordinară ⁽³⁾,

întrucât:

- (1) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene („carta”) și articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc.
- (2) Principiile și normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal ar trebui, indiferent de cetățenia sau de locul de reședință al persoanelor fizice, să respecte drepturile și libertățile fundamentale ale acestora, în special dreptul la protecția datelor cu caracter personal. Prezentul regulament urmărește să contribuie la realizarea unui spațiu de libertate, securitate și justiție și a unei uniuni economice, la progresul economic și social, la consolidarea și convergența economiilor în cadrul pieței interne și la bunăstarea persoanelor fizice.
- (3) Directiva 95/46/CE a Parlamentului European și a Consiliului ⁽⁴⁾ vizează armonizarea nivelului de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește activitățile de prelucrare și asigurarea liberei circulații a datelor cu caracter personal între statele membre.

⁽¹⁾ JO C 229, 31.7.2012, p. 90.

⁽²⁾ JO C 391, 18.12.2012, p.127.

⁽³⁾ Poziția Parlamentului European din 12 martie 2014 (nepublicată încă în Jurnalul Oficial) și Poziția în primă lectură a Consiliului din 8 aprilie 2016 (nepublicată încă în Jurnalul Oficial). Poziția Parlamentului European din 14 aprilie 2016.

⁽⁴⁾ Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO L 281, 23.11.1995, p. 31).

- (4) Prelucrarea datelor cu caracter personal ar trebui să fie în serviciul cetățenilor. Dreptul la protecția datelor cu caracter personal nu este un drept absolut; acesta trebuie luat în considerare în raport cu funcția pe care o îndeplinește în societate și echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității. Prezentul regulament respectă toate drepturile fundamentale și libertățile și principiile recunoscute în cartă astfel cum sunt consacrate în tratate, în special respectarea vieții private și de familie, a reședinței și a comunicațiilor, a protecției datelor cu caracter personal, a libertății de gândire, de conștiință și de religie, a libertății de exprimare și de informare, a libertății de a desfășura o activitate comercială, dreptul la o cale de atac eficientă și la un proces echitabil, precum și diversitatea culturală, religioasă și lingvistică.
- (5) Integrarea economică și socială care rezultă din funcționarea pieței interne a condus la o creștere substanțială a fluxurilor transfrontaliere de date cu caracter personal. Schimbul de date cu caracter personal între actori publici și privați, inclusiv persoane fizice, asociații și întreprinderi, s-a intensificat în întreaga Uniune. Conform dreptului Uniunii, autoritățile naționale din statele membre sunt chemate să coopereze și să facă schimb de date cu caracter personal pentru a putea să își îndeplinească atribuțiile sau să execute sarcini în numele unei autorități dintr-un alt stat membru.
- (6) Evoluțiile tehnologice rapide și globalizarea au generat noi provocări pentru protecția datelor cu caracter personal. Amploarea colectării și a schimbului de date cu caracter personal a crescut în mod semnificativ. Tehnologia permite atât societăților private, cât și autorităților publice să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităților lor. Din ce în ce mai mult, persoanele fizice fac publice la nivel mondial informații cu caracter personal. Tehnologia a transformat deopotrivă economia și viața socială și ar trebui să faciliteze în continuare libera circulație a datelor cu caracter personal în cadrul Uniunii și transferul către țări terțe și organizații internaționale, asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal.
- (7) Aceste evoluții impun un cadru solid și mai coerent în materie de protecție a datelor în Uniune, însoțit de o aplicare riguroasă a normelor, luând în considerare importanța creării unui climat de încredere care va permite economiei digitale să se dezvolte pe piața internă. Persoanele fizice ar trebui să aibă control asupra propriilor date cu caracter personal, iar securitatea juridică și practică pentru persoane fizice, operatori economici și autorități publice ar trebui să fie consolidată.
- (8) În cazul în care prezentul regulament prevede specificări sau restricționări ale normelor sale de către dreptul intern, statele membre pot, în măsura în care acest lucru este necesar pentru coerență și pentru a asigura înțelegerea dispozițiilor naționale de către persoanele cărora li se aplică acestea, să încorporeze elemente din prezentul regulament în dreptul lor intern.
- (9) Obiectivele și principiile Directivei 95/46/CE rămân solide, dar aceasta nu a prevenit fragmentarea modului în care protecția datelor este pusă în aplicare în Uniune, insecuritatea juridică sau percepția publică larg răspândită conform căreia există riscuri semnificative pentru protecția persoanelor fizice, în special în legătură cu activitatea online. Diferențele dintre nivelurile de protecție a drepturilor și libertăților persoanelor fizice, în special a dreptului la protecția datelor cu caracter personal, în ceea ce privește prelucrarea datelor cu caracter personal din statele membre pot împiedica libera circulație a datelor cu caracter personal în întreaga Uniune. Aceste diferențe pot constitui, prin urmare, un obstacol în desfășurarea de activități economice la nivelul Uniunii, pot denatura concurența și pot împiedica autoritățile să îndeplinească responsabilitățile care le revin în temeiul dreptului Uniunii. Această diferență între nivelurile de protecție este cauzată de existența unor deosebiri în ceea ce privește transpunerea și aplicarea Directivei 95/46/CE.
- (10) Pentru a se asigura un nivel consecvent și ridicat de protecție a persoanelor fizice și pentru a se îndepărta obstacolele din calea circulației datelor cu caracter personal în cadrul Uniunii, nivelul protecției drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea unor astfel de date ar trebui să fie echivalent în toate statele membre. Aplicarea consecventă și omogenă a normelor în materie de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ar trebui să fie asigurată în întreaga Uniune. În ceea ce privește prelucrarea datelor cu caracter personal în vederea respectării unei obligații legale, a îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul, statelor membre ar trebui să li se permită să mențină sau să introducă dispoziții de drept intern care să clarifice într-o mai mare măsură aplicarea normelor prezentului regulament. În coroborare cu legislația generală și orizontală privind protecția datelor, prin care este pusă în aplicare Directiva 95/46/CE, statele membre au mai multe legi sectoriale specifice în domenii care necesită dispoziții mai precise. Prezentul regulament oferă, de asemenea, statelor membre o marjă de manevră în specificarea normelor sale, inclusiv în ceea ce privește prelucrarea categoriilor speciale de date cu caracter personal („date sensibile”). În acest sens, prezentul regulament nu exclude dreptul statelor membre care stabilește circumstanțele aferente unor situații de prelucrare specifice, inclusiv stabilirea cu o mai mare precizie a condițiilor în care prelucrarea datelor cu caracter personal este legală.

- (11) Protecția efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea și stabilirea în detaliu a drepturilor persoanelor vizate și a obligațiilor celor care prelucrează și decid prelucrarea datelor cu caracter personal, ci și competențe echivalente pentru monitorizarea și asigurarea conformității cu normele de protecție a datelor cu caracter personal și sancțiuni echivalente pentru infracțiuni în statele membre.
- (12) Articolul 16 alineatul (2) din TFUE mandatează Parlamentul European și Consiliul să stabilească normele privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal, precum și normele privind libera circulație a acestor date.
- (13) În vederea asigurării unui nivel uniform de protecție pentru persoanele fizice în întreaga Uniune și a preîntâmpinării discrepanțelor care împiedică libera circulație a datelor în cadrul pieței interne, este necesar un regulament în scopul de a furniza securitate juridică și transparență pentru operatorii economici, inclusiv microîntreprinderi și întreprinderi mici și mijlocii, precum și de a oferi persoanelor fizice în toate statele membre același nivel de drepturi, obligații și responsabilități opozabile din punct de vedere juridic pentru operatori și persoanele împuternicite de aceștia, pentru a se asigura o monitorizare coerentă a prelucrării datelor cu caracter personal, sancțiuni echivalente în toate statele membre, precum și cooperarea eficace a autorităților de supraveghere ale diferitelor state membre. Pentru buna funcționare a pieței interne este necesar ca libera circulație a datelor cu caracter personal în cadrul Uniunii să nu fie restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal. Pentru a se lua în considerare situația specifică a microîntreprinderilor și a întreprinderilor mici și mijlocii, prezentul regulament include o derogare pentru organizațiile cu mai puțin de 250 de angajați în ceea ce privește păstrarea evidențelor. În plus, instituțiile și organele Uniunii și statele membre și autoritățile lor de supraveghere sunt încurajate să ia în considerare necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii în aplicarea prezentului regulament. Noțiunea de microîntreprinderi și de întreprinderi mici și mijlocii ar trebui să se bazeze pe articolul 2 din anexa la Recomandarea 2003/361/CE a Comisiei ⁽¹⁾.
- (14) Protecția conferită de prezentul regulament ar trebui să vizeze persoanele fizice, indiferent de cetățenia sau de locul de reședință al acestora, în ceea ce privește prelucrarea datelor cu caracter personal ale acestora. Prezentul regulament nu se aplică prelucrării datelor cu caracter personal care privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și datele de contact ale persoanei juridice.
- (15) Pentru a preveni apariția unui risc major de eludare, protecția persoanelor fizice ar trebui să fie neutră din punct de vedere tehnologic și să nu depindă de tehnologiile utilizate. Protecția persoanelor fizice ar trebui să se aplice prelucrării datelor cu caracter personal prin mijloace automatizate, precum și prelucrării manuale, în cazul în care datele cu caracter personal sunt cuprinse sau destinate să fie cuprinse într-un sistem de evidență. Dosarele sau seturile de dosare, precum și copertele acestora, care nu sunt structurate în conformitate cu criteriile specificului ar trebui să intre în domeniul de aplicare al prezentului regulament.
- (16) Prezentul regulament nu se aplică chestiunilor de protecție a drepturilor și libertăților fundamentale sau la libera circulație a datelor cu caracter personal referitoare la activități care nu intră în domeniul de aplicare al dreptului Uniunii, de exemplu activitățile privind securitatea națională. Prezentul regulament nu se aplică prelucrării datelor cu caracter personal de către statele membre atunci când acestea desfășoară activități legate de politica externă și de securitatea comună a Uniunii.
- (17) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ⁽²⁾ se aplică prelucrării de date cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii. Regulamentul (CE) nr. 45/2001 și alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal ar trebui adaptate la principiile și normele stabilite în prezentul regulament și aplicate în conformitate cu prezentul regulament. În vederea asigurării unui cadru solid și coerent în materie de protecție a datelor în Uniune, ar trebui ca după adoptarea prezentului regulament să se aducă Regulamentului (CE) nr. 45/2001 adaptările necesare, astfel încât acestea să poată fi aplicate odată cu prezentul regulament.
- (18) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice și care, prin urmare, nu are legătură cu o activitate profesională sau

⁽¹⁾ Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii [C(2003) 1422] (JO L 124, 20.5.2003, p. 36).

⁽²⁾ Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

comercială. Activitățile personale sau domestice ar putea include corespondența și repertoriul de adrese sau activitățile din cadrul rețelelor sociale și activitățile online desfășurate în contextul respectivelor activități. Cu toate acestea, prezentul regulament se aplică operatorilor sau persoanelor împuternicite de operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activități personale sau domestice.

- (19) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, precum și libera circulație a acestor date, face obiectul unui act juridic specific al Uniunii. Prin urmare, prezentul regulament nu ar trebui să se aplice activităților de prelucrare în aceste scopuri. Cu toate acestea, datele cu caracter personal prelucrate de către autoritățile publice în temeiul prezentului regulament, atunci când sunt utilizate în aceste scopuri, ar trebui să fie reglementate printr-un act juridic mai specific al Uniunii, și anume Directiva (UE) 2016/680 a Parlamentului European și a Consiliului ⁽¹⁾. Statele membre pot încredința autorităților competente în sensul Directivei (UE) 2016/680 sarcini care nu sunt neapărat îndeplinite în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, astfel încât prelucrarea datelor cu caracter personal pentru alte scopuri, în măsura în care se încadrează în domeniul de aplicare al dreptului Uniunii, să intre în domeniul de aplicare al prezentului regulament.

În ceea ce privește prelucrarea datelor cu caracter personal de către aceste autorități competente în scopuri care intră în domeniul de aplicare al prezentului regulament, statele membre ar trebui să poată menține sau introduce dispoziții mai detaliate pentru a adapta aplicarea normelor din prezentul regulament. Aceste dispoziții pot stabili mai precis cerințe specifice pentru prelucrarea datelor cu caracter personal de către respectivele autorități competente în aceste alte scopuri, ținând seama de structura constituțională, organizatorică și administrativă a statului membru în cauză. Atunci când prelucrarea de date cu caracter personal de către organisme private face obiectul prezentului regulament, prezentul regulament ar trebui să prevadă posibilitatea ca statele membre, în anumite condiții, să impună prin lege restricții asupra anumitor obligații și drepturi, în cazul în care asemenea restricții constituie o măsură necesară și proporțională într-o societate democratică în scopul garantării unor interese specifice importante, printre care se numără siguranța publică și prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor sau executarea pedepselor, inclusiv protejarea împotriva amenințărilor la adresa siguranței publice și prevenirea acestora. Acest lucru este relevant, de exemplu, în cadrul combaterii spălării de bani sau al activităților laboratoarelor criminalistice.

- (20) Deși prezentul regulament se aplică, *inter alia*, activităților instanțelor și ale altor autorități judiciare, dreptul Uniunii sau al statelor membre ar putea să precizeze operațiunile și procedurile de prelucrare în ceea ce privește prelucrarea datelor cu caracter personal de către instanțe și alte autorități judiciare. Prelucrarea datelor cu caracter personal nu ar trebui să fie de competența autorităților de supraveghere în cazul în care instanțele își exercită atribuțiile judiciare, în scopul garantării independenței sistemului judiciar în îndeplinirea sarcinilor sale judiciare, inclusiv în luarea deciziilor. Supravegherea unor astfel de operațiuni de prelucrare a datelor ar trebui să poată fi încredințată unor organisme specifice din cadrul sistemului judiciar al statului membru, care ar trebui să asigure în special respectarea normelor prevăzute de prezentul regulament, să sensibilizeze membrii sistemului judiciar cu privire la obligațiile care le revin în temeiul prezentului regulament și să trateze plângerile în legătură cu astfel de operațiuni de prelucrare a datelor.
- (21) Prezentul regulament nu aduce atingere aplicării Directivei 2000/31/CE a Parlamentului European și a Consiliului ⁽²⁾, în special normelor privind răspunderea furnizorilor intermediari de servicii prevăzute la articolele 12-15 din directiva menționată. Respectiva directivă își propune să contribuie la buna funcționare a pieței interne, prin asigurarea liberei circulații a serviciilor societății informaționale între statele membre.
- (22) Orice prelucrare a datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune ar trebui efectuată în conformitate cu prezentul regulament, indiferent dacă procesul de prelucrare în sine are loc sau nu în cadrul Uniunii. Sediul implică exercitarea efectivă și reală a unei activități în cadrul unor înțelegeri stabile. Forma juridică a unor astfel de înțelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință.

⁽¹⁾ Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (a se vedea pagina 89 din prezentul Jurnal Oficial).

⁽²⁾ Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (directiva privind comerțul electronic) (JO L 178, 17.7.2000, p. 1).

- (23) Pentru a se asigura că persoanele fizice nu sunt lipsite de protecția la care au dreptul în temeiul prezentului regulament, prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Uniunii de către un operator sau o persoană împuternicită de acesta care nu își are sediul în Uniune ar trebui să facă obiectul prezentului regulament în cazul în care activitățile de prelucrare au legătură cu oferirea de bunuri sau servicii unor astfel de persoane vizate, indiferent dacă acestea sunt sau nu legate de o plată. Pentru a determina dacă un astfel de operator sau o astfel de persoană împuternicită de operator oferă bunuri sau servicii unor persoane vizate care se află pe teritoriul Uniunii, ar trebui să se stabilească dacă reiese că operatorul sau persoana împuternicită de operator intenționează să furnizeze servicii persoanelor vizate din unul sau mai multe state membre din Uniune. Întrucât simplul fapt că există acces la un site al operatorului, al persoanei împuternicite de operator sau al unui intermediar în Uniune, că este disponibilă o adresă de e-mail și alte date de contact sau că este utilizată o limbă folosită în general în țara terță în care operatorul își are sediul este insuficient pentru a confirma o astfel de intenție, factori precum utilizarea unei limbi sau a unei monede utilizate în general în unul sau mai multe state membre cu posibilitatea de a comanda bunuri și servicii în respectiva limbă sau menționarea unor clienți sau utilizatori care se află pe teritoriul Uniunii pot conduce la concluzia că operatorul intenționează să ofere bunuri sau servicii unor persoane vizate în Uniune.
- (24) Prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Uniunii de către un operator sau o persoană împuternicită de acesta care nu își are sediul în Uniune ar trebui, de asemenea, să facă obiectul prezentului regulament în cazul în care este legată de monitorizarea comportamentului unor astfel de persoane vizate, în măsura în care acest comportament se manifestă pe teritoriul Uniunii. Pentru a se determina dacă o activitate de prelucrare poate fi considerată ca „monitorizare a comportamentului” persoanelor vizate, ar trebui să se stabilească dacă persoanele fizice sunt urmărite pe internet, inclusiv posibila utilizare ulterioară a unor tehnici de prelucrare a datelor cu caracter personal care constau în crearea unui profil al unei persoane fizice, în special în scopul de a lua decizii cu privire la aceasta sau de a analiza sau de a face previziuni referitoare la preferințele personale, comportamentele și atitudinile acesteia.
- (25) În cazul în care dreptul unui stat membru se aplică în temeiul dreptului internațional public, prezentul regulament ar trebui să se aplice, de asemenea, unui operator care nu este stabilit în Uniune, ci, de exemplu, într-o misiune diplomatică sau într-un oficiu consular al unui stat membru.
- (26) Principiile protecției datelor ar trebui să se aplice oricărei informații referitoare la o persoană fizică identificată sau identificabilă. Datele cu caracter personal care au fost supuse pseudonimizării, care ar putea fi atribuite unei persoane fizice prin utilizarea de informații suplimentare, ar trebui considerate informații referitoare la o persoană fizică identificabilă. Pentru a se determina dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană, în scopul identificării, în mod direct sau indirect, a persoanei fizice respective. Pentru a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace pentru identificarea persoanei fizice, ar trebui luați în considerare toți factorii obiectivi, precum costurile și intervalul de timp necesare pentru identificare, ținându-se seama atât de tehnologia disponibilă la momentul prelucrării, cât și de dezvoltarea tehnologică. Principiile protecției datelor ar trebui, prin urmare, să nu se aplice informațiilor anonime, adică informațiilor care nu sunt legate de o persoană fizică identificată sau identificabilă sau datelor cu caracter personal care sunt anonimizate astfel încât persoana vizată nu este sau nu mai este identificabilă. Prin urmare, prezentul regulament nu se aplică prelucrării unor astfel de informații anonime, inclusiv în cazul în care acestea sunt utilizate în scopuri statistice sau de cercetare.
- (27) Prezentul regulament nu se aplică datelor cu caracter personal referitoare la persoane decedate. Statele membre pot să prevadă norme privind prelucrarea datelor cu caracter personal referitoare la persoane decedate.
- (28) Aplicarea pseudonimizării datelor cu caracter personal poate reduce riscurile pentru persoanele vizate și poate ajuta operatorii și persoanele împuternicite de aceștia să își îndeplinească obligațiile de protecție a datelor. Introducerea explicită a conceptului de „pseudonimizare” în prezentul regulament nu este destinată să împiedice alte eventuale măsuri de protecție a datelor.
- (29) Pentru a crea stimulente pentru aplicarea pseudonimizării atunci când sunt prelucrate date cu caracter personal, ar trebui să fie posibile măsuri de pseudonimizare, permițând în același timp analiza generală, în cadrul aceluiași operator atunci când operatorul a luat măsurile tehnice și organizatorice necesare pentru a se asigura că prezentul regulament este pus în aplicare în ceea ce privește respectiva prelucrare a datelor și că informațiile suplimentare pentru atribuirea datelor cu caracter personal unei anumite persoane vizate sunt păstrate separat. Operatorul care prelucrează datele cu caracter personal ar trebui să indice persoanele autorizate din cadrul aceluiași operator.

- (30) Persoanele fizice pot fi asociate cu identificadorii online furnizați de dispozitivele, aplicațiile, instrumentele și protocoalele lor, cum ar fi adresele IP, identificadorii cookie sau alți identifikatori precum etichetele de identificare prin frecvențe radio. Aceștia pot lăsa urme care, în special atunci când sunt combinate cu identifikatori unici și alte informații primite de servere, pot fi utilizate pentru crearea de profiluri ale persoanelor fizice și pentru identificarea lor.
- (31) Autoritățile publice cărora le sunt divulgate date cu caracter personal în conformitate cu o obligație legală în vederea exercitării funcției lor oficiale, cum ar fi autoritățile fiscale și vamale, unitățile de investigare financiară, autoritățile administrative independente sau autoritățile piețelor financiare responsabile de reglementarea și supravegherea piețelor titlurilor de valoare, nu ar trebui să fie considerate destinatari în cazul în care primesc date cu caracter personal care sunt necesare pentru efectuarea unei anumite anchete de interes general, în conformitate cu dreptul Uniunii sau cel al statelor membre. Cererile de divulgare trimise de autoritățile publice ar trebui să fie întotdeauna prezentate în scris, motivate și ocazionale și nu ar trebui să se refere la un sistem de evidență în totalitate sau să conducă la interconectarea sistemelor de evidență. Prelucrarea datelor cu caracter personal de către autoritățile publice respective ar trebui să respecte normele aplicabile în materie de protecție a datelor în conformitate cu scopurile prelucrării.
- (32) Consimțământul ar trebui acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declarație făcută în scris, inclusiv în format electronic, sau verbal. Acesta ar putea include bifarea unei căsuțe atunci când persoana vizitează un site, alegerea parametrilor tehnici pentru serviciile societății informaționale sau orice altă declarație sau acțiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu ar trebui să constituie un consimțământ. Consimțământul ar trebui să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul ar trebui dat pentru toate scopurile prelucrării. În cazul în care consimțământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară și concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimțământul.
- (33) Adesea nu este posibil, în momentul colectării datelor cu caracter personal, să se identifice pe deplin scopul prelucrării datelor în scopuri de cercetare științifică. Din acest motiv, persoanelor vizate ar trebui să li se permită să își exprime consimțământul pentru anumite domenii ale cercetării științifice atunci când sunt respectate standardele etice recunoscute pentru cercetarea științifică. Persoanele vizate ar trebui să aibă posibilitatea de a-și exprima consimțământul doar pentru anumite domenii de cercetare sau părți ale proiectelor de cercetare în măsura permisă de scopul preconizat.
- (34) Datele genetice ar trebui definite drept date cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care rezultă în urma unei analize a unei mostre de material biologic al persoanei fizice în cauză, în special a unei analize cromozomiale, a unei analize a acidului dezoxiribonucleic (ADN) sau a acidului ribonucleic (ARN) sau a unei analize a oricărui alt element ce permite obținerea unor informații echivalente.
- (35) Datele cu caracter personal privind sănătatea ar trebui să includă toate datele având legătură cu starea de sănătate a persoanei vizate care dezvăluie informații despre starea de sănătate fizică sau mentală trecută, prezentă sau viitoare a persoanei vizate. Acestea includ informații despre persoana fizică colectate în cadrul înscrierii acesteia la serviciile de asistență medicală sau în cadrul acordării serviciilor respective persoanei fizice în cauză, astfel cum sunt menționate în Directiva 2011/24/UE a Parlamentului European și a Consiliului ⁽¹⁾; un număr, un simbol sau un semn distinctiv atribuit unei persoane fizice pentru identificarea singulară a acesteia în scopuri medicale; informații rezultate din testarea sau examinarea unei părți a corpului sau a unei substanțe corporale, inclusiv din date genetice și eșantioane de material biologic; precum și orice informații privind, de exemplu, o boală, un handicap, un risc de îmbolnăvire, istoricul medical, tratamentul clinic sau starea fiziologică sau biomedicală a persoanei vizate, indiferent de sursa acestora, ca de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro.
- (36) Sediul principal al unui operator în Uniune ar trebui să fie locul în care se află administrația centrală a acestuia în Uniune, cu excepția cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului în Uniune. În acest caz, acesta din urmă ar trebui considerat drept

⁽¹⁾ Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere (JO L 88, 4.4.2011, p. 45).

sediul principal. Sediul principal al unui operator în Uniune ar trebui să fie determinat conform unor criterii obiective și ar trebui să implice exercitarea efectivă și reală a unor activități de gestionare care să determine principalele decizii cu privire la scopurile și mijloacele de prelucrare în cadrul unor înțelegeri stabile. Acest criteriu nu ar trebui să depindă de realizarea prelucrării datelor cu caracter personal în locul respectiv. Prezența și utilizarea mijloacelor tehnice și a tehnologiilor de prelucrare a datelor cu caracter personal sau activitățile de prelucrare nu constituie un sediu principal și, prin urmare, nu sunt criteriul determinant în acest sens. Sediul principal al persoanei împuternicite de operator ar trebui să fie locul în care se află administrația centrală a acestuia în Uniune sau, în cazul în care nu are o administrație centrală în Uniune, locul în care se desfășoară principalele activități de prelucrare în Uniune. În cazurile care implică atât operatorul, cât și persoana împuternicită de operator, autoritatea de supraveghere principală competentă ar trebui să rămână autoritatea de supraveghere a statului membru în care operatorul își are sediul principal, dar autoritatea de supraveghere a persoanei împuternicite de operator ar trebui considerată ca fiind o autoritate de supraveghere vizată și acea autoritate de supraveghere ar trebui să participe la procedura de cooperare prevăzută de prezentul regulament. În orice caz, autoritățile de supraveghere ale statului membru sau ale statelor membre în care persoana împuternicită de operator are unul sau mai multe sedii nu ar trebui considerate ca fiind autorități de supraveghere vizate în cazul în care proiectul de decizie nu se referă decât la operator. În cazul în care prelucrarea este efectuată de un grup de întreprinderi, sediul principal al întreprinderii care exercită controlul ar trebui considerat drept sediul principal al grupului de întreprinderi, cu excepția cazului în care scopurile și mijloacele aferente prelucrării sunt stabilite de o altă întreprindere.

- (37) Un grup de întreprinderi ar trebui să cuprindă o întreprindere care exercită controlul și întreprinderile controlate de aceasta, în cadrul căruia întreprinderea care exercită controlul ar trebui să fie întreprinderea care poate exercita o influență dominantă asupra celorlalte întreprinderi, de exemplu în temeiul proprietății, al participării financiare sau al regulilor care o reglementează sau al competenței de a pune în aplicare norme în materie de protecție a datelor cu caracter personal. O întreprindere care controlează prelucrarea datelor cu caracter personal în întreprinderile sale afiliate ar trebui considerată, împreună cu acestea din urmă, drept „grup de întreprinderi”.
- (38) Copiii au nevoie de o protecție specifică a datelor lor cu caracter personal, întrucât pot fi mai puțin conștienți de riscurile, consecințele, garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal. Această protecție specifică ar trebui să se aplice în special utilizării datelor cu caracter personal ale copiilor în scopuri de marketing sau pentru crearea de profiluri de personalitate sau de utilizator și la colectarea datelor cu caracter personal privind copiii în momentul utilizării serviciilor oferite direct copiilor. Consimțământul titularului răspunderii părintești nu ar trebui să fie necesar în contextul serviciilor de prevenire sau consiliere oferite direct copiilor.
- (39) Orice prelucrare de date cu caracter personal ar trebui să fie legală și echitabilă. Ar trebui să fie transparent pentru persoanele fizice că sunt colectate, utilizate, consultate sau prelucrate în alt mod datele cu caracter personal care le privesc și în ce măsură datele cu caracter personal sunt sau vor fi prelucrate. Principiul transparenței prevede că orice informații și comunicări referitoare la prelucrarea respectivelor date cu caracter personal sunt ușor accesibile și ușor de înțeles și că se utilizează un limbaj simplu și clar. Acest principiu se referă în special la informarea persoanelor vizate privind identitatea operatorului și scopurile prelucrării, precum și la oferirea de informații suplimentare, pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoanele fizice vizate și dreptul acestora de a li se confirma și comunica datele cu caracter personal care le privesc care sunt prelucrate. Persoanele fizice ar trebui informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal și cu privire la modul în care să își exercite drepturile în legătură cu prelucrarea. În special, scopurile specifice în care datele cu caracter personal sunt prelucrate ar trebui să fie explicite și legitime și să fie determinate la momentul colectării datelor respective. Datele cu caracter personal ar trebui să fie adecvate, relevante și limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Aceasta necesită, în special, asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum. Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace. În vederea asigurării faptului că datele cu caracter personal nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ștergere sau revizuirea periodică. Ar trebui să fie luate toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau șterse. Datele cu caracter personal ar trebui prelucrate într-un mod care să asigure în mod adecvat securitatea și confidențialitatea acestora, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizată a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare.
- (40) Pentru ca prelucrarea datelor cu caracter personal să fie legală, aceasta ar trebui efectuată pe baza consimțământului persoanei vizate sau în temeiul unui alt motiv legitim, prevăzut de lege, fie în prezentul regulament, fie

în alt act din dreptul Uniunii sau din dreptul intern, după cum se prevede în prezentul regulament, inclusiv necesitatea respectării obligațiilor legale la care este supus operatorul sau necesitatea de a executa un contract la care persoana vizată este parte sau pentru a parcurge etapele premergătoare încheierii unui contract, la solicitarea persoanei vizate.

- (41) Ori de câte ori prezentul regulament face trimitere la un temei juridic sau la o măsură legislativă, aceasta nu necesită neapărat un act legislativ adoptat de către un parlament, fără a aduce atingere cerințelor care decurg din ordinea constituțională a statului membru în cauză. Cu toate acestea, un astfel de temei juridic sau o astfel de măsură legislativă ar trebui să fie clară și precisă, iar aplicarea acesteia ar trebui să fie previzibilă pentru persoanele vizate de aceasta, în conformitate cu jurisprudența Curții de Justiție a Uniunii Europene („Curtea de Justiție”) și a Curții Europene a Drepturilor Omului.
- (42) În cazul în care prelucrarea se bazează pe consimțământul persoanei vizate, operatorul ar trebui să fie în măsură să demonstreze faptul că persoana vizată și-a dat consimțământul pentru operațiunea de prelucrare. În special, în contextul unei declarații scrise cu privire la un alt aspect, garanțiile ar trebui să asigure că persoana vizată este conștientă de faptul că și-a dat consimțământul și în ce măsură a făcut acest lucru. În conformitate cu Directiva 93/13/CEE a Consiliului (¹), ar trebui furnizată o declarație de consimțământ formulată în prealabil de către operator, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, iar această declarație nu ar trebui să conțină clauze abuzive. Pentru ca acordarea consimțământului să fie în cunoștință de cauză, persoana vizată ar trebui să fie la curent cel puțin cu identitatea operatorului și cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal. Consimțământul nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată.
- (43) Pentru a garanta faptul că a fost acordat în mod liber, consimțământul nu ar trebui să constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal în cazul particular în care există un dezechilibru evident între persoana vizată și operator, în special în cazul în care operatorul este o autoritate publică, iar acest lucru face improbabilă acordarea consimțământului în mod liber în toate circumstanțele aferente respectivei situații particulare. Consimțământul este considerat a nu fi acordat în mod liber în cazul în care aceasta nu permite să se acorde consimțământul separat pentru diferitele operațiuni de prelucrare a datelor cu caracter personal, deși acest lucru este adecvat în cazul particular, sau dacă executarea unui contract, inclusiv furnizarea unui serviciu, este condiționată de consimțământ, în ciuda faptului că consimțământul în cauză nu este necesar pentru executarea contractului.
- (44) Prelucrarea ar trebui să fie considerată legală în cazul în care este necesară în cadrul unui contract sau în vederea încheierii unui contract.
- (45) În cazul în care prelucrarea este efectuată în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice, prelucrarea ar trebui să aibă un temei în dreptul Uniunii sau în dreptul intern. Prezentul regulament nu impune existența unei legi specifice pentru fiecare prelucrare în parte. Poate fi suficientă o singură lege drept temei pentru mai multe operațiuni de prelucrare efectuate în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice. De asemenea, ar trebui ca scopul prelucrării să fie stabilit în dreptul Uniunii sau în dreptul intern. Mai mult decât atât, dreptul respectiv ar putea să specifice condițiile generale ale prezentului regulament care reglementează legalitatea prelucrării datelor cu caracter personal, să determine specificațiile pentru stabilirea operatorului, a tipului de date cu caracter personal care fac obiectul prelucrării, a persoanelor vizate, a entităților cărora le pot fi divulgate datele cu caracter personal, a limitărilor în funcție de scop, a perioadei de stocare și a altor măsuri pentru a garanta o prelucrare legală și echitabilă. De asemenea, ar trebui să se stabilească în dreptul Uniunii sau în dreptul intern dacă operatorul care îndeplinește o sarcină care servește unui interes public sau care face parte din exercitarea autorității publice ar trebui să fie o autoritate publică sau o altă persoană fizică sau juridică guvernată de dreptul public sau, atunci când motive de interes public justifică acest lucru, inclusiv în scopuri medicale, precum sănătatea publică și protecția socială, precum și gestionarea serviciilor de asistență medicală, de dreptul privat, cum ar fi o asociație profesională.
- (46) Prelucrarea datelor cu caracter personal ar trebui, de asemenea, să fie considerată legală în cazul în care este necesară în scopul asigurării protecției unui interes care este esențial pentru viața persoanei vizate sau pentru

(¹) Directiva 93/13/CEE a Consiliului din 5 aprilie 1993 privind clauzele abuzive în contractele încheiate cu consumatorii (JO L 95, 21.4.1993, p. 29).

viața unei alte persoane fizice. Prelucrarea datelor cu caracter personal care are drept temei interesele vitale ale unei alte persoane fizice ar trebui efectuată numai în cazul în care prelucrarea nu se poate baza în mod evident pe un alt temei juridic. Unele tipuri de prelucrare pot servi atât unor motive importante de interes public, cât și intereselor vitale ale persoanei vizate, de exemplu în cazul în care prelucrarea este necesară în scopuri umanitare, inclusiv în vederea monitorizării unei epidemii și a răspândirii acesteia sau în situații de urgențe umanitare, în special în situații de dezastre naturale sau provocate de om.

- (47) Interesele legitime ale unui operator, inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terțe părți, pot constitui un temei juridic pentru prelucrare, cu condiția să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate, luând în considerare așteptările rezonabile ale persoanelor vizate bazate pe relația acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relație relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia. În orice caz, existența unui interes legitim ar necesita o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată poate preconiza în mod rezonabil, în momentul și în contextul colectării datelor cu caracter personal, posibilitatea prelucrării în acest scop. Interesele și drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date atunci când datele cu caracter personal sunt prelucrate în circumstanțe în care persoanele vizate nu preconizează în mod rezonabil o prelucrare ulterioară. Întrucât legiuitorul trebuie să furnizeze temeiul juridic pentru prelucrarea datelor cu caracter personal de către autoritățile publice, temeiul juridic respectiv nu ar trebui să se aplice prelucrării de către autoritățile publice în îndeplinirea sarcinilor care le revin. Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor constituie, de asemenea, un interes legitim al operatorului de date în cauză. Prelucrarea de date cu caracter personal care are drept scop marketingul direct poate fi considerată ca fiind desfășurată pentru un interes legitim.
- (48) Operatorii care fac parte dintr-un grup de întreprinderi sau instituții afiliate unui organism central pot avea un interes legitim de a transmite date cu caracter personal în cadrul grupului de întreprinderi în scopuri administrative interne, inclusiv în scopul prelucrării datelor cu caracter personal ale clienților sau angajaților. Principiile generale ale transferului de date cu caracter personal, în cadrul unui grup de întreprinderi, către o întreprindere situată într-o țară terță rămân neschimbate.
- (49) Prelucrarea datelor cu caracter personal în măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor, și anume capacitatea unei rețele sau a unui sistem de informații de a face față, la un anumit nivel de încredere, evenimentelor accidentale sau acțiunilor ilegale sau rău intenționate care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor cu caracter personal stocate sau transmise, precum și securitatea serviciilor conexe oferite de aceste rețele și sisteme, sau accesibile prin intermediul acestora, de către autoritățile publice, echipele de intervenție în caz de urgență informatică, echipele de intervenție în cazul producerii unor incidente care afectează securitatea informatică, furnizorii de rețele și servicii de comunicații electronice, precum și de către furnizorii de servicii și tehnologii de securitate, constituie un interes legitim al operatorului de date în cauză. Acesta ar putea include, de exemplu, prevenirea accesului neautorizat la rețelele de comunicații electronice și a difuzării de coduri dăunătoare și oprirea atacurilor de „blocare a serviciului”, precum și prevenirea daunelor aduse calculatoarelor și sistemelor de comunicații electronice.
- (50) Prelucrarea datelor cu caracter personal în alte scopuri decât scopurile pentru care datele cu caracter personal au fost inițial colectate ar trebui să fie permisă doar atunci când prelucrarea este compatibilă cu scopurile respective pentru care datele cu caracter personal au fost inițial colectate. În acest caz nu este necesar un temei juridic separat de cel pe baza căruia a fost permisă colectarea datelor cu caracter personal. În cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul, dreptul Uniunii sau dreptul intern poate stabili și specifica sarcinile și scopurile pentru care prelucrarea ulterioară ar trebui considerată a fi compatibilă și legală. Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ar trebui considerată ca reprezentând operațiuni de prelucrare legale compatibile. Temeiul juridic prevăzut în dreptul Uniunii sau în dreptul intern pentru prelucrarea datelor cu caracter personal poate constitui, de asemenea, un temei juridic pentru prelucrarea ulterioară. Pentru a stabili dacă scopul prelucrării ulterioare este compatibil cu scopul pentru care au fost colectate inițial datele cu caracter personal, operatorul, după ce a îndeplinit toate cerințele privind legalitatea prelucrării inițiale, ar trebui să țină seama, printre altele, de orice legătură între respectivele scopuri și scopurile prelucrării ulterioare preconizate, de contextul în care au fost colectate datele cu caracter personal, în special de așteptările rezonabile ale persoanelor vizate, bazate pe relația lor cu operatorul, în ceea ce privește utilizarea ulterioară a datelor, de natura datelor cu caracter personal, de

consecințele prelucrării ulterioare preconizate asupra persoanelor vizate, precum și de existența garanțiilor corespunzătoare atât în cadrul operațiunilor de prelucrare inițiale, cât și în cadrul operațiunilor de prelucrare ulterioare preconizate.

În cazul în care persoana vizată și-a dat consimțământul sau prelucrarea se bazează pe dreptul Uniunii sau pe dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja, în special, obiective importante de interes public general, operatorul ar trebui să aibă posibilitatea de a prelucra în continuare datele cu caracter personal, indiferent de compatibilitatea scopurilor. În orice caz, aplicarea principiilor stabilite de prezentul regulament și, în special, informarea persoanei vizate cu privire la aceste alte scopuri și la drepturile sale, inclusiv dreptul la opoziție, ar trebui să fie garantate. Indicarea unor posibile infracțiuni sau amenințări la adresa siguranței publice de către operator și transmiterea către o autoritate competentă a datelor cu caracter personal relevante în cazuri individuale sau în mai multe cazuri legate de aceeași infracțiune sau de aceeași amenințări la adresa siguranței publice ar trebui considerată ca fiind în interesul legitim urmărit de operator. Cu toate acestea, o astfel de transmitere în interesul legitim al operatorului sau prelucrarea ulterioară a datelor cu caracter personal ar trebui interzisă în cazul în care prelucrarea nu este compatibilă cu o obligație legală, profesională sau cu o altă obligație de păstrare a confidențialității.

- (51) Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale necesită o protecție specifică, deoarece contextul prelucrării acestora ar putea genera riscuri considerabile la adresa drepturilor și libertăților fundamentale. Aceste date cu caracter personal ar trebui să includă datele cu caracter personal care dezvăluie originea rasială sau etnică, utilizarea termenului „origine rasială” în prezentul regulament neimplicând o acceptare de către Uniune a teoriilor care urmăresc să stabilească existența unor rase umane separate. Prelucrarea fotografiilor nu ar trebui să fie considerată în mod sistematic ca fiind o prelucrare de categorii speciale de date cu caracter personal, întrucât fotografiile intră sub incidența definiției datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice. Asemenea date cu caracter personal nu ar trebui prelucrate, cu excepția cazului în care prelucrarea este permisă în cazuri specifice prevăzute de prezentul regulament, ținând seama de faptul că dreptul statelor membre poate prevedea dispoziții specifice cu privire la protecția datelor în scopul adaptării aplicării normelor din prezentul regulament în vederea respectării unei obligații legale sau a îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul. Pe lângă cerințele specifice pentru o astfel de prelucrare, ar trebui să se aplice principiile generale și alte norme prevăzute de prezentul regulament, în special în ceea ce privește condițiile pentru prelucrarea legală. Ar trebui prevăzute în mod explicit derogări de la interdicția generală de prelucrare a acestor categorii speciale de date cu caracter personal, printre altele atunci când persoana vizată își dă consimțământul explicit sau în ceea ce privește nevoile specifice în special atunci când prelucrarea este efectuată în cadrul unor activități legitime de către anumite asociații sau fundații al căror scop este de a permite exercitarea libertăților fundamentale.
- (52) Derogarea de la interdicția privind prelucrarea categoriilor speciale de date cu caracter personal ar trebui să fie permisă, de asemenea, în cazul în care dreptul Uniunii sau dreptul intern prevede acest lucru și ar trebui să facă obiectul unor garanții adecvate, astfel încât să fie protejate datele cu caracter personal și alte drepturi fundamentale, atunci când acest lucru se justifică din motive de interes public, în special în cazul prelucrării datelor cu caracter personal în domeniul legislației privind ocuparea forței de muncă, protecția socială, inclusiv pensiile, precum și în scopuri de securitate, supraveghere și alertă în materie de sănătate, pentru prevenirea sau controlul bolilor transmisibile și a altor amenințări grave la adresa sănătății. Această derogare poate fi acordată în scopuri medicale, inclusiv sănătatea publică și gestionarea serviciilor de asistență medicală, în special în vederea asigurării calității și eficienței din punctul de vedere al costurilor ale procedurilor utilizate pentru soluționarea cererilor de prestații și servicii în cadrul sistemului de asigurări de sănătate, sau în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. De asemenea, prelucrarea unor asemenea date cu caracter personal ar trebui permisă, printr-o derogare, atunci când este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiție, indiferent dacă are loc în cadrul unei proceduri în fața unei instanțe sau în cadrul unei proceduri administrative sau a unei proceduri extrajudiciare.
- (53) Categoriile speciale de date cu caracter personal care necesită un nivel mai ridicat de protecție ar trebui prelucrate doar în scopuri legate de sănătate atunci când este necesar pentru realizarea acestor scopuri în beneficiul persoanelor fizice și al societății în general, în special în contextul gestionării serviciilor și sistemelor de sănătate sau de asistență socială, inclusiv prelucrarea acestor date de către autoritățile de management și de către autoritățile centrale naționale din domeniul sănătății în scopul controlului calității, furnizării de informații de gestiune și al supravegherii generale a sistemului de sănătate sau de asistență socială la nivel național și local, precum și în contextul asigurării continuității asistenței medicale sau sociale și a asistenței medicale transfrontaliere ori în scopuri de securitate, supraveghere și alertă în materie de sănătate ori în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice în temeiul dreptului Uniunii sau al dreptului intern, care trebuie să urmărească un obiectiv de interes public, precum și în cazul studiilor realizate în interes public în domeniul sănătății publice. Prin urmare, prezentul regulament ar trebui să prevadă condiții armonizate pentru prelucrarea categoriilor speciale de date cu caracter personal privind sănătatea, în ceea ce privește nevoile specifice, în special atunci când prelucrarea acestor date este efectuată în anumite scopuri legate de sănătate de către persoane care fac obiectul unei obligații legale de a păstra secretul profesional. Dreptul

Uniunii sau dreptul intern ar trebui să prevadă măsuri specifice și adecvate pentru a proteja drepturile fundamentale și datele cu caracter personal ale persoanelor fizice. Statele membre ar trebui să aibă posibilitatea de a menține sau de a introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea. Totuși, acest lucru nu ar trebui să împiedice libera circulație a datelor cu caracter personal în cadrul Uniunii atunci când aceste condiții se aplică prelucrării transfrontaliere a unor astfel de date.

- (54) Prelucrarea categoriilor speciale de date cu caracter personal poate fi necesară din motive de interes public în domeniile sănătății publice, fără consimțământul persoanei vizate. O astfel de prelucrare ar trebui condiționată de măsuri adecvate și specifice destinate să protejeze drepturile și libertățile persoanelor fizice. În acest context, conceptul de „sănătate publică” ar trebui interpretat astfel cum este definit în Regulamentul (CE) nr. 1338/2008 al Parlamentului European și al Consiliului ⁽¹⁾, și anume toate elementele referitoare la sănătate și anume starea de sănătate, inclusiv morbiditatea sau handicapul, factorii determinanți care au efect asupra stării de sănătate, necesitățile în domeniul asistenței medicale, resursele alocate asistenței medicale, furnizarea asistenței medicale și asigurarea accesului universal la aceasta, precum și cheltuielile și sursele de finanțare în domeniul sănătății și cauzele mortalității. Această prelucrare a datelor privind sănătatea din motive de interes public nu ar trebui să ducă la prelucrarea acestor date în alte scopuri de către părți terțe, cum ar fi angajatorii sau societățile de asigurări și băncile.
- (55) În plus, prelucrarea datelor cu caracter personal de către autoritățile publice în vederea realizării obiectivelor prevăzute de dreptul constituțional sau de dreptul internațional public, ale asociațiilor religioase recunoscute oficial se efectuează din motive de interes public.
- (56) În cazul în care, în cadrul activităților electorale, funcționarea sistemului democratic necesită, într-un stat membru, ca partidele politice să colecteze date cu caracter personal privind opiniile politice ale persoanelor, prelucrarea unor astfel de date poate fi permisă din motive de interes public, cu condiția să se prevadă garanțiile corespunzătoare.
- (57) Dacă datele cu caracter personal prelucrate de un operator nu îi permit acestuia să identifice o persoană fizică, operatorul de date nu ar trebui să aibă obligația de a obține informații suplimentare în vederea identificării persoanei vizate, cu unicul scop de a respecta oricare dintre dispozițiile prezentului regulament. Cu toate acestea, operatorul nu ar trebui să refuze să preia informațiile suplimentare furnizate de persoana vizată cu scopul de a sprijini exercitarea drepturilor acesteia. Identificarea ar trebui să includă identificarea digitală a unei persoane vizate, de exemplu prin mecanisme de autentificare precum aceleași acreditări utilizate de către persoana vizată pentru a accesa serviciile online oferite de operatorul de date.
- (58) Principiul transparenței prevede că orice informații care se adresează publicului sau persoanei vizate să fie concise, ușor accesibile și ușor de înțeles și să se utilizeze un limbaj simplu și clar, precum și vizualizare acolo unde este cazul. Aceste informații ar putea fi furnizate în format electronic, de exemplu atunci când sunt adresate publicului, prin intermediul unui site. Acest lucru este important în special în situații în care datorită multitudinii actorilor și a complexității, din punct de vedere tehnologic, a practicii, este dificil ca persoana vizată să știe și să înțeleagă dacă datele cu caracter personal care o privesc sunt colectate, de către cine și în ce scop, cum este cazul publicității online. Întrucât copiii necesită o protecție specifică, orice informații și orice comunicare, în cazul în care prelucrarea vizează un copil, ar trebui să fie exprimate într-un limbaj simplu și clar, astfel încât copilul să îl poată înțelege cu ușurință.
- (59) Ar trebui să fie prevăzute modalități de facilitare a exercitării de către persoana vizată a drepturilor care îi sunt conferite prin prezentul regulament, inclusiv mecanismele prin care aceasta poate solicita și, dacă este cazul, obține, în mod gratuit, în special, acces la datele cu caracter personal, precum și rectificarea sau ștergerea acestora, și exercitarea dreptului la opoziție. Operatorul ar trebui să ofere, de asemenea, modalități de introducere a cererilor pe cale electronică, mai ales în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice. Operatorul ar trebui să aibă obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate și cel târziu în termen de o lună și, în cazul în care nu intenționează să se conformeze respectivele cereri, să motiveze acest refuz.

⁽¹⁾ Regulamentul (CE) nr. 1338/2008 al Parlamentului European și al Consiliului din 16 decembrie 2008 privind statisticile comunitare referitoare la sănătatea publică, precum și la sănătatea și siguranța la locul de muncă (JO L 354, 31.12.2008, p. 70).

- (60) Conform principiilor prelucrării echitabile și transparente, persoana vizată este informată cu privire la existența unei operațiuni de prelucrare și la scopurile acesteia. Operatorul ar trebui să furnizeze persoanei vizate orice informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă, ținând seama de circumstanțele specifice și de contextul în care sunt prelucrate datele cu caracter personal. În plus, persoana vizată ar trebui informată cu privire la crearea de profiluri, precum și la consecințele acesteia. Atunci când datele cu caracter personal sunt colectate de la persoana vizată, aceasta ar trebui informată, de asemenea, dacă are obligația de a furniza datele cu caracter personal și care sunt consecințele în cazul unui refuz. Aceste informații pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea ar trebui să poată fi citite automat.
- (61) Informațiile în legătură cu prelucrarea datelor cu caracter personal referitoare la persoana vizată ar trebui furnizate acesteia la momentul colectării de la persoana vizată sau, în cazul în care datele cu caracter personal sunt obținute din altă sursă, într-o perioadă rezonabilă, în funcție de circumstanțele cazului. În cazul în care datele cu caracter personal pot fi divulgate în mod legitim unui alt destinatar, persoana vizată ar trebui informată atunci când datele cu caracter personal sunt divulgate pentru prima dată destinatarului. În cazul în care operatorul intenționează să prelucreze datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul ar trebui să furnizeze persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și alte informații necesare. În cazul în care originea datelor cu caracter personal nu a putut fi comunicată persoanei vizate din cauză că au fost utilizate surse diverse, informațiile generale ar trebui furnizate.
- (62) Cu toate acestea, nu este necesară impunerea obligației de a furniza informații în cazul în care persoana vizată deține deja informațiile, în cazul în care înregistrarea sau divulgarea datelor cu caracter personal este prevăzută în mod expres de lege sau în cazul în care informarea persoanei vizate se dovedește imposibilă sau ar implica eforturi disproporționate. Acesta din urmă ar putea fi cazul în special atunci când prelucrarea se efectuează în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. În această privință, ar trebui luate în considerare numărul persoanelor vizate, vechimea datelor și orice garanții adecvate adoptate.
- (63) O persoană vizată ar trebui să aibă drept de acces la datele cu caracter personal colectate care o privesc și ar trebui să își exercite acest drept cu ușurință și la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia. Acest lucru include dreptul persoanelor vizate de a avea acces la datele lor privind sănătatea, de exemplu datele din registrele lor medicale conținând informații precum diagnostice, rezultate ale examinărilor, evaluări ale medicilor curanți și orice tratament sau intervenție efectuată. Orice persoană vizată ar trebui, prin urmare, să aibă dreptul de a cunoaște și de a i se comunica în special scopurile în care sunt prelucrate datele, dacă este posibil perioada pentru care se prelucrează datele cu caracter personal, destinarii datelor cu caracter personal, logica de prelucrare automată a datelor cu caracter personal și, cel puțin în cazul în care se bazează pe crearea de profiluri, consecințele unei astfel de prelucrări. Dacă acest lucru este posibil, operatorul de date ar trebui să poată furniza acces de la distanță la un sistem sigur, care să ofere persoanei vizate acces direct la datele sale cu caracter personal. Acest drept nu ar trebui să aducă atingere drepturilor sau libertăților altora, inclusiv secretului comercial sau proprietății intelectuale și, în special, drepturilor de autor care asigură protecția programelor software. Cu toate acestea, considerațiile de mai sus nu ar trebui să aibă drept rezultat refuzul de a furniza toate informațiile persoanei vizate. Atunci când operatorul prelucrează un volum mare de informații privind persoana vizată, operatorul ar trebui să poată solicita ca, înainte de a îi fi furnizate informațiile, persoana vizată să precizeze informațiile sau activitățile de prelucrare la care se referă cererea sa.
- (64) Operatorul ar trebui să ia toate măsurile rezonabile pentru a verifica identitatea unei persoane vizate care solicită acces la date, în special în contextul serviciilor online și al identificatorilor online. Un operator nu ar trebui să rețină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacționeze la cereri potențiale.
- (65) O persoană vizată ar trebui să aibă dreptul la rectificarea datelor cu caracter personal care o privesc și „dreptul de a fi uitată”, în cazul în care păstrarea acestor date încalcă prezentul regulament sau dreptul Uniunii sau dreptul intern sub incidența căruia intră operatorul. În special, persoanele vizate ar trebui să aibă dreptul ca datele lor cu caracter personal să fie șterse și să nu mai fie prelucrate, în cazul în care datele cu caracter personal nu mai sunt necesare pentru scopurile în care sunt colectate sau sunt prelucrate, în cazul în care persoanele vizate și-au retras consimțământul pentru prelucrare sau în cazul în care acestea se opun prelucrării datelor cu caracter personal care le privesc sau în cazul în care prelucrarea datelor cu caracter personal ale acestora nu este conformă cu

prezentul regulament. Acest drept este relevant în special în cazul în care persoana vizată și-a dat consimțământul când era copil și nu cunoștea pe deplin riscurile pe care le implică prelucrarea, iar ulterior dorește să elimine astfel de date cu caracter personal, în special de pe internet. Persoana vizată ar trebui să aibă posibilitatea de a-și exercita acest drept în pofida faptului că nu mai este copil. Cu toate acestea, păstrarea în continuare a datelor cu caracter personal ar trebui să fie legală în cazul în care este necesară pentru exercitarea dreptului la libertatea de exprimare și de informare, pentru respectarea unei obligații legale, pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul, din motive de interes public în domeniul sănătății publice, în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice sau pentru constatarea, exercitarea sau apărarea unui drept în instanță.

- (66) Pentru a se consolida „dreptul de a fi uitat” în mediul online, dreptul de ștergere ar trebui să fie extins astfel încât un operator care a făcut publice date cu caracter personal ar trebui să aibă obligația de a informa operatorii care prelucrează respectivele date cu caracter personal să șteargă orice linkuri către datele respective sau copii sau reproduceri ale acestora. În acest scop, operatorul în cauză ar trebui să ia măsuri rezonabile, ținând seama de tehnologia disponibilă și de mijloacele aflate la dispoziția lui, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal în ceea ce privește cererea persoanei vizate.
- (67) Metodele de restricționare a prelucrării de date cu caracter personal ar putea include, printre altele, mutarea temporară a datelor cu caracter personal selectate într-un alt sistem de prelucrare, sau anularea accesului utilizatorilor la datele selectate sau înlăturarea temporară a datelor publicate de pe un site. În ceea ce privește sistemele automatizate de evidență a datelor, restricționarea prelucrării ar trebui, în principiu, asigurată prin mijloace tehnice în așa fel încât datele cu caracter personal să nu facă obiectul unor operațiuni de prelucrare ulterioară și să nu mai poată fi schimbate. Faptul că prelucrarea datelor cu caracter personal este restricționată ar trebui indicat în mod clar în sistem.
- (68) Pentru a spori suplimentar controlul asupra propriilor date, persoana vizată ar trebui, în cazul în care datele cu caracter personal sunt prelucrate prin mijloace automate, să poată primi datele cu caracter personal care o privesc și pe care le-a furnizat unui operator, într-un format structurat, utilizat în mod curent, prelucrabil automat și interoperabil și să le poată transmite unui alt operator. Operatorii de date ar trebui să fie încurajați să dezvolte formate interoperabile care să permită portabilitatea datelor. Acest drept ar trebui să se aplice în cazul în care persoana vizată a furnizat datele cu caracter personal pe baza propriului consimțământ sau în cazul în care prelucrarea datelor este necesară pentru executarea unui contract. Acest drept nu ar trebui să se aplice în cazul în care prelucrarea se bazează pe un alt temei juridic decât consimțământul sau contractul. Prin însăși natura sa, acest drept nu ar trebui exercitat împotriva operatorilor care prelucrează date cu caracter personal în cadrul exercitării funcțiilor lor publice. Acesta nu ar trebui să se aplice în special în cazul în care prelucrarea de date cu caracter personal este necesară în vederea respectării unei obligații legale căreia îi este supus operatorul sau în cazul îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea unei autorități publice cu care este investit operatorul. Dreptul persoanei vizate de a transmite sau de a primi date cu caracter personal care o privesc nu ar trebui să creeze pentru operatori obligația de a adopta sau de a menține sisteme de prelucrare care să fie compatibile din punct de vedere tehnic. În cazul în care, într-un anumit set de date cu caracter personal, sunt implicate mai multe persoane vizate, dreptul de a primi datele cu caracter personal nu ar trebui să aducă atingere drepturilor și libertăților altor persoane vizate, în conformitate cu prezentul regulament. De asemenea, acest drept nu ar trebui să aducă atingere dreptului persoanei vizate de a obține ștergerea datelor cu caracter personal și limitărilor dreptului respectiv, astfel cum sunt prevăzute în prezentul regulament, și nu ar trebui, în special, să implice ștergerea acelor date cu caracter personal referitoare la persoana vizată care au fost furnizate de către aceasta în vederea executării unui contract, în măsura în care și atât timp cât datele respective sunt necesare pentru executarea contractului. Persoana vizată ar trebui să aibă dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul, dacă acest lucru este fezabil din punct de vedere tehnic.
- (69) În cazurile în care datele cu caracter personal ar putea fi prelucrate în mod legal deoarece prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul sau pe baza intereselor legitime ale unui operator sau ale unei părți terțe, o persoană vizată ar trebui să aibă totuși dreptul de a se opune prelucrării oricăror date cu caracter personal care se referă la situația sa particulară. Ar trebui să revină operatorului sarcina de a demonstra că interesele sale legitime și imperioase prevalează asupra intereselor sau a drepturilor și libertăților fundamentale ale persoanei vizate.
- (70) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de marketing direct, persoana vizată ar trebui să aibă dreptul de a se opune unei astfel de prelucrări, inclusiv creării de profiluri în măsura în care aceasta are legătură cu marketingul direct, indiferent dacă prelucrarea în cauză este cea inițială sau una ulterioară, în orice moment și în mod gratuit. Acest drept ar trebui adus în mod explicit în atenția persoanei vizate și prezentat în mod clar și separat de orice alte informații.

- (71) Persoana vizată ar trebui să aibă dreptul de a nu face obiectul unei decizii, care poate include o măsură, care evaluează aspecte personale referitoare la persoana vizată, care se bazează exclusiv pe prelucrarea automată și care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă, cum ar fi refuzul automat al unei cereri de credit online sau practicile de recrutare pe cale electronică, fără intervenție umană. O astfel de prelucrare include „crearea de profiluri”, care constă în orice formă de prelucrare automată a datelor cu caracter personal prin evaluarea aspectelor personale referitoare la o persoană fizică, în special în vederea analizării sau preconizării anumitor aspecte privind randamentul la locul de muncă al persoanei vizate, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările, atunci când aceasta produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă. Cu toate acestea, luarea de decizii pe baza unei astfel de prelucrări, inclusiv crearea de profiluri, ar trebui permisă în cazul în care este autorizată în mod expres în dreptul Uniunii sau în dreptul intern care se aplică operatorului, inclusiv în scopul monitorizării și prevenirii fraudei și a evaziunii fiscale, desfășurate în conformitate cu reglementările, standardele și recomandările instituțiilor Uniunii sau ale organismelor naționale de supraveghere, și în scopul asigurării securității și fiabilității unui serviciu oferit de operator sau în cazul în care este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator sau în cazul în care persoana vizată și-a dat în mod explicit consimțământul. În orice caz, o astfel de prelucrare ar trebui să facă obiectul unor garanții corespunzătoare, care ar trebui să includă o informare specifică a persoanei vizate și dreptul acesteia de a obține intervenție umană, de a-și exprima punctul de vedere, de a primi o explicație privind decizia luată în urma unei astfel de evaluări, precum și dreptul de a contesta decizia. O astfel de măsură nu ar trebui să se refere la un copil.

Pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată, având în vedere circumstanțele specifice și contextul în care sunt prelucrate datele cu caracter personal, operatorul ar trebui să utilizeze proceduri matematice sau statistice adecvate pentru crearea de profiluri, să implementeze măsuri tehnice și organizatorice adecvate pentru a asigura în special faptul că factorii care duc la inexactități ale datelor cu caracter personal sunt corecți și că riscul de erori este redus la minimum, precum și să securizeze datele cu caracter personal într-un mod care să țină seama de pericolele potențiale la adresa intereselor și drepturilor persoanei vizate și care să prevină, printre altele, efectele discriminatorii împotriva persoanelor pe motiv de rasă sau origine etnică, opinii politice, religie sau convingeri, apartenență sindicală, caracteristici genetice, stare de sănătate sau orientare sexuală sau care să ducă la măsuri care să aibă astfel de efecte. Procesul decizional automatizat și crearea de profiluri pe baza unor categorii speciale de date cu caracter personal ar trebui permise numai în condiții specifice.

- (72) Crearea de profiluri este supusă normelor prezentului regulament care reglementează prelucrarea datelor cu caracter personal, precum temeiurile juridice ale prelucrării sau principiile de protecție a datelor. Comitetul european pentru protecția datelor instituit prin prezentul regulament („comitetul”) ar trebui să poată emite orientări în acest context.
- (73) Dreptul Uniunii sau dreptul intern poate impune restricții în privința unor principii specifice, în privința dreptului de informare, a dreptului de acces la datele cu caracter personal și de rectificare sau ștergere a acestora, în privința dreptului la portabilitatea datelor, a dreptului la opoziție, a deciziilor bazate pe crearea de profiluri, precum și în privința comunicării unei încălcări a securității datelor cu caracter personal persoanei vizate și a anumitor obligații conexe ale operatorilor, în măsura în care acest lucru este necesar și proporțional într-o societate democratică pentru a se garanta siguranța publică, inclusiv protecția vieții oamenilor, în special ca răspuns la dezastru naturale sau provocate de om, prevenirea, investigarea și urmărirea penală a infracțiunilor sau executarea pedepselor, inclusiv protejarea împotriva amenințărilor la adresa siguranței publice sau împotriva încălcării eticii în cazul profesiilor reglementate și prevenirea acestora, alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, menținerea de registre publice din motive de interes public general, prelucrarea ulterioară a datelor cu caracter personal arhivate pentru a transmite informații specifice legate de comportamentul politic în perioada regimurilor fostelor state totalitare, protecția persoanei vizate sau a drepturilor și libertăților unor terți, inclusiv protecția socială, sănătatea publică și scopurile umanitare. Aceste restricții ar trebui să fie conforme cu cerințele prevăzute de cartă și de Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale.
- (74) Ar trebui să se stabilească responsabilitatea și răspunderea operatorului pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său. În special, operatorul ar trebui să fie obligat să implementeze măsuri adecvate și eficiente și să fie în măsură să demonstreze conformitatea activităților de prelucrare cu prezentul regulament, inclusiv eficacitatea măsurilor. Aceste măsuri ar trebui să țină seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul pentru drepturile și libertățile persoanelor fizice.

- (75) Riscul pentru drepturile și libertățile persoanelor fizice, prezentând grade diferite de probabilitate de materializare și de gravitate, poate fi rezultatul unei prelucrări a datelor cu caracter personal care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care: prelucrarea poate conduce la discriminare, furt sau fraudă a identității, pierdere financiară, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional, inversarea neautorizată a pseudonimizării sau la orice alt dezavantaj semnificativ de natură economică sau socială; persoanele vizate ar putea fi private de drepturile și libertățile lor sau împiedicate să-și exercite controlul asupra datelor lor cu caracter personal; datele cu caracter personal prelucrate sunt date care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența sindicală; sunt prelucrate date genetice, date privind sănătatea sau date privind viața sexuală sau privind condamnările penale și infracțiunile sau măsurile de securitate conexe; sunt evaluate aspecte de natură personală, în special analizarea sau previzionarea unor aspecte privind randamentul la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările, în scopul de a se crea sau de a se utiliza profiluri personale; sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale unor copii; sau prelucrarea implică un volum mare de date cu caracter personal și afectează un număr larg de persoane vizate.
- (76) Probabilitatea de a se materializa și gravitatea riscului pentru drepturile și libertățile persoanei vizate ar trebui să fie determinate în funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor cu caracter personal. Riscul ar trebui apreciat pe baza unei evaluări obiective prin care se stabilește dacă operațiunile de prelucrare a datelor prezintă un risc sau un risc ridicat.
- (77) Orientări pentru implementarea unor măsuri adecvate și pentru demonstrarea conformității de către operator sau persoana împuternicită de operator, mai ales în ceea ce privește identificarea riscului legat de prelucrare, evaluarea acestuia din punctul de vedere al originii, naturii, probabilității de a se materializa și al gravității, precum și identificarea bunelor practici pentru atenuarea riscului ar putea fi oferite în special prin coduri de conduită aprobate, certificări aprobate, orientări ale comitetului sau prin indicații furnizate de un responsabil cu protecția datelor. Comitetul poate, de asemenea, să emită orientări cu privire la operațiunile de prelucrare care sunt considerate puțin susceptibile de a genera un risc ridicat pentru drepturile și libertățile persoanelor fizice și să indice măsurile care se pot dovedi suficiente în asemenea cazuri pentru a aborda un astfel de risc.
- (78) Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare pentru a se asigura îndeplinirea cerințelor din prezentul regulament. Pentru a fi în măsură să demonstreze conformitatea cu prezentul regulament, operatorul ar trebui să adopte politici interne și să pună în aplicare măsuri care să respecte în special principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor. Astfel de măsuri ar putea consta, printre altele, în reducerea la minimum a prelucrării datelor cu caracter personal, pseudonimizarea acestor date cât mai curând posibil, transparența în ceea ce privește funcțiile și prelucrarea datelor cu caracter personal, abilitarea persoanei vizate să monitorizeze prelucrarea datelor, abilitarea operatorului să creeze elemente de siguranță și să le îmbunătățească. Atunci când elaborează, proiectează, selectează și utilizează aplicații, servicii și produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează date cu caracter personal pentru a-și îndeplini rolul, producătorii acestor produse și furnizorii acestor servicii și aplicații ar trebui să fie încurajați să aibă în vedere dreptul la protecția datelor la momentul elaborării și proiectării unor astfel de produse, servicii și aplicații și, ținând cont de stadiul actual al dezvoltării, să se asigure că operatorii și persoanele împuternicite de operatori sunt în măsură să își îndeplinească obligațiile referitoare la protecția datelor. Principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor ar trebui să fie luate în considerare și în contextul licitațiilor publice.
- (79) Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și a persoanelor împuternicite de operator, inclusiv în ceea ce privește monitorizarea de către autoritățile de supraveghere și măsurile adoptate de acestea, necesită o atribuire clară a responsabilităților în temeiul prezentului regulament, inclusiv în cazul în care un operator stabilește scopurile și mijloacele prelucrării împreună cu alți operatori sau în cazul în care o operațiune de prelucrare este efectuată în numele unui operator.
- (80) Atunci când un operator sau o persoană împuternicită de operator care nu este stabilită în Uniune prelucrează date cu caracter personal ale unor persoane vizate care se află pe teritoriul Uniunii, iar activitățile sale de prelucrare au legătură cu oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată, sau cu monitorizarea comportamentului unor persoane vizate dacă acesta se manifestă în cadrul Uniunii, operatorul sau persoana împuternicită de operator ar trebui să desemneze un reprezentant, cu excepția cazului în care prelucrarea are caracter ocazional, nu include prelucrarea pe scară largă a unor categorii speciale de date cu caracter personal și nici prelucrarea de date

referitoare la condamnări penale și la infracțiuni, și este puțin susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice, având în vedere natura, contextul, domeniul de aplicare și scopurile prelucrării, precum și a cazului în care operatorul este o autoritate publică sau un organism public. Reprezentantul ar trebui să acționeze în numele operatorului sau al persoanei împuternicite de operator, putând fi contactat de orice autoritate de supraveghere. Reprezentantul ar trebui desemnat în mod explicit, printr-un mandat scris al operatorului sau al persoanei împuternicite de operator, să acționeze în numele acestuia (acesteia) în ceea ce privește obligațiile lor în temeiul prezentului regulament. Desemnarea unui astfel de reprezentant nu aduce atingere responsabilității sau răspunderii operatorului sau a persoanei împuternicite de operator în temeiul prezentului regulament. Un astfel de reprezentant ar trebui să își îndeplinească sarcinile în conformitate cu mandatul primit de la operator sau de la persoana împuternicită de operator, inclusiv să coopereze cu autoritățile de supraveghere competente în ceea ce privește orice acțiune întreprinsă pentru a asigura respectarea prezentului regulament. Reprezentantul desemnat ar trebui să fie supus unor proceduri de asigurare a respectării legii în cazul nerespectării prezentului regulament de către operator sau de către persoana împuternicită de operator.

- (81) Pentru a asigura respectarea cerințelor impuse de prezentul regulament în ceea ce privește prelucrarea care trebuie efectuată în numele operatorului de către persoana împuternicită de operator, atunci când atribuie activități de prelucrare unei persoane împuternicite de operator, acesta din urmă ar trebui să utilizeze numai persoane împuternicite care oferă garanții suficiente, în special în ceea ce privește cunoștințele de specialitate, fiabilitatea și resursele, pentru a implementa măsuri tehnice și organizatorice care îndeplinesc cerințele impuse de prezentul regulament, inclusiv pentru securitatea prelucrării. Aderarea de către persoana împuternicită de operator la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate fi utilizată drept element care să demonstreze respectarea obligațiilor de către operator. Efectuarea prelucrării de către o persoană împuternicită de un operator ar trebui să fie reglementată printr-un contract sau un alt tip de act juridic, în temeiul dreptului Uniunii sau al dreptului intern, care creează obligații pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopurile prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate, și ar trebui să țină seama de sarcinile și responsabilitățile specifice ale persoanei împuternicite de operator în contextul prelucrării care trebuie efectuată, precum și de riscul pentru drepturile și libertățile persoanei vizate. Operatorul și persoana împuternicită de operator pot alege să utilizeze un contract individual sau clauze contractuale standard care sunt adoptate fie direct de Comisie, fie de o autoritate de supraveghere în conformitate cu mecanismul de asigurare a coerenței și apoi adoptate de Comisie. După finalizarea prelucrării în numele operatorului, persoana împuternicită de operator ar trebui să returneze sau să șteargă, în funcție de opțiunea operatorului, datele cu caracter personal, cu excepția cazului în care există o cerință de stocare a datelor cu caracter personal în temeiul dreptului Uniunii sau al dreptului intern care instituie obligații pentru persoana împuternicită de operator.
- (82) În vederea demonstrării conformității cu prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să păstreze evidențe ale activităților de prelucrare aflate în responsabilitatea sa. Fiecare operator și fiecare persoană împuternicită de operator ar trebui să aibă obligația de a coopera cu autoritatea de supraveghere și de a pune la dispoziția acesteia, la cerere, aceste evidențe, pentru a putea fi utilizate în scopul monitorizării operațiunilor de prelucrare respective.
- (83) În vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să evalueze riscurile inerente prelucrării și să implementeze măsuri pentru atenuarea acestor riscuri, cum ar fi criptarea. Măsurile respective ar trebui să asigure un nivel corespunzător de securitate, inclusiv confidențialitatea, luând în considerare stadiul actual al dezvoltării și costurile implementării în raport cu riscurile și cu natura datelor cu caracter personal a căror protecție trebuie asigurată. La evaluarea riscului pentru securitatea datelor cu caracter personal, ar trebui să se acorde atenție riscurilor pe care le prezintă prelucrarea datelor, cum ar fi distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, în mod accidental sau ilegal, care pot duce în special la prejudicii fizice, materiale sau morale.
- (84) Pentru a favoriza respectarea dispozițiilor prezentului regulament în cazurile în care operațiunile de prelucrare sunt susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul ar trebui să fie responsabil de efectuarea unei evaluări a impactului asupra protecției datelor, care să estimeze, în special, originea, natura, specificitatea și gravitatea acestui risc. Rezultatul evaluării ar trebui luat în considerare la stabilirea măsurilor adecvate care trebuie luate pentru a demonstra că prelucrarea datelor cu caracter personal respectă prezentul regulament. În cazul în care o evaluare a impactului asupra protecției datelor arată că operațiunile de prelucrare implică un risc ridicat, pe care operatorul nu îl poate atenua prin măsuri adecvate sub aspectul tehnologiei disponibile și al costurilor implementării, ar trebui să aibă loc o consultare a autorității de supraveghere înainte de prelucrare.
- (85) Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură

economică sau socială adus persoanei fizice în cauză. Prin urmare, de îndată ce a luat cunoștință de producerea unei încălcări a securității datelor cu caracter personal, operatorul ar trebui să notifice această încălcare autorității de supraveghere, fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore după ce a luat la cunoștință de existența acesteia, cu excepția cazului în care operatorul este în măsură să demonstreze, în conformitate cu principiul responsabilității, că încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. Atunci când notificarea nu se poate realiza în termen de 72 de ore, aceasta ar trebui să cuprindă motivele întârzierii, iar informațiile pot fi furnizate treptat, fără altă întârziere.

- (86) Operatorul ar trebui să comunice persoanei vizate o încălcare a securității datelor cu caracter personal, fără întârzieri nejustificate, atunci când încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanei fizice, pentru a-i permite să ia măsurile de precauție necesare. Comunicarea ar trebui să descrie natura încălcării securității datelor cu caracter personal și să cuprindă recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative. Comunicările către persoanele vizate ar trebui efectuate în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu autoritatea de supraveghere, respectându-se orientările furnizate de aceasta sau de alte autorități competente, cum ar fi autoritățile de aplicare a legii. De exemplu, necesitatea de a atenua un risc imediat de producere a unui prejudiciu ar presupune comunicarea cu promptitudine către persoanele vizate, în timp ce necesitatea de a implementa măsuri corespunzătoare împotriva încălcării în continuare a securității datelor cu caracter personal sau împotriva unor încălcări similare ale securității datelor cu caracter personal ar putea justifica un termen mai îndelungat pentru comunicare.
- (87) Ar trebui să se stabilească dacă au fost implementate toate măsurile tehnologice de protecție și organizatorice corespunzătoare în scopul de a se stabili imediat dacă s-a produs o încălcare a securității datelor cu caracter personal și de a se informa cu promptitudine autoritatea de supraveghere și persoana vizată. Faptul că notificarea a fost efectuată fără întârziere nejustificată ar trebui stabilit luându-se în considerare, în special, natura și gravitatea încălcării securității datelor cu caracter personal, precum și consecințele și efectele negative ale acesteia asupra persoanei vizate. Această notificare poate conduce la o intervenție a autorității de supraveghere, în conformitate cu sarcinile și competențele specificate în prezentul regulament.
- (88) La stabilirea de norme detaliate privind formatul și procedurile aplicabile notificării referitoare la încălcările securității datelor cu caracter personal, ar trebui să se acorde atenția cuvenită circumstanțelor în care a avut loc încălcarea, stabilindu-se inclusiv dacă protecția datelor cu caracter personal a fost sau nu a fost asigurată prin măsuri tehnice de protecție corespunzătoare, care să limiteze efectiv probabilitatea fraudării identității sau a altor forme de utilizare abuzivă. În plus, astfel de norme și proceduri ar trebui să țină cont de interesele legitime ale autorităților de aplicare a legii în cazurile în care divulgarea timpurie ar putea îngreuna în mod inutil investigarea circumstanțelor în care a avut loc o încălcare a datelor cu caracter personal.
- (89) Directiva 95/46/CE a prevăzut o obligație generală de a notifica prelucrarea datelor cu caracter personal autorităților de supraveghere. Cu toate că obligația respectivă generează sarcini administrative și financiare, aceasta nu a contribuit întotdeauna la îmbunătățirea protecției datelor cu caracter personal. Prin urmare, astfel de obligații de notificare generală nediferențiată ar trebui să fie abrogate și înlocuite cu proceduri și mecanisme eficace care să pună accentul, în schimb, pe acele tipuri de operațiuni de prelucrare susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice prin însăși natura lor, prin domeniul lor de aplicare, prin contextul și prin scopurile lor. Astfel de tipuri de operațiuni de prelucrare pot fi cele care presupun, în special, utilizarea unor noi tehnologii sau care reprezintă un nou tip de operațiuni, pentru care nicio evaluare a impactului asupra protecției datelor nu a fost efectuată anterior de către operator ori care devin necesare dată fiind perioada de timp care s-a scurs de la prelucrarea inițială.
- (90) În astfel de cazuri, operatorul ar trebui să efectueze, înainte de prelucrare, o evaluare a impactului asupra protecției datelor, în scopul evaluării gradului specific de probabilitate a materializării riscului ridicat și gravitatea acestuia, având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și sursele riscului. Respectiva evaluare a impactului ar trebui să includă, în special, măsurile, garanțiile și mecanismele avute în vedere pentru atenuarea riscului respectiv, pentru asigurarea protecției datelor cu caracter personal și pentru demonstrarea conformității cu prezentul regulament.
- (91) Aceasta ar trebui să se aplice, în special, operațiunilor de prelucrare la scară largă, care au drept obiectiv prelucrarea unui volum considerabil de date cu caracter personal la nivel regional, național sau supranațional, care ar putea afecta un număr mare de persoane vizate și care sunt susceptibile de a genera un risc ridicat, de exemplu, din cauza sensibilității lor, în cazul în care, în conformitate cu nivelul atins al cunoștințelor tehnologice, se folosește la scară largă o tehnologie nouă, precum și altor operațiuni de prelucrare care generează un risc ridicat pentru drepturile și libertățile persoanelor vizate, în special în cazul în care operațiunile respective

limitează capacitatea persoanelor vizate de a-și exercita drepturile. Ar trebui efectuată o evaluare a impactului asupra protecției datelor și în situațiile în care datele cu caracter personal sunt prelucrate în scopul luării de decizii care vizează anumite persoane fizice în urma unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, pe baza creării de profiluri pentru datele respective, sau în urma prelucrării unor categorii speciale de date cu caracter personal, a unor date biometrice sau a unor date privind condamnările penale și infracțiunile sau măsurile de securitate conexe. Este la fel de necesară o evaluare a impactului asupra protecției datelor pentru monitorizarea la scară largă a zonelor accesibile publicului, mai ales în cazul utilizării dispozitivelor optoelectronice sau pentru orice alte operațiuni în cazul în care autoritatea de supraveghere competentă consideră că prelucrarea este susceptibilă de a genera un risc ridicat pentru drepturile și libertățile persoanelor vizate, în special deoarece acestea împiedică persoanele vizate să exercite un drept sau să utilizeze un serviciu ori un contract, sau deoarece acestea sunt efectuate în mod sistematic la scară largă. Prelucrarea datelor cu caracter personal nu ar trebui considerată a fi la scară largă în cazul în care prelucrarea se referă la date cu caracter personal de la pacienți sau clienți de către un anumit medic, un alt profesionist în domeniul sănătății sau un avocat. În aceste cazuri, o evaluare a impactului asupra protecției datelor nu ar trebui să fie obligatorie.

- (92) În unele circumstanțe ar putea fi rezonabil și util din punct de vedere economic ca o evaluare a impactului asupra protecției datelor să aibă o perspectivă mai extinsă decât cea a unui singur proiect, de exemplu în cazul în care autorități sau organisme publice intenționează să instituie o aplicație sau o platformă de prelucrare comună sau în cazul în care mai mulți operatori preconizează să introducă o aplicație comună sau un mediu de prelucrare comun în cadrul unui sector sau segment industrial sau pentru o activitate orizontală utilizată la scară largă.
- (93) În contextul adoptării legislației naționale pe care se bazează îndeplinirea sarcinilor autorității publice sau ale organismului public și care reglementează operațiunea sau seria de operațiuni de prelucrare în cauză, statele membre pot considera că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.
- (94) În cazul în care o evaluare a impactului asupra protecției datelor arată că prelucrarea ar genera, în absența garanțiilor, măsurilor de securitate și mecanismelor de atenuare a riscului, un risc ridicat pentru drepturile și libertățile persoanelor fizice, iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile și al costurilor implementării, autoritatea de supraveghere ar trebui să fie consultată înainte de începerea activităților de prelucrare. Un astfel de risc ridicat este susceptibil să fie generat de anumite tipuri de prelucrare, precum și de amploarea și frecvența prelucrării, care pot duce și la producerea unor prejudicii sau pot atinge drepturile și libertățile persoanelor fizice. Autoritatea de supraveghere ar trebui să răspundă cererii de consultare într-un anumit termen. Cu toate acestea, lipsa unei reacții din partea autorității de supraveghere în termenul respectiv ar trebui să nu aducă atingere niciunei intervenții a autorității de supraveghere în conformitate cu sarcinile și competențele sale prevăzute în prezentul regulament, inclusiv competența de a interzice operațiuni de prelucrare. Ca parte a acestui proces de consultare, rezultatul unei evaluări a impactului asupra protecției datelor efectuate cu privire la prelucrarea în cauză poate fi transmis autorității de supraveghere, în special măsurile avute în vedere pentru a atenua riscul pentru drepturile și libertățile persoanelor fizice.
- (95) Persoana împuternicită de operator ar trebui să acorde asistență operatorului, dacă este necesar și la cerere, la asigurarea respectării obligațiilor care decurg din realizarea de evaluări ale impactului asupra protecției datelor și din consultarea prealabilă a autorității de supraveghere.
- (96) În timpul elaborării unei măsuri legislative sau de reglementare care prevede prelucrarea unor date cu caracter personal ar trebui, de asemenea, să aibă loc o consultare a autorității de supraveghere, pentru a garanta conformitatea prelucrării avute în vedere cu prezentul regulament și, în special, pentru a atenua riscul la care este expusă persoana vizată.
- (97) În cazul în care prelucrarea este efectuată de o autoritate publică, cu excepția instanțelor sau a autorităților judiciare independente atunci când acționează în calitatea lor judiciară, în cazul în care, în sectorul privat, prelucrarea este efectuată de un operator a cărui activitate principală constă în operațiuni de prelucrare care necesită o monitorizare regulată și sistematică a persoanelor vizate pe scară largă, sau în cazul în care activitatea principală a operatorului sau a persoanei împuternicite de operator constă în prelucrarea pe scară largă de categorii speciale de date cu caracter personal și de date privind condamnările penale și infracțiunile, o persoană care deține cunoștințe de specialitate în materie de legislație și practici privind protecția datelor ar trebui să acorde asistență operatorului sau persoanei împuternicite de operator pentru monitorizarea conformității, la nivel intern, cu prezentul regulament. În sectorul privat, activitățile principale ale unui operator se referă la activitățile sale de bază, și nu la prelucrarea datelor cu caracter personal drept activități auxiliare. Nivelul necesar al cunoștințelor de specialitate ar trebui să fie stabilit în special în funcție de operațiunile de prelucrare a datelor

efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate de operator sau de persoana împuternicită de operator. Acești responsabili cu protecția datelor, indiferent dacă sunt sau nu angajați ai operatorului, ar trebui să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent.

- (98) Asociațiile sau alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori ar trebui încurajate să elaboreze coduri de conduită, în limitele prezentului regulament, astfel încât să se faciliteze aplicarea efectivă a prezentului regulament, luându-se în considerare caracteristicile specifice ale prelucrării efectuate în anumite sectoare și necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii. În special, astfel de coduri de conduită ar putea să ajusteze obligațiile operatorilor și ale persoanelor împuternicite de operatori, ținând seama de riscul aferent prelucrării care este susceptibil de a fi generat pentru drepturile și libertățile persoanelor fizice.
- (99) Atunci când elaborează un cod de conduită sau când modifică sau extind un astfel de cod, asociațiile și alte organisme care reprezintă categorii de operatori sau persoane împuternicite de operatori ar trebui să consulte părțile implicate relevante, inclusiv persoanele vizate, dacă este fezabil, și să ia în considerare contribuțiile transmise și opiniile exprimate în cadrul unor astfel de consultări.
- (100) Pentru a se îmbunătăți transparența și conformitatea cu prezentul regulament, ar trebui să se încurajeze instituirea de mecanisme de certificare, precum și de sigilii și mărci în materie de protecție a datelor, care să permită persoanelor vizate să evalueze rapid nivelul de protecție a datelor aferent produselor și serviciilor relevante.
- (101) Fluxurile de date cu caracter personal către și dinspre țări situate în afara Uniunii și organizații internaționale sunt necesare pentru dezvoltarea comerțului internațional și a cooperării internaționale. Creșterea acestor fluxuri a generat noi provocări și preocupări cu privire la protecția datelor cu caracter personal. Cu toate acestea, în cazul în care se transferă date cu caracter personal din Uniune către operatori, persoane împuternicite de operatori sau alți destinatari din țări terțe sau organizații internaționale, nivelul de protecție a persoanelor fizice asigurat în Uniune prin prezentul regulament nu ar trebui să fie diminuat, inclusiv în cazurile de transferuri ulterioare de date cu caracter personal dinspre țara terță sau organizația internațională către operatori, persoane împuternicite de operatori din aceeași sau dintr-o altă țară terță sau organizație internațională. În orice caz, transferurile către țări terțe și organizații internaționale pot fi desfășurate numai în conformitate deplină cu prezentul regulament. Un transfer ar putea avea loc numai dacă, sub rezerva respectării celorlalte dispoziții ale prezentului regulament, operatorul sau persoana împuternicită de operator îndeplinește condițiile prevăzute de dispozițiile prezentului regulament privind transferul de date cu caracter personal către țări terțe sau organizații internaționale.
- (102) Prezentul regulament nu aduce atingere acordurilor internaționale încheiate între Uniune și țări terțe în vederea reglementării transferului de date cu caracter personal, inclusiv garanții adecvate pentru persoanele vizate. Statele membre pot încheia acorduri internaționale care implică transferul de date cu caracter personal către țări terțe sau organizații internaționale, în măsura în care astfel de acorduri nu afectează prezentul regulament și nici alte dispoziții din dreptul Uniunii și includ un nivel corespunzător de protecție a drepturilor fundamentale ale persoanelor vizate.
- (103) Comisia poate decide, cu efect în întreaga Uniune, că o țară terță, un teritoriu sau un anumit sector dintr-o țară terță sau o organizație internațională oferă un nivel adecvat de protecție a datelor, asigurând astfel securitate juridică și uniformitate în Uniune în ceea ce privește țara terță sau organizația internațională care este considerată a furniza un astfel de nivel de protecție. În aceste cazuri, transferurile de date cu caracter personal către țara terță sau organizația internațională respectivă pot avea loc fără a fi necesar să se obțină autorizări suplimentare. De asemenea, Comisia poate să decidă, după trimiterea unei notificări și a unei justificări complete țării terțe sau organizației internaționale, să anuleze o astfel de decizie.
- (104) În conformitate cu valorile fundamentale pe care se întemeiază Uniunea, în special protecția drepturilor omului, Comisia ar trebui, în evaluarea sa referitoare la țara terță sau la un teritoriu sau la un sector specificat dintr-o țară terță, să ia în considerare modul în care aceasta respectă statul de drept, accesul la justiție, precum și normele și standardele internaționale în materie de drepturi ale omului și legislația sa generală și sectorială, inclusiv legislația privind securitatea publică, apărarea și securitatea națională, precum și ordinea publică și dreptul penal. Adoptarea unei decizii privind caracterul adecvat al nivelului de protecție pentru un teritoriu sau un sector specificat dintr-o țară terță ar trebui să țină seama de criterii clare și obiective, cum ar fi activitățile specifice de prelucrare și domeniul de aplicare al standardelor legale aplicabile și legislația în vigoare în țara terță respectivă. Țara terță ar trebui să ofere garanții care să asigure un nivel adecvat de protecție, echivalent în esență cu cel

asigurat în cadrul Uniunii, în special atunci când datele cu caracter personal sunt prelucrate în unul sau mai multe sectoare specifice. În special, țara terță ar trebui să asigure o supraveghere efectivă independentă în materie de protecție a datelor și să prevadă mecanisme de cooperare cu autoritățile statelor membre de protecție a datelor, iar persoanele vizate ar trebui să beneficieze de drepturi efective și opozabile și de reparații efective pe cale administrativă și judiciară.

- (105) Pe lângă angajamentele internaționale asumate de țara terță sau de organizația internațională, Comisia ar trebui să țină seama de obligațiile care decurg din participarea țării terțe sau a organizației internaționale la sistemele multilaterale sau regionale, în special în ceea ce privește protecția datelor cu caracter personal, precum și de punerea în aplicare a unor astfel de obligații. În special, ar trebui să fie luată în considerare aderarea țării terțe la Convenția Consiliului European din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal și protocolul adițional la aceasta. Comisia ar trebui să consulte comitetul atunci când evaluează nivelul de protecție din țările terțe sau din organizațiile internaționale.
- (106) Comisia ar trebui să monitorizeze funcționarea deciziilor privind nivelul de protecție dintr-o țară terță sau un teritoriu sau un anumit sector dintr-o țară terță sau dintr-o organizație internațională și să monitorizeze funcționarea deciziilor adoptate în temeiul articolului 25 alineatul (6) sau al articolului 26 alineatul (4) din Directiva 95/46/CE. În deciziile sale privind caracterul adecvat al nivelului de protecție, Comisia ar trebui să prevadă un mecanism de revizuire periodică a modului lor de funcționare. Această revizuire periodică ar trebui să fie efectuată în consultare cu țara terță sau organizația internațională în cauză și ar trebui să ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională. În scopul monitorizării și al efectuării revizuirilor periodice, Comisia ar trebui să ia în considerare opiniile și constatările Parlamentului European și ale Consiliului, precum și ale altor organisme și surse relevante. Comisia ar trebui să evalueze, într-un termen rezonabil, funcționarea deciziilor din urmă și să raporteze toate constatările relevante comitetului, în sensul Regulamentului (UE) nr. 182/2011 al Parlamentului European și al Consiliului ⁽¹⁾, după cum s-a stabilit în temeiul prezentului regulament, Parlamentului European și Consiliului.
- (107) Comisia poate să recunoască faptul că o țară terță, un teritoriu sau un sector specificat dintr-o țară terță sau o organizație internațională nu mai asigură un nivel adecvat de protecție a datelor. În consecință, transferul de date cu caracter personal către țara terță sau organizația internațională respectivă ar trebui să fie interzis, cu excepția cazului în care sunt îndeplinite cerințele prevăzute în prezentul regulament privind transferurile în baza unor garanții adecvate, inclusiv regulile corporatiste obligatorii și derogările de la situațiile specifice. În acest caz, ar trebui să se prevadă dispoziții pentru consultări între Comisie și astfel de țări terțe sau organizații internaționale. Comisia ar trebui ca, în timp util, să informeze țara terță sau organizația internațională cu privire la aceste motive și să inițieze consultări cu aceasta pentru remedierea situației.
- (108) În absența unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator ar trebui să adopte măsuri pentru a compensa lipsa protecției datelor într-o țară terță prin intermediul unor garanții adecvate pentru persoana vizată. Astfel de garanții adecvate pot consta în utilizarea regulilor corporatiste obligatorii, a clauzelor standard de protecție a datelor adoptate de o autoritate de supraveghere sau a clauzelor contractuale autorizate de o autoritate de supraveghere. Respectivul garanții ar trebui să asigure respectarea cerințelor în materie de protecție a datelor și drepturi ale persoanelor vizate corespunzătoare prelucrării în interiorul Uniunii, inclusiv disponibilitatea unor drepturi opozabile ale persoanelor vizate și a unor căi de atac eficiente, printre care dreptul de acces la reparații efective pe cale administrativă sau judiciară și dreptul de a solicita despăgubiri, în Uniune sau într-o țară terță. Acestea ar trebui să se refere în special la respectarea principiilor generale privind prelucrarea datelor cu caracter personal: principiul protecției datelor începând cu momentul conceperii și principiul protecției implicite a datelor. Transferurile pot fi efectuate și de către autoritățile sau organismele publice cu autorități sau organisme publice în țări terțe sau cu organizații internaționale cu atribuții și funcții corespunzătoare, inclusiv pe baza dispozițiilor care prevăd drepturi opozabile și efective pentru persoanele vizate, care trebuie introduse în acordurile administrative, cum ar fi un memorandum de înțelegere. Autorizația din partea autorității de supraveghere competente ar trebui obținută atunci când garanțiile sunt oferite în cadrul unor acorduri administrative fără caracter juridic obligatoriu.
- (109) Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecție a datelor, adoptate de Comisie sau de o autoritate de supraveghere, nu ar trebui să împiedice operatorii

⁽¹⁾ Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

sau persoanele împuternicite de aceștia să includă clauzele standard în materie de protecție a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator și o altă persoană împuternicită de operator, și nici să adauge alte clauze sau garanții suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de o autoritate de supraveghere sau nu prejudiciază drepturile sau libertățile fundamentale ale persoanelor vizate. Operatorii și persoanele împuternicite de operatori ar trebui să fie încurajați să ofere garanții suplimentare prin intermediul unor angajamente contractuale care să completeze clauzele standard în materie de protecție.

- (110) Un grup de întreprinderi sau un grup de întreprinderi implicat într-o activitate economică comună ar trebui să poată utiliza regulile corporatiste obligatorii aprobate pentru transferurile sale internaționale dinspre Uniune către organizații din cadrul aceluiași grup de întreprinderi sau grup de întreprinderi implicate într-o activitate economică comună, cu condiția ca astfel de reguli corporatiste să includă toate principiile esențiale și drepturile opozabile în scopul asigurării unor garanții adecvate pentru transferurile sau categoriile de transferuri de date cu caracter personal.
- (111) Ar trebui să se prevadă posibilitatea de a se efectua transferuri în anumite circumstanțe în care persoana vizată și-a dat consimțământul explicit, în care transferul este ocazional și necesar în legătură cu un contract sau cu o acțiune în justiție, indiferent dacă este în contextul unei proceduri judiciare sau în contextul unei proceduri administrative sau extrajudiciare, inclusiv în cadrul procedurilor înaintate organismelor de reglementare. De asemenea, ar trebui să se prevadă posibilitatea de a se efectua transferuri în cazul în care motive importante de interes public stabilite de dreptul Uniunii sau de dreptul intern impun acest lucru sau în cazul în care transferul se efectuează dintr-un registru instituit prin lege și destinat să fie consultat de către public sau de către persoane care au un interes legitim. În acest ultim caz, un astfel de transfer nu ar trebui să implice totalitatea datelor cu caracter personal sau ansamblul categoriilor de date conținute în registru, iar atunci când registrul este destinat să fie consultat de persoane care au un interes legitim, transferul ar trebui să fie efectuat doar la cererea persoanelor respective sau dacă acestea sunt destinatarii, luând pe deplin în considerare interesele și drepturile fundamentale ale persoanei vizate.
- (112) Aceste derogări ar trebui să se aplice, în special, transferurilor de date solicitate și necesare din considerente importante de interes public, de exemplu în cazul schimbului internațional de date între autoritățile din domeniul concurenței, administrațiile fiscale sau vamale, între autoritățile de supraveghere financiară, între serviciile competente în materie de securitate socială sau de sănătate publică, de exemplu în cazul depistării punctelor de contact pentru bolile contagioase sau pentru reducerea și/sau eliminarea dopajului în sport. Un transfer de date cu caracter personal ar trebui, de asemenea, să fie considerat legal în cazul în care este necesar în scopul protejării unui interes care este esențial în interesele vitale ale persoanei vizate sau ale unei alte persoane, inclusiv pentru integritatea fizică sau pentru viața acesteia, în cazul în care persoana vizată nu are capacitatea să își dea consimțământul. În absența unei decizii privind caracterul adecvat al nivelului de protecție, dreptul Uniunii sau dreptul intern poate, din considerente importante de interes public, stabili în mod expres limite asupra transferului unor categorii specifice de date către o țară terță sau o organizație internațională. Statele membre ar trebui să notifice Comisiei aceste dispoziții. Orice transfer către o organizație umanitară internațională al datelor cu caracter personal ale unei persoane vizate care se află în incapacitate fizică sau juridică de a își da consimțământul, în vederea îndeplinirii unei sarcini care decurge din Convențiile de la Geneva sau în vederea conformării cu dreptul internațional umanitar aplicabil în conflictele armate, ar putea fi considerat necesar pentru un motiv important de interes public sau pentru că este în interesul vital al persoanei vizate.
- (113) Transferurile care pot fi considerate ca nefiind repetitive și care se referă doar la un număr limitat de persoane vizate, ar putea, de asemenea, să fie efectuate în scopul realizării intereselor legitime urmărite de operator, atunci când asupra respectivelor interese nu prevalează interesele sau drepturile și libertățile persoanei vizate și atunci când operatorul a evaluat toate circumstanțele aferente transferului de date. Operatorul ar trebui să acorde o atenție deosebită naturii datelor cu caracter personal, scopului și duratei operațiunii sau operațiunilor propuse de prelucrare, precum și situației din țara de origine, din țara terță și din țara de destinație finală și ar trebui să ofere garanții adecvate pentru protecția drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Astfel de transferuri ar trebui să fie posibile numai în cazurile reziduale în care nu se poate aplica niciunul dintre celelalte motive de transfer. În ceea ce privește scopurile de cercetare științifică sau istorică sau scopurile statistice, ar trebui să se ia în considerare așteptările legitime ale societății cu privire la creșterea nivelului de cunoștințe. Operatorul ar trebui să informeze autoritatea de supraveghere și persoana vizată cu privire la transfer.
- (114) În orice caz, atunci când Comisia nu a luat o decizie cu privire la nivelul adecvat de protecție a datelor dintr-o țară terță, operatorul sau persoana împuternicită de operator ar trebui să utilizeze soluții care să ofere persoanelor vizate drepturi opozabile și efective în ceea ce privește prelucrarea datelor lor în Uniune odată ce aceste date au fost transferate, astfel încât persoanele vizate să beneficieze în continuare de drepturi fundamentale și garanții.

- (115) Unele țări terțe au adoptat legi, reglementări și alte acte juridice care au drept obiectiv să reglementeze în mod direct activitățile de prelucrare a datelor ale persoanelor fizice și juridice aflate sub jurisdicția statelor membre. Aceasta poate include hotărâri ale instanțelor judecătorești sau decizii ale autorităților administrative din țări terțe care solicită unui operator sau unei persoane împuternicite de operator să transfere sau să divulge date cu caracter personal și care nu se bazează pe un acord internațional, cum ar fi un tratat de asistență juridică reciprocă, în vigoare între țara terță solicitantă și Uniune sau un stat membru. Aplicarea extraterritorială a acestor legi, reglementări și alte acte juridice poate încălca dreptul internațional și poate împiedica asigurarea protecției persoanelor fizice asigurată în Uniune prin prezentul regulament. Transferurile ar trebui să fie permise numai în cazul îndeplinirii condițiilor prevăzute de prezentul regulament pentru un transfer către țări terțe. Acesta ar putea fi cazul, *inter alia*, atunci când divulgarea este necesară dintr-un motiv important de interes public recunoscut în dreptul Uniunii sau în dreptul intern care se aplică operatorului.
- (116) Fluxul transfrontalier de date cu caracter personal în afara Uniunii poate expune unui risc sporit capacitatea persoanelor fizice de a-și exercita drepturile în materie de protecție a datelor, în special pentru a-și asigura protecția împotriva utilizării sau a divulgării ilegale a acestor informații. În același timp, autoritățile de supraveghere pot constata că se află în imposibilitatea de a trata plângeri sau de a efectua investigații referitoare la activitățile desfășurate în afara frontierelor lor. Eforturile acestora de a conlucra în context transfrontalier pot fi, de asemenea, îngreunate de insuficiența competențelor de prevenire sau remediere, de caracterul eterogen al regimurilor juridice și de existența unor obstacole de ordin practic, cum ar fi constrângerile în materie de resurse. Prin urmare, este necesar să se promoveze o cooperare mai strânsă între autoritățile de supraveghere a protecției datelor pentru a putea face schimb de informații și a desfășura investigații împreună cu omologii lor internaționali. În scopul elaborării de mecanisme de cooperare internațională pentru a facilita și a oferi asistență internațională reciprocă în asigurarea aplicării legislației din domeniul protecției datelor cu caracter personal, Comisia și autoritățile de supraveghere ar trebui să facă schimb de informații și să coopereze în cadrul activităților legate de exercitarea competențelor lor cu autoritățile competente din țări terțe, pe bază de reciprocitate și în conformitate cu prezentul regulament.
- (117) Instituirea în statele membre a unor autorități de supraveghere, împuternicite să își îndeplinească sarcinile și să își exercite competențele în deplină independență, este un element esențial al protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Statele membre ar trebui să poată institui mai multe autorități de supraveghere, pentru a reflecta structura lor constituțională, organizatorică și administrativă.
- (118) Independența autorităților de supraveghere nu ar trebui să însemne că autoritățile de supraveghere nu pot face obiectul unor mecanisme de control sau de monitorizare în ceea ce privește cheltuielile acestora sau unui control jurisdicțional.
- (119) În cazul în care un stat membru instituie mai multe autorități de supraveghere, acesta ar trebui să stabilească prin lege mecanisme care să asigure participarea efectivă a autorităților de supraveghere respective la mecanismul pentru asigurarea coerenței. Statul membru respectiv ar trebui, în special, să desemneze autoritatea de supraveghere care îndeplinește funcția de punct unic de contact pentru participarea efectivă a acestor autorități la mecanism, în scopul asigurării unei cooperări rapide și armonioase cu alte autorități de supraveghere, cu comitetul și cu Comisia.
- (120) Fiecare autoritate de supraveghere ar trebui să beneficieze de resurse financiare și umane, de spațiile și de infrastructura necesare pentru îndeplinirea cu eficacitate a sarcinilor lor, inclusiv a celor legate de asistența reciprocă și cooperarea cu alte autorități de supraveghere în întreaga Uniune. Fiecare autoritate de supraveghere ar trebui să aibă un buget public anual separat, care poate face parte din bugetul general de stat sau național.
- (121) Condițiile generale pentru membrul sau membrii autorității de supraveghere ar trebui stabilite de lege în fiecare stat membru și ar trebui, în special, să prevadă că respectivii membri sunt numiți printr-o procedură transparentă fie de parlamentul, de guvernul ori șeful de stat al statului membru pe baza unei propuneri din partea guvernului, a unui membru al guvernului, a parlamentului sau a unei camere a parlamentului, fie de către un organism independent împuternicit prin dreptul intern. În vederea asigurării independenței autorității de supraveghere, membrul sau membrii acesteia ar trebui să acționeze cu integritate, să nu întreprindă acțiuni incompatibile cu îndatoririle lor, iar, pe durata mandatului, ar trebui să nu desfășoare activități incompatibile, remunerate sau nu. Autoritatea de supraveghere ar trebui să aibă personal propriu, ales de autoritatea de supraveghere sau de un organism independent înființat în temeiul dreptului intern, care ar trebui să fie subordonat exclusiv membrului sau membrilor autorității de supraveghere.
- (122) Fiecare autoritate de supraveghere ar trebui să aibă, pe teritoriul statului membru de care aparține, atribuția de a exercita competențele și de a îndeplini sarcinile cu care este investită în conformitate cu prezentul regulament.

Aceasta ar trebui să includă în special prelucrarea în contextul activităților unui sediu al operatorului sau al persoanei împuternicite de operator pe teritoriul propriului stat membru, prelucrarea datelor cu caracter personal efectuată de autoritățile publice sau de organisme private care acționează în interes public, prelucrarea care afectează persoanele vizate de pe teritoriul său sau prelucrarea efectuată de către un operator sau o persoană împuternicită de operator care nu își are sediul în Uniune în cazul în care aceasta privește persoane vizate care își au reședința pe teritoriul său. Aceasta ar trebui să includă tratarea plângerilor depuse de o persoană vizată, efectuarea de investigații privind aplicarea prezentului regulament și promovarea informării publicului cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal.

- (123) Autoritățile de supraveghere ar trebui să monitorizeze aplicarea dispozițiilor prevăzute de prezentul regulament și să contribuie la aplicarea coerentă a acestuia în întreaga Uniune, în scopul asigurării protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal și al facilitării liberei circulații a datelor cu caracter personal în interiorul pieței interne. În acest sens, autoritățile de supraveghere ar trebui să coopereze reciproc, precum și cu Comisia, fără să fie necesar niciun acord între statele membre cu privire la acordarea de asistență reciprocă sau cu privire la respectiva cooperare.
- (124) În cazul în care prelucrarea datelor cu caracter personal se desfășoară în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune, iar operatorul sau persoana împuternicită de operator are sedii în mai multe state membre, sau în cazul în care prelucrarea care se desfășoară în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator din Uniune afectează sau este susceptibilă să afecteze semnificativ persoane vizate din mai multe state membre, autoritatea de supraveghere a sediului principal al operatorului sau al persoanei împuternicite de operator ori a sediului unic al operatorului sau al persoanei împuternicite de operator ar trebui să acționeze în calitate de autoritate principală. Aceasta ar trebui să coopereze cu celelalte autorități vizate, pentru că operatorul sau persoana împuternicită de operator are un sediu pe teritoriul statului lor membru, pentru că persoanele vizate care își au reședința pe teritoriul lor sunt afectate în mod semnificativ sau pentru că le-a fost înaintată o plângere. De asemenea, în cazul în care o persoană vizată care nu își are reședința în statul membru respectiv a depus o plângere, autoritatea de supraveghere la care a fost depusă plângerea ar trebui, de asemenea, să fie o autoritate de supraveghere vizată. În cadrul sarcinilor sale de a emite orientări cu privire la orice chestiune referitoare la punerea în aplicare a prezentului regulament, comitetul ar trebui să poată emite orientări privind, în special, criteriile care trebuie luate în considerare pentru a se stabili dacă prelucrarea în cauză afectează în mod semnificativ persoane vizate din mai multe state membre și privind conținutul unei obiecții relevante și motivate.
- (125) Autoritatea principală ar trebui să aibă competența de a adopta decizii obligatorii privind măsurile de aplicare a competențelor care îi sunt conferite în conformitate cu prezentul regulament. În calitatea sa de autoritate principală, autoritatea de supraveghere ar trebui să implice îndeaproape și să coordoneze activitățile autorităților de supraveghere vizate în procesul decizional. În cazurile în care decizia este de respingere parțială sau totală a plângerii din partea persoanei vizate, o asemenea decizie ar trebui adoptată de către autoritatea de supraveghere la care s-a depus plângerea.
- (126) Decizia ar trebui convenită în comun de autoritatea de supraveghere principală și de autoritățile de supraveghere vizate și ar trebui să vizeze sediul principal sau sediul unic al operatorului sau al persoanei împuternicite de operator și să fie obligatorie pentru operator și pentru persoana împuternicită de operator. Operatorul sau persoana împuternicită de operator ar trebui să ia măsurile necesare pentru a asigura conformitatea cu prezentul regulament și punerea în aplicare a deciziei notificate de autoritatea de supraveghere principală sediului principal al operatorului sau al persoanei împuternicite de operator în ceea ce privește activitățile de prelucrare în Uniune.
- (127) Fiecare autoritate de supraveghere care nu acționează ca autoritate de supraveghere principală ar trebui să aibă competența de a trata cazuri locale, în care operatorul sau persoana împuternicită de operator are sedii în mai multe state membre, dar obiectul respectivei prelucrări privește doar prelucrarea efectuată într-un singur stat membru și implicând doar persoane vizate din acel unic stat membru, de exemplu în cazul în care obiectul îl constituie prelucrarea datelor cu caracter personal ale angajaților în contextul specific legat de forța de muncă dintr-un stat membru. În astfel de cazuri, autoritatea de supraveghere ar trebui să informeze fără întârziere autoritatea de supraveghere principală cu privire la această chestiune. După ce a fost informată, autoritatea de supraveghere principală ar trebui să decidă dacă va trata ea însăși cazul în temeiul dispoziției privind cooperarea între autoritatea de supraveghere principală și alte autorități de supraveghere vizate („mecanismul ghișeului unic”), sau dacă autoritatea de supraveghere care a informat-o ar trebui să se ocupe de caz la nivel local. Atunci când decide dacă va trata cazul, autoritatea de supraveghere principală ar trebui să ia în considerare dacă există un sediu al operatorului sau al persoanei împuternicite de operator în statul membru al autorității de supraveghere care a informat-o, în vederea garantării respectării efective a unei decizii în ceea ce privește operatorul sau persoana împuternicită de operator. În cazul în care autoritatea de supraveghere principală decide să trateze

cazul, autoritatea de supraveghere care a informat-o ar trebui să beneficieze de posibilitatea de a prezenta un proiect de decizie, de care autoritatea de supraveghere principală ar trebui să țină seama în cea mai mare măsură atunci când pregătește proiectul său de decizie în cadrul respectivului mecanism al ghișeului unic.

- (128) Normele privind autoritatea de supraveghere principală și mecanismul ghișeului unic nu ar trebui să se aplice în cazul în care prelucrarea este efectuată de autorități publice sau organisme private în interes public. În asemenea cazuri, singura autoritate de supraveghere competentă să își exercite competențele care i-au fost atribuite în conformitate cu prezentul regulament ar trebui să fie autoritatea de supraveghere a statului membru în care autoritatea publică sau organismul privat își are sediul.
- (129) Pentru a se asigura consecvența monitorizării și a aplicării prezentului regulament în întreaga Uniune, autoritățile de supraveghere ar trebui să aibă în fiecare stat membru aceleași sarcini și competențe efective, inclusiv competențe de investigare, competențe corective și sancțiuni, precum și competențe de autorizare și de consiliere, în special în cazul plângerilor depuse de persoane fizice, precum și, fără a aduce atingere competențelor autorităților de urmărire penală în temeiul dreptului intern, de a aduce în atenția autorităților judiciare cazurile de încălcare a prezentului regulament și de a se implica în proceduri judiciare. Aceste competențe ar trebui să includă și competența de a impune o limitare temporară sau definitivă, inclusiv o interdicție, asupra prelucrării. Statele membre pot stabili alte sarcini legate de protecția datelor cu caracter personal în temeiul prezentului regulament. Competențele autorităților de supraveghere ar trebui exercitate în conformitate cu garanții procedurale adecvate prevăzute în dreptul Uniunii și în dreptul intern, în mod imparțial, echitabil și într-un termen rezonabil. În special, fiecare măsură ar trebui să fie adecvată, necesară și proporțională în scopul de a asigura conformitatea cu dispozițiile prezentului regulament, luând în considerare circumstanțele fiecărui caz în parte, să respecte dreptul oricărei persoane de a fi ascultată înainte de luarea oricărei măsuri individuale care ar putea să îi aducă atingere și să evite costurile inutile și inconvenientele excesive pentru persoanele în cauză. Competențele de investigare în ceea ce privește accesul în incinte ar trebui exercitate în conformitate cu cerințele specifice din dreptul procedural național, cum ar fi obligația de a obține în prealabil o autorizare judiciară. Fiecare măsură obligatorie din punct de vedere juridic luată de autoritatea de supraveghere ar trebui să fie prezentată în scris, să fie clară și lipsită de ambiguitate, să indice autoritatea de supraveghere care a emis măsura, data emiterii măsurii, să poarte semnătura șefului sau a unui membru al autorității de supraveghere autorizat de acesta, să furnizeze motivele pentru care s-a luat măsura și să facă trimitere la dreptul la o cale de atac eficientă. Acest lucru nu ar trebui să excludă cerințe suplimentare în conformitate cu dreptul procedural național. Adoptarea unor astfel de decizii obligatorii din punct de vedere juridic implică faptul că se poate da naștere unui control jurisdicțional în statul membru al autorității de supraveghere care a adoptat decizia.
- (130) În cazul în care autoritatea de supraveghere la care s-a depus plângerea nu este autoritatea de supraveghere principală, autoritatea de supraveghere principală ar trebui să coopereze îndeaproape cu autoritatea de supraveghere la care s-a depus plângerea, în conformitate cu dispozițiile privind cooperarea și consecvența prevăzute în prezentul regulament. În astfel de cazuri, autoritatea de supraveghere principală ar trebui, atunci când ia măsuri destinate să producă efecte juridice, inclusiv impunerea de amenzi administrative, să țină seama cât mai mult posibil de opinia autorității de supraveghere la care a fost depusă plângerea și care ar trebui să își mențină competența de a desfășura orice investigație pe teritoriul propriului stat membru, în colaborare cu autoritatea de supraveghere principală.
- (131) În cazurile în care o altă autoritate de supraveghere ar trebui să acționeze în calitate de autoritate de supraveghere principală pentru activitățile de prelucrare ale operatorului sau ale persoanei împuternicite de operator, dar obiectul concret al unei plângeri sau posibila încălcare vizează numai activitățile de prelucrare ale operatorului sau ale persoanei împuternicite de operator în statul membru în care a fost depusă plângerea sau a fost depistată posibila încălcare, iar chestiunea nu afectează în mod substanțial sau nu este susceptibilă să afecteze în mod substanțial persoane vizate din alte state membre, autoritatea de supraveghere care a primit o plângere sau a depistat ori a fost informată în alt mod asupra unor situații de posibile încălcări ale prezentului regulament ar trebui să încerce o soluționare pe cale amiabilă cu operatorul și, în cazul în care aceasta eșuează, să își exercite plenitudinea competențelor. Aceasta ar trebui să includă activități specifice de prelucrare efectuate pe teritoriul statului membru al autorității de supraveghere ori cu privire la persoane vizate de pe teritoriul aceluși stat membru, activități de prelucrare care au loc în contextul unei oferte de bunuri sau servicii destinate în mod special persoanelor vizate pe teritoriul statului membru al autorității de supraveghere sau activități de prelucrare care trebuie evaluate ținând seama de obligațiile juridice relevante în temeiul dreptului intern.
- (132) Activitățile de creștere a gradului de conștientizare organizate pentru public de autoritățile de supraveghere ar trebui să includă măsuri specifice care să vizeze operatorii și persoanele împuternicite de operatori, inclusiv microîntreprinderile și întreprinderile mici și mijlocii, precum și persoanele fizice, în special în context educațional.

- (133) Autoritățile de supraveghere ar trebui să își acorde reciproc asistență în îndeplinirea sarcinilor care le revin, pentru a se asigura coerența aplicării prezentului regulament pe piața internă. O autoritate de supraveghere care solicită asistență reciprocă poate adopta o măsură provizorie în cazul în care nu primește un răspuns la o solicitare de asistență reciprocă în termen de o lună de la primirea solicitării de către cealaltă autoritate de supraveghere.
- (134) Fiecare autoritate de supraveghere ar trebui să participe, după caz, la operațiuni comune între autoritățile de supraveghere. Autoritatea de supraveghere căreia i s-a adresat solicitarea ar trebui să aibă obligația de a răspunde cererii într-un anumit termen.
- (135) Pentru a se asigura aplicarea coerentă a prezentului regulament în întreaga Uniune, ar trebui să se instituie un mecanism pentru asigurarea coerenței în cadrul căruia autoritățile de supraveghere să coopereze. Acest mecanism ar trebui să se aplice, în special, în cazul în care o autoritate de supraveghere intenționează să adopte o măsură prevăzută a produce efecte juridice în ceea ce privește operațiunile de prelucrare care afectează în mod substanțial un număr semnificativ de persoane vizate din mai multe state membre. Mecanismul ar trebui să se aplice, de asemenea, în cazul în care o autoritate de supraveghere vizată sau Comisia solicită ca aspectul respectiv să fie tratat în cadrul mecanismului pentru asigurarea coerenței. Acest mecanism nu ar trebui să aducă atingere măsurilor pe care Comisia le poate adopta în exercitarea competențelor care îi revin în temeiul tratatelor.
- (136) În aplicarea mecanismului pentru asigurarea coerenței, comitetul ar trebui, într-un anumit termen, să emită un aviz în cazul în care o majoritate a membrilor săi decide astfel sau în cazul în care orice autoritate de supraveghere vizată sau Comisia solicită acest lucru. Comitetul ar trebui, de asemenea, să fie împuternicit să adopte decizii obligatorii din punct de vedere juridic în cazul unor litigii între autoritățile de supraveghere. În acest scop, acesta ar trebui să emită, în principiu cu o majoritate de două treimi din membrii săi, decizii obligatorii din punct de vedere juridic, în cazuri bine definite, în cazul în care există opinii divergente între autoritățile de supraveghere, în special în cadrul mecanismului de cooperare între autoritatea de supraveghere principală și autoritățile de supraveghere vizate privind fondul cauzei, în special existența sau nu a unei încălcări a prezentului regulament.
- (137) Este posibil să existe o necesitate urgentă de a se acționa pentru asigurarea protecției drepturilor și libertăților persoanelor vizate, în special în cazul în care există pericolul ca exercitarea unui drept al unei persoane vizate să fie împiedicată în mod considerabil. Prin urmare, o autoritate de supraveghere ar trebui să poată adopta măsuri provizorii pe teritoriul său, justificate în mod corespunzător, având o perioadă de valabilitate determinată care nu ar trebui să depășească trei luni.
- (138) Aplicarea unui astfel de mecanism ar trebui să constituie o condiție pentru legalitatea unei măsuri destinate să producă efecte juridice, luate de o autoritate de supraveghere, în cazurile în care aplicarea acesteia este obligatorie. În alte cazuri cu relevanță transfrontalieră, ar trebui pus în aplicare mecanismul de cooperare între autoritatea de supraveghere principală și autoritățile de supraveghere vizate, iar între autoritățile de supraveghere vizate s-ar putea acorda asistență reciprocă și s-ar putea desfășura operațiuni comune pe bază bilaterală sau multilaterală, fără declanșarea mecanismului pentru asigurarea coerenței.
- (139) Cu scopul de a promova aplicarea coerentă a prezentului regulament, comitetul ar trebui instituit ca organ independent al Uniunii. Pentru a-și îndeplini obiectivele, comitetul ar trebui să aibă personalitate juridică. Comitetul ar trebui să fie reprezentat de președintele său. Acesta ar trebui să înlocuiască Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, instituit prin Directiva 95/46/CE. Acesta ar trebui să fie alcătuit din șefii autorităților de supraveghere din fiecare stat membru și din Autoritatea Europeană pentru Protecția Datelor sau reprezentanții acestora. Comisia ar trebui să participe la activitățile comitetului fără a avea drept de vot, iar Autoritatea Europeană pentru Protecția Datelor ar trebui să aibă drepturi de vot speciale. Comitetul ar trebui să contribuie la aplicarea coerentă a prezentului regulament în întreaga Uniune, inclusiv prin oferirea de consiliere Comisiei, în special cu privire la nivelul de protecție în țările terțe și în cadrul organizațiilor internaționale, și prin promovarea cooperării autorităților de supraveghere în întreaga Uniune. Comitetul ar trebui să acționeze în mod independent în îndeplinirea sarcinilor sale.
- (140) Comitetul ar trebui să fie asistat de un secretariat asigurat de Autoritatea Europeană pentru Protecția Datelor. Personalul Autorității Europene pentru Protecția Datelor implicat în îndeplinirea sarcinilor conferite comitetului în temeiul prezentului regulament ar trebui să își îndeplinească sarcinile exclusiv conform instrucțiunilor președintelui comitetului și să raporteze acestuia.
- (141) Orice persoană vizată ar trebui să aibă dreptul de a depune o plângere la o singură autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, precum și dreptul la o cale de atac eficientă în

conformitate cu articolul 47 din cartă, în cazul în care persoana vizată consideră că drepturile sale în temeiul prezentului regulament sunt încălcate sau în cazul în care autoritatea de supraveghere nu reacționează la o plângere, respinge sau refuză parțial sau total o plângere sau nu acționează atunci când o astfel de acțiune este necesară pentru asigurarea protecției drepturilor persoanei vizate. Investigația în urma unei plângeri ar trebui să fie efectuată, sub control judiciar, în măsura în care este necesar, în funcție de caz. Autoritatea de supraveghere ar trebui să informeze persoana vizată cu privire la evoluția și soluționarea plângerii într-un termen rezonabil. În eventualitatea în care cazul necesită o investigație suplimentară sau coordonarea cu o altă autoritate de supraveghere, ar trebui să se furnizeze informații intermediare persoanei vizate. În vederea facilitării depunerii plângerilor, fiecare autoritate de supraveghere ar trebui să ia măsuri precum punerea la dispoziție a unui formular de depunere a plângerii, care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.

- (142) În cazul în care persoana vizată consideră că drepturile sale în temeiul prezentului regulament sunt încălcate, aceasta ar trebui să aibă dreptul de a mandata un organism, o organizație sau o asociație fără scop lucrativ care este înființat(ă) în conformitate cu dreptul intern, ale cărui (cărei) obiective statutare sunt în interesul public și care își desfășoară activitatea în domeniul asigurării protecției datelor cu caracter personal, să depună o plângere în numele său la o autoritate de supraveghere, să exercite dreptul la o cale de atac în numele persoanelor vizate sau, în cazul în care se prevede în dreptul intern, să exercite dreptul de a primi despăgubiri în numele persoanelor vizate. Un stat membru poate prevedea ca un astfel de organism, organizație sau asociație să aibă dreptul de a depune o plângere în statul membru respectiv, independent de mandatul acordat de o persoană vizată, și să aibă dreptul la o cale de atac eficientă în cazul în care are motive să considere că drepturile unei persoane vizate au fost încălcate ca rezultat al unei prelucrări a datelor cu caracter personal care încalcă prezentul regulament. Organismul, organizația sau asociația în cauza nu poate pretinde despăgubiri în numele unei persoane vizate, independent de mandatul acordat de persoana vizată.
- (143) Orice persoană fizică sau juridică are dreptul de a introduce o acțiune în anulare împotriva deciziilor comitetului în fața Curții de Justiție, în conformitate cu condițiile prevăzute la articolul 263 din TFUE. În calitate de destinatar ale acestor decizii, autoritățile de supraveghere vizate care doresc să le conteste trebuie să introducă o acțiune împotriva deciziilor respective în termen de două luni de la data la care le-au fost notificate, în conformitate cu articolul 263 din TFUE. În cazul în care deciziile comitetului vizează în mod direct și individual un operator, o persoană împuternicită de operator sau reclamantul, aceștia din urmă pot introduce o acțiune în anularea respectivelor decizii în termen de două luni de la publicarea acestora pe site-ul comitetului, în conformitate cu articolul 263 din TFUE. Fără a aduce atingere acestui drept în temeiul articolului 263 din TFUE, orice persoană fizică sau juridică ar trebui să aibă dreptul la o cale de atac judiciară eficientă în fața instanței naționale competente împotriva unei decizii a unei autorități de supraveghere care produce efecte juridice privind respectiva persoană. O astfel de decizie se referă în special la exercitarea competențelor de investigare, corective și de autorizare de către autoritatea de supraveghere sau la refuzul sau respingerea plângerilor. Cu toate acestea, dreptul la o cale de atac judiciară eficientă nu include măsuri ale autorităților de supraveghere care nu sunt obligatorii din punct de vedere juridic, cum ar fi avizele emise de autoritatea de supraveghere sau consiliere furnizată de aceasta. Acțiunile împotriva unei autorități de supraveghere ar trebui să fie aduse în fața instanțelor statului membru în care este stabilită autoritatea de supraveghere și ar trebui să se desfășoare în conformitate cu dreptul procesual al statului membru respectiv. Respectivul instanțe ar trebui să își exercite competența judiciară deplină, care ar trebui să includă competența de a examina toate aspectele de fapt sau de drept care au relevanță pentru litigiul cu care acestea sunt sesizate.

În cazul în care o plângere a fost respinsă sau refuzată de o autoritate de supraveghere, reclamantul poate introduce o acțiune la instanțele din același stat membru. În contextul căilor de atac judiciare privind aplicarea prezentului regulament, instanțele naționale care consideră necesară o decizie privind chestiunea respectivă pentru a le permite să ia o hotărâre pot sau, în cazul prevăzut la articolul 267 din TFUE, trebuie să solicite Curții de Justiție să pronunțe o decizie preliminară privind interpretarea dreptului Uniunii, inclusiv a prezentului regulament. În plus, în cazul în care o decizie a unei autorități de supraveghere care pune în aplicare o decizie a comitetului este contestată în fața unei instanțe naționale și este în discuție validitatea deciziei comitetului, respectiva instanță națională nu are competența de a declara nulă decizia comitetului, ci trebuie să aducă chestiunea validității în fața Curții de Justiție, în conformitate cu articolul 267 din TFUE, astfel cum a fost interpretat de Curtea de Justiție, ori de câte ori instanța națională consideră decizia nulă. Cu toate acestea, o instanță națională nu poate să transmită o chestiune cu privire la validitatea deciziei comitetului la cererea unei persoane fizice sau juridice care a avut posibilitatea de a introduce o acțiune în anulare împotriva respectivei decizii, în special dacă aceasta era vizată în mod direct și individual de decizia în cauză, dar nu a făcut acest lucru în termenul prevăzut la articolul 263 din TFUE.

- (144) Atunci când o instanță sesizată cu o procedură împotriva unei decizii a unei autorități de supraveghere are motive să creadă că în fața unei instanțe competente dintr-un alt stat membru au fost introduse proceduri cu privire la aceeași prelucrare, cum ar fi același obiect al prelucrării, de către același operator sau aceeași persoană împuternicită de operator, sau aceeași cauză, instanța respectivă ar trebui să contacteze cea de a doua instanță pentru a confirma existența unor astfel de proceduri conexe. În cazul în care aceste proceduri conexe se află pe

rolul unei instanțe dintr-un alt stat membru, orice instanță, cu excepția celei sesizate inițial, poate să își suspende procedurile sau, la cererea uneia dintre părți, își poate declina competența în favoarea instanței sesizate inițial, cu condiția ca aceasta din urmă să aibă competența de a soluționa procedurile în cauză și ca dreptul care i se aplică să îi permită consolidarea acestor proceduri conexe. Procedurile sunt considerate conexe atunci când sunt atât de strâns legate între ele încât este oportună instrumentarea și judecarea lor în același timp pentru a se evita riscul pronunțării unor hotărâri ireconciliabile în cazul judecării lor în mod separat.

- (145) În ceea ce privește acțiunile inițiate împotriva unui operator sau unei persoane împuternicite de operator, reclamantul ar trebui să aibă posibilitatea de a introduce acțiunea în fața instanțelor din statele membre în care operatorul sau persoana împuternicită de operator are un sediu sau în care persoana vizată își are reședința, cu excepția cazului în care operatorul este o autoritate publică dintr-un stat membru ce acționează în exercitarea competențelor sale publice.
- (146) Operatorul sau persoana împuternicită de operator ar trebui să plătească despăgubiri pentru orice prejudiciu pe care o persoană îl poate suferi ca urmare a unei prelucrări care încalcă prezentul regulament. Operatorul sau persoana împuternicită de operator ar trebui să fie exonerată de răspundere dacă dovedesc că nu sunt în niciun fel răspunzători pentru prejudiciu. Conceptul de prejudiciu ar trebui interpretat în sens larg, din perspectiva jurisprudenței Curții de Justiție, într-un mod care să reflecte pe deplin obiectivele prezentului regulament. Această dispoziție nu aduce atingere niciunei cereri de despăgubire care rezultă din încălcarea altor norme din dreptul Uniunii sau din dreptul intern. O prelucrare care încalcă prezentul regulament include și prelucrarea care încalcă actele delegate și de punere în aplicare adoptate în conformitate cu prezentul regulament și cu dreptul intern care specifică norme din prezentul regulament. Persoanele vizate ar trebui să primească despăgubiri integrale și eficiente pentru prejudiciul pe care le-au suferit. În cazul în care operatorii sau persoanele împuternicite de operatori sunt implicate în aceeași prelucrare, fiecare operator sau fiecare persoană împuternicită de operator ar trebui să fie considerată răspunzătoare pentru întregul prejudiciu. Cu toate acestea, atunci când procedurile juridice care le vizează sunt conexe, în conformitate cu dreptul intern, despăgubirile pot fi împărțite în funcție de răspunderea fiecărui operator sau a fiecărei persoane împuternicite de operator, cu condiția să se asigure despăgubirea integrală și efectivă a persoanei vizate care a suferit prejudiciul. Orice operator sau persoană împuternicită de operator care a plătit despăgubiri integrale poate formula ulterior o acțiune în regres împotriva altor operatori sau persoane împuternicite de operatori implicate în aceeași prelucrare.
- (147) În cazul în care prezentul regulament cuprinde norme specifice privind competența judiciară, în special în ceea ce privește căile de atac judiciare, inclusiv acțiunile în despăgubiri, împotriva unui operator sau a unei persoane împuternicite de operator, normele generale privind competența judiciară precum cele din Regulamentul (UE) nr. 1215/2012 al Parlamentului European și al Consiliului ⁽¹⁾ nu ar trebui să aducă atingere aplicării unor astfel de norme specifice.
- (148) Pentru a consolida respectarea aplicării normelor prevăzute în prezentul regulament, ar trebui impuse sancțiuni, inclusiv amenzi administrative, pentru orice încălcare a prezentului regulament, pe lângă sau în locul măsurilor adecvate impuse de autoritatea de supraveghere în temeiul prezentului regulament. În cazul unei încălcări minore sau în cazul în care amenda susceptibilă de a fi impusă ar constitui o sarcină disproporționată pentru o persoană fizică, poate fi emis un avertisment în locul unei amenzi. Cu toate acestea, ar trebui să se ia în considerare în mod corespunzător natura, gravitatea și durata încălcării, caracterul deliberat al încălcării, acțiunile întreprinse pentru a reduce prejudiciul cauzat, gradul de răspundere sau orice încălcări anterioare relevante, modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, conformitatea cu măsurile adoptate împotriva operatorului sau a persoanei împuternicite de operator, aderarea la un cod de conduită și orice alt factor agravant sau atenuant. Impunerea de sancțiuni, inclusiv de amenzi administrative, ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu carta, inclusiv o protecție judiciară eficientă și un proces echitabil.
- (149) Statele membre ar trebui să poată stabili normele privind sancțiunile penale pentru încălcările prezentului regulament, inclusiv pentru încălcarea normelor de drept intern adoptate în temeiul și în limitele prezentului regulament. Respectivul sancțiuni penale pot, de asemenea, permite privarea de profiturile obținute prin încălcarea prezentului regulament. Cu toate acestea, impunerea de sancțiuni penale pentru încălcări ale unor asemenea norme de drept intern și de sancțiuni administrative nu ar trebui să ducă la încălcarea principiului *ne bis in idem*, astfel cum a fost interpretat de Curtea de Justiție.
- (150) Pentru consolidarea și armonizarea sancțiunilor administrative în cazul încălcării prezentului regulament, fiecare autoritate de supraveghere ar trebui să aibă competența de a impune amenzi administrative. Prezentul regulament

⁽¹⁾ Regulamentul (UE) nr. 1215/2012 al Parlamentului European și al Consiliului din 12 decembrie 2012 privind competența judiciară, recunoașterea și executarea hotărârilor în materie civilă și comercială (JO L 351, 20.12.2012, p. 1).

ar trebui să indice încălcările, și limita maximă și criteriile pentru stabilirea amenzilor administrative aferente, care ar trebui să fie stabilite de autoritatea de supraveghere competentă în fiecare caz în parte, ținând seama de toate circumstanțele relevante ale situației specifice, luându-se în considerare în mod corespunzător, în special, natura, gravitatea și durata încălcării, precum și consecințele acesteia și măsurile luate pentru a se asigura respectarea obligațiilor în temeiul prezentului regulament și pentru a se preveni sau atenua consecințele încălcării. În cazul în care amenzile administrative sunt impuse unei întreprinderi, o întreprindere ar trebui înțeleasă ca fiind o întreprindere în conformitate cu articolele 101 și 102 din TFUE în aceste scopuri. În cazul în care se impun amenzi administrative unor persoane care nu sunt întreprinderi, autoritatea de supraveghere ar trebui să țină seama de nivelul general al veniturilor din statul membru respectiv, precum și de situația economică a persoanei atunci când estimează cuantumul adecvat al amenzii. Mecanismul pentru asigurarea coerenței poate fi, de asemenea, utilizat pentru a promova aplicarea consecventă a amenzilor administrative. Competența de a stabili dacă și în ce măsură autoritățile publice ar trebui să facă obiectul unor amenzi administrative ar trebui să revină statelor membre. Impunerea unei amenzi administrative sau transmiterea unei avertizări nu afectează aplicarea altor competențe ale autorităților de supraveghere sau a altor sancțiuni în temeiul prezentului regulament.

- (151) Sistemele juridice ale Danemarcei și Estoniei nu permit amenzi administrative astfel cum sunt prevăzute în prezentul regulament. Normele privind amenzile administrative pot fi aplicate astfel încât, în Danemarca, amenda să fie impusă de instanțele naționale competente ca sancțiune penală, iar în Estonia amenda să fie impusă de autoritatea de supraveghere în cadrul unei proceduri privind delictele, cu condiția ca o astfel de aplicare a normelor în statele membre respective să aibă un efect echivalent cu cel al amenzilor administrative impuse de autoritățile de supraveghere. Prin urmare, instanțele naționale competente ar trebui să țină seama de recomandarea autorității de supraveghere care a inițiat amenda. În orice caz, amenzile impuse ar trebui să fie eficiente, proporționale și disuasive.
- (152) În cazul în care prezentul regulament nu armonizează sancțiunile administrative sau în alte cazuri, acolo unde este necesar, de exemplu în cazul unor încălcări grave ale prezentului regulament, statele membre ar trebui să pună în aplicare un sistem care să prevadă sancțiuni eficiente, proporționale și disuasive. Natura unor astfel de sancțiuni, penale sau administrative, ar trebui stabilită în dreptul intern.
- (153) Dreptul statelor membre ar trebui să stabilească un echilibru între normele care reglementează libertatea de exprimare și de informare, inclusiv exprimarea jurnalistică, academică, artistică și/sau literară, și dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament. Prelucrarea datelor cu caracter personal exclusiv în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare ar trebui să facă obiectul unor derogări sau al unor excepții de la anumite dispoziții ale prezentului regulament în cazul în care este necesară stabilirea unui echilibru între dreptul la protecția datelor cu caracter personal și dreptul la libertatea de exprimare și de informare, astfel cum este prevăzut în articolul 11 din cartă. Acest lucru ar trebui să se aplice în special prelucrării datelor cu caracter personal în domeniul audiovizualului, precum și în arhivele de știri și în bibliotecile ziarelor. Prin urmare, statele membre ar trebui să adopte măsuri legislative care să prevadă excepțiile și derogările necesare în vederea asigurării echilibrului între aceste drepturi fundamentale. Statele membre ar trebui să adopte astfel de excepții și derogări în ceea ce privește principiile generale, drepturile persoanelor vizate, operatorul și persoana împuternicită de operator, transferul de date cu caracter personal către țări terțe sau organizații internaționale, autoritățile de supraveghere independente, cooperarea și coerența, precum și în ceea ce privește situații specifice de prelucrare a datelor. În cazul în care aceste excepții sau derogări diferă de la un stat membru la altul, ar trebui să se aplice dreptul statului membru sub incidența căruia intră operatorul. Pentru a ține seama de importanța dreptului la libertatea de exprimare în fiecare societate democratică, este necesar ca noțiunile legate de această libertate, cum ar fi jurnalismul, să fie interpretate în sens larg.
- (154) Prezentul regulament permite luarea în considerare a principiului accesului public la documente oficiale în aplicarea prezentului regulament. Accesul public la documente oficiale poate fi considerat a fi în interes public. Datele cu caracter personal din documentele deținute de o autoritate publică sau de un organism public ar trebui să poată fi divulgate de autoritatea respectivă sau de organismul respectiv în cazul în care dreptul Uniunii sau dreptul intern sub incidența căruia intră autoritatea publică sau organismul public prevede acest lucru. Dreptul Uniunii și dreptul intern ar trebui să asigure un echilibru între accesul public la documentele oficiale și reutilizarea informațiilor din sectorul public, pe de o parte, și dreptul la protecția datelor cu caracter personal, pe de altă parte, și ar putea prin urmare să prevadă echilibrul necesar cu dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament. Trimiterea la autoritățile și organismele publice ar trebui, în acest context, să includă toate autoritățile sau alte organisme reglementate de dreptul intern privind accesul public la documente. Directiva 2003/98/CE a Parlamentului European și a Consiliului ⁽¹⁾ lasă intact și nu aduce atingere în niciun fel nivelului de protecție a persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal

⁽¹⁾ Directiva 2003/98/CE a Parlamentului European și a Consiliului din 17 noiembrie 2003 privind reutilizarea informațiilor din sectorul public (JO L 345, 31.12.2003, p. 90).

în conformitate cu dreptul Uniunii și cu cel intern și, în special, nu modifică drepturile și obligațiile prevăzute de prezentul regulament. În special, directiva sus-menționată nu se aplică documentelor la care accesul este exclus sau restrâns în temeiul regimurilor de acces din motive legate de protecția datelor cu caracter personal și nici părților din documente accesibile în temeiul respectivelor regimuri care conțin date cu caracter personal a căror reutilizare a fost stabilită prin lege ca fiind incompatibilă cu dreptul privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

- (155) Dreptul intern sau acordurile colective, inclusiv „acordurile de muncă”, pot prevedea norme specifice care să reglementeze prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă, în special condițiile în care datele cu caracter personal în contextul ocupării unui loc de muncă pot fi prelucrate pe baza consimțământului angajatului, în scopul recrutării, al respectării clauzelor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii, al egalității și diversității la locul de muncă, al asigurării sănătății și securității la locul de muncă, precum și în scopul exercitării și beneficiii, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și în scopul încetării raporturilor de muncă.
- (156) Prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ar trebui să facă obiectul unor garanții adecvate pentru drepturile și libertățile persoanei vizate în temeiul prezentului regulament. Respectivul garanții ar trebui să asigure faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, principiul reducerii la minimum a datelor. Prelucrarea ulterioară a datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice se efectuează atunci când operatorul a evaluat fezabilitatea pentru îndeplinirea acestor obiective prin prelucrarea unor date cu caracter personal care nu permit sau nu mai permit identificarea persoanelor vizate, cu condiția să existe garanții adecvate (cum ar fi pseudonimizarea datelor cu caracter personal). Statele membre ar trebui să prevadă garanții adecvate pentru prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. Statele membre ar trebui să fie autorizate să ofere, în anumite condiții și sub rezerva unor garanții adecvate pentru persoanele vizate, precizări și derogări în ceea ce privește cererile de informații și dreptul la rectificare, dreptul la ștergere, dreptul de a fi uitat, dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, precum și dreptul la opoziție în cazul prelucrării datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. Condițiile și garanțiile în cauză pot genera proceduri specifice astfel încât persoanele vizate să își exercite respectivele drepturi dacă acest lucru este adecvat în contextul scopurilor vizate de prelucrarea specifică, precum și măsuri tehnice și organizaționale vizând reducerea la minimum a prelucrării datelor cu caracter personal, în conformitate cu principiile proporționalității și necesității. Prelucrarea datelor cu caracter personal în scopuri științifice ar trebui să fie, de asemenea, conformă cu alte acte legislative relevante, cum ar fi cele privind studiile clinice.
- (157) Prin combinarea informațiilor din registre, cercetătorii pot obține noi cunoștințe de mare valoare în ceea ce privește bolile cu largă răspândire, cum ar fi bolile cardiovasculare, cancerul și depresia. Pe baza registrelor, rezultatele cercetărilor pot fi întărite, întrucât acestea se bazează pe o populație mai mare. În domeniul științelor sociale, cercetarea pe baza registrelor le permite cercetătorilor să obțină informații esențiale despre corelarea pe termen lung a unei serii de condiții sociale, precum șomajul sau educația, cu alte condiții de viață. Rezultatele cercetărilor obținute pe baza registrelor furnizează cunoștințe solide, de înaltă calitate, care pot constitui baza pentru elaborarea și punerea în aplicare a unor politici bazate pe cunoaștere și care pot îmbunătăți calitatea vieții pentru un număr de persoane, eficiența serviciilor sociale. Pentru a facilita cercetarea științifică, datele cu caracter personal pot fi prelucrate în scopuri de cercetare științifică, sub rezerva condițiilor și a garanțiilor corespunzătoare stabilite în dreptul Uniunii sau în dreptul intern.
- (158) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare, prezentul regulament ar trebui să se aplice și prelucrării respective, ținând seama de faptul că prezentul regulament nu ar trebui să se aplice persoanelor decedate. Autoritățile publice sau organismele publice sau private care dețin evidențe de interes public ar trebui, în temeiul dreptului Uniunii sau al dreptului național, să aibă o obligație legală de a dobândi, a păstra, a evalua, a pregăti, a descrie, a comunica, a promova, a disemina și a asigura accesul la evidențe de valoare durabilă de interes public general. Statele membre ar trebui, de asemenea, să poată să prevadă prelucrarea ulterioară a datelor cu caracter personal în scopuri de arhivare, de exemplu cu scopul de a furniza informații specifice referitoare la comportamentul politic în perioada fostelor regimuri de stat totalitare, la genociduri, la crime împotriva umanității, în special holocaustul, sau la crime de război.

- (159) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică, prezentul regulament ar trebui să se aplice și prelucrării respective. În sensul prezentului regulament, prelucrarea datelor cu caracter personal în scopuri de cercetare științifică ar trebui să fie interpretată în sens larg, incluzând de exemplu dezvoltarea tehnologică și activitățile demonstrative, cercetarea fundamentală, cercetarea aplicată și cercetarea finanțată din surse private. Ar trebui, în plus, luat în considerare obiectivul Uniunii de creare a unui Spațiu european de cercetare, astfel cum este menționat la articolul 179 alineatul (1) din TFUE. Scopurile de cercetare științifică ar trebui să includă, de asemenea, studii efectuate în interes public în domeniul sănătății publice. Pentru a îndeplini caracteristicile specifice ale prelucrării datelor cu caracter personal în scopuri de cercetare științifică, ar trebui să se aplice condiții specifice, în special în ceea ce privește publicarea sau divulgarea într-un alt mod a datelor cu caracter personal în contextul scopurilor de cercetare științifică. În cazul în care rezultatul cercetării științifice, în special în contextul sănătății, constituie un motiv pentru măsuri suplimentare în interesul persoanei vizate, normele generale ale prezentului regulament ar trebui să se aplice având în vedere aceste măsuri.
- (160) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare istorică, prezentul regulament ar trebui să se aplice și prelucrării respective. Acest lucru ar trebui să includă, de asemenea, cercetarea istorică și cercetarea în scopuri genealogice, ținând seama de faptul că prezentul regulament nu ar trebui să se aplice persoanelor decedate.
- (161) În scopul acordării consimțământului de a participa la activități de cercetare științifică în cadrul testelor clinice, ar trebui să se aplice dispozițiile relevante ale Regulamentului (UE) nr. 536/2014 al Parlamentului European și al Consiliului ⁽¹⁾.
- (162) În cazul în care datele cu caracter personal sunt prelucrate în scopuri statistice, prezentul regulament ar trebui să se aplice prelucrării respective. Dreptul Uniunii sau dreptul intern ar trebui, în limitele prezentului regulament, să determine conținutul statistic, controlul accesului, specificațiile pentru prelucrarea datelor cu caracter personal în scopuri statistice și măsurile adecvate pentru a proteja drepturile și libertățile persoanelor vizate și pentru a asigura confidențialitatea datelor statistice. Aceste rezultate statistice pot fi utilizate ulterior în diferite scopuri, inclusiv în scopuri de cercetare științifică. Scopuri statistice înseamnă orice operațiune de colectare și prelucrare de date cu caracter personal necesară pentru anchetele statistice sau pentru producerea de rezultate statistice. Scopurile statistice presupun că rezultatul prelucrării în scopuri statistice nu constituie date cu caracter personal, ci date agregate și că acest rezultat sau datele cu caracter personal nu sunt utilizate în sprijinul unor măsuri sau decizii privind o anumită persoană fizică.
- (163) Informațiile confidențiale pe care autoritățile statistice de la nivelul Uniunii și de la nivel național le colectează în vederea elaborării de statistici europene și naționale oficiale ar trebui să fie protejate. Statisticile europene ar trebui concepute, elaborate și difuzate în conformitate cu principiile statistice prevăzute la articolul 338 alineatul (2) din TFUE, în timp ce statisticile naționale ar trebui, de asemenea, să fie în conformitate cu dreptul intern. Regulamentul (CE) nr. 223/2009 al Parlamentului European și al Consiliului ⁽²⁾ prevede specificații suplimentare privind confidențialitatea datelor statistice pentru statisticile europene.
- (164) În ceea ce privește competențele autorităților de supraveghere de a obține de la operator sau de la persoana imputernicită de operator accesul la datele cu caracter personal și accesul în clădirile lor, statele membre pot adopta, pe cale legislativă și în limitele stabilite de prezentul regulament, norme specifice pentru protejarea secretului profesional sau a altor obligații echivalente, în măsura în care acest lucru este necesar pentru a asigura un echilibru între dreptul la protecția datelor cu caracter personal și obligația de păstrare a secretului profesional. Aceasta nu aduce atingere obligațiilor existente ale statelor membre de a adopta norme privind secretul profesional în situațiile cerute de dreptul Uniunii.
- (165) Prezentul regulament respectă și nu aduce atingere statutului de care beneficiază, în temeiul dreptului constituțional existent, bisericile și asociațiile sau comunitățile religioase din statele membre, astfel cum este recunoscut în articolul 17 din TFUE.
- (166) În vederea îndeplinirii obiectivelor prezentului regulament, și anume protejarea drepturilor și libertăților fundamentale ale persoanelor fizice și, în special, a dreptului acestora la protecția datelor cu caracter personal, și

⁽¹⁾ Regulamentul (UE) nr. 536/2014 al Parlamentului European și al Consiliului din 16 aprilie 2014 privind studiile clinice intervenționale cu medicamente de uz uman și de abrogare a Directivei 2001/20/CE (JO L 158, 27.5.2014, p. 1).

⁽²⁾ Regulamentul (CE) nr. 223/2009 al Parlamentului European și al Consiliului din 11 martie 2009 privind statisticile europene și de abrogare a Regulamentului (CE, Euratom) nr. 1101/2008 al Parlamentului European și al Consiliului privind transmiterea de date statistice confidențiale Biroului Statistic al Comunităților Europene, a Regulamentului (CE) nr. 322/97 al Consiliului privind statisticile comunitare și a Deciziei 89/382/CEE, Euratom a Consiliului de constituire a Comitetului pentru programele statistice ale Comunităților Europene (JO L 87, 31.3.2009, p. 164).

pentru a se garanta libera circulație a datelor cu caracter personal pe teritoriul Uniunii, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui să fie delegată Comisiei. În special, ar trebui adoptate acte delegate în ceea ce privește criteriile și cerințele privind mecanismele de certificare, informațiile care trebuie prezentate prin pictograme standardizate și procedurile pentru furnizarea unor astfel de pictograme. Este deosebit de important ca, în cadrul activității sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți. Atunci când pregătește și elaborează acte delegate, Comisia ar trebui să asigure transmiterea simultană, la timp și în mod corespunzător a documentelor relevante către Parlamentul European și către Consiliu.

- (167) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentului regulament, Comisia ar trebui investită cu competențe de executare în situațiile stabilite de prezentul regulament. Competențele respective ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011. În acest context, Comisia ar trebui să ia în considerare măsuri specifice pentru microîntreprinderi și pentru întreprinderile mici și mijlocii.
- (168) Procedura de examinare ar trebui utilizată pentru adoptarea de acte de punere în aplicare privind: clauzele contractuale standard dintre operatori și persoanele împuternicite de operatori, precum și dintre persoanele împuternicite de operatori; codurile de conduită; standardele tehnice și mecanismele de certificare; nivelul adecvat de protecție oferit de o țară terță, de un teritoriu sau de un anumit sector de prelucrare din țara terță respectivă, sau de o organizație internațională; clauzele standard de protecție a datelor; formatele și procedurile pentru schimbul electronic de informații între operatori, persoanele împuternicite de operatori și autoritățile de supraveghere pentru regulile corporatiste obligatorii; asistența reciprocă; precum și modalitățile de realizare a schimbului electronic de informații între autoritățile de supraveghere, precum și între autoritățile de supraveghere și comitetul.
- (169) Comisia ar trebui să adopte acte de punere în aplicare imediat aplicabile atunci când dovezile disponibile arată că o țară terță, un teritoriu sau un anumit sector de prelucrare din țara terță respectivă, sau o organizație internațională nu asigură un nivel de protecție adecvat, precum și din motive imperative de urgență.
- (170) Deoarece obiectivul prezentului regulament, și anume asigurarea unui nivel echivalent de protecție a persoanelor fizice și libera circulație a datelor cu caracter personal în întreaga Uniune, nu poate fi realizat în mod satisfăcător de către statele membre dar, având în vedere amploarea sau efectele acțiunii, poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este definit la articolul 5 din Tratatul privind Uniunea Europeană („Tratatul UE”). În conformitate cu principiul proporționalității, astfel cum este definit la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivelor menționate.
- (171) Directiva 95/46/CE ar trebui să fie abrogată prin prezentul regulament. Prelucrările în derulare la data aplicării prezentului regulament ar trebui să fie aduse în conformitate cu prezentul regulament în termen de doi ani de la data intrării în vigoare a prezentului regulament. În cazul în care prelucrările se bazează pe consimțământ în temeiul Directivei 95/46/CE, nu este necesar ca persoana vizată să își dea încă o dată consimțământul în cazul în care modul în care consimțământul a fost dat este în conformitate cu condițiile din prezentul regulament, astfel încât operatorului să i se permită să continue o astfel de prelucrare după data aplicării prezentului regulament. Deciziile adoptate ale Comisiei și autorizațiile autorităților de supraveghere emise pe baza Directivei 95/46/CE rămân în vigoare până când vor fi modificate, înlocuite sau abrogate.
- (172) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 și a emis un avis la 7 martie 2012 ⁽¹⁾.
- (173) Prezentul regulament ar trebui să se aplice tuturor aspectelor referitoare la protecția drepturilor și libertăților fundamentale legate de prelucrarea datelor cu caracter personal, care nu fac obiectul unor obligații specifice cu același obiectiv ca cel stabilit în Directiva 2002/58/CE a Parlamentului European și a Consiliului ⁽²⁾, inclusiv obligațiile privind operatorul și drepturile persoanelor fizice. Pentru a se clarifica relația dintre prezentul regulament și Directiva 2002/58/CE, respectiva directivă ar trebui să fie modificată în consecință. După adoptarea prezentului regulament, Directiva 2002/58/CE ar trebui să fie revizuită în special pentru a se asigura coerența cu prezentul regulament,

⁽¹⁾ JO C 192, 30.6.2012, p. 7.

⁽²⁾ Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

Dispoziții generale

Articolul 1

Obiect și obiective

- (1) Prezentul regulament stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, precum și normele referitoare la libera circulație a datelor cu caracter personal.
- (2) Prezentul regulament asigură protecția drepturilor și libertăților fundamentale ale persoanelor fizice și în special a dreptului acestora la protecția datelor cu caracter personal.
- (3) Libera circulație a datelor cu caracter personal în interiorul Uniunii nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

Articolul 2

Domeniul de aplicare material

- (1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.
- (2) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:
 - (a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii;
 - (b) de către statele membre atunci când desfășoară activități care intră sub incidența capitolului 2 al titlului V din Tratatul UE;
 - (c) de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice;
 - (d) de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmării penale a infracțiunilor, sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.
- (3) Pentru prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii, se aplică Regulamentul (CE) nr. 45/2001. Regulamentul (CE) nr. 45/2001 și alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal se adaptează la principiile și normele din prezentul regulament în conformitate cu articolul 98.
- (4) Prezentul regulament nu aduce atingere aplicării Directivei 2000/31/CE, în special normelor privind răspunderea furnizorilor de servicii intermediari, prevăzute la articolele 12-15 din directiva menționată.

Articolul 3

Domeniul de aplicare teritorial

- (1) Prezentul regulament se aplică prelucrării datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.

(2) Prezentul regulament se aplică prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activitățile de prelucrare sunt legate de:

- (a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată; sau
- (b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.

(3) Prezentul regulament se aplică prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internațional public.

Articolul 4

Definiții

În sensul prezentului regulament:

1. „date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;
2. „prelucrare” înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;
3. „restricționarea prelucrării” înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;
4. „creare de profiluri” înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;
5. „pseudonimizare” înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;
6. „sistem de evidență a datelor” înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;
7. „operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;
8. „persoană împuternicită de operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
9. „destinatar” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (cărui) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice

căroră li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

10. „parte terță” înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directă autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;
11. „consimțământ” al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;
12. „încălcarea securității datelor cu caracter personal” înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;
13. „date genetice” înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;
14. „date biometrice” înseamnă o date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;
15. „date privind sănătatea” înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;
16. „sediul principal” înseamnă:
 - (a) în cazul unui operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acestuia în Uniune, cu excepția cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are competența de a dispune punerea în aplicare a acestor decizii, caz în care sediul care a luat deciziile respective este considerat a fi sediul principal;
 - (b) în cazul unei persoane împuternicite de operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acesteia în Uniune, sau, în cazul în care persoana împuternicită de operator nu are o administrație centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activitățile principale de prelucrare, în contextul activităților unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligații specifice în temeiul prezentului regulament;
17. „reprezentant” înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul articolului 27, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul prezentului regulament;
18. „întreprindere” înseamnă o persoană fizică sau juridică ce desfășoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații care desfășoară în mod regulat o activitate economică;
19. „grup de întreprinderi” înseamnă o întreprindere care exercită controlul și întreprinderile controlate de aceasta;
20. „reguli corporatiste obligatorii” înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;
21. „autoritate de supraveghere” înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 51;

22. „autoritate de supraveghere vizată” înseamnă o autoritate de supraveghere care este vizată de procesul de prelucrare a datelor cu caracter personal deoarece:
- (a) operatorul sau persoana împuternicită de operator este stabilită pe teritoriul statului membru al autorității de supraveghere respective;
 - (b) persoanele vizate care își au reședința în statul membru în care se află autoritatea de supraveghere respectivă sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare; sau
 - (c) la autoritatea de supraveghere respectivă a fost depusă o plângere;
23. „prelucrare transfrontalieră” înseamnă:
- (a) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre; sau
 - (b) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre;
24. „obiecție relevantă și motivată” înseamnă o obiecție la un proiect de decizie în scopul de a stabili dacă există o încălcare a prezentului regulament sau dacă măsurile preconizate în ceea ce privește operatorul sau persoana împuternicită de operator respectă prezentul regulament, care demonstrează în mod clar importanța riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate și, după caz, libera circulație a datelor cu caracter personal în cadrul Uniunii;
25. „serviciile societății informaționale” înseamnă un serviciu astfel cum este definit la articolul 1 alineatul (1) litera (b) din Directiva 98/34/CE a Parlamentului European și a Consiliului (⁽¹⁾);
26. „organizație internațională” înseamnă o organizație și organismele sale subordonate reglementate de dreptul internațional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe țări sau în temeiul unui astfel de acord.

CAPITOLUL II

Principii

Articolul 5

Principii legate de prelucrarea datelor cu caracter personal

- (1) Datele cu caracter personal sunt:
- (a) prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”);
 - (b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89 alineatul (1) („limitări legate de scop”);
 - (c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”);
 - (d) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate”);

(¹) Directiva 98/34/CE a Parlamentului European și a Consiliului din 22 iunie 1998 de stabilire a unei proceduri pentru furnizarea de informații în domeniul standardelor și reglementărilor tehnice și al normelor privind serviciile societății informaționale (JO L 204, 21.7.1998, p. 37).

- (e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate („limitări legate de stocare”);
 - (f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate”).
- (2) Operatorul este responsabil de respectarea alineatului (1) și poate demonstra această respectare („responsabilitate”).

Articolul 6

Legalitatea prelucrării

- (1) Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:
- (a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
 - (b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
 - (c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
 - (d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
 - (e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul;
 - (f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Litera (f) din primul paragraf nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor.

(2) Statele membre pot menține sau introduce dispoziții mai specifice de adaptare a aplicării normelor prezentului regulament în ceea ce privește prelucrarea în vederea respectării alineatului (1) literele (c) și (e) prin definirea unor cerințe specifice mai precise cu privire la prelucrare și a altor măsuri de asigurare a unei prelucrări legale și echitabile, inclusiv pentru alte situații concrete de prelucrare, astfel cum este prevăzut în capitolul IX.

(3) Temeiul pentru prelucrarea menționată la alineatul (1) literele (c) și (e) trebuie să fie prevăzut în:

- (a) dreptul Uniunii; sau
- (b) dreptul intern care se aplică operatorului.

Scopul prelucrării este stabilit pe baza respectivului temei juridic sau, în ceea ce privește prelucrarea menționată la alineatul (1) litera (e), este necesar pentru îndeplinirea unei sarcini efectuate în interes public sau în cadrul exercitării unei funcții publice atribuite operatorului. Respectivul temei juridic poate conține dispoziții specifice privind adaptarea aplicării normelor prezentului regulament, printre altele: condițiile generale care reglementează legalitatea prelucrării de către operator; tipurile de date care fac obiectul prelucrării; persoanele vizate; entitățile cărora le pot fi divulgate datele și scopul pentru care respectivele date cu caracter personal pot fi divulgate; limitările legate de scop; perioadele de stocare;

și operațiunile și procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale și echitabile cum sunt cele pentru alte situații concrete de prelucrare astfel cum sunt prevăzute în capitolul IX. Dreptul Uniunii sau dreptul intern urmărește un obiectiv de interes public și este proporțional cu obiectivul legitim urmărit.

(4) În cazul în care prelucrarea în alt scop decât cel pentru care datele cu caracter personal au fost colectate nu se bazează pe consimțământul persoanei vizate sau pe dreptul Uniunii sau dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja obiectivele menționate la articolul 23 alineatul (1), operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial, ia în considerare, printre altele:

- (a) orice legătură dintre scopurile în care datele cu caracter personal au fost colectate și scopurile prelucrării ulterioare preconizate;
- (b) contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește relația dintre persoanele vizate și operator;
- (c) natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date cu caracter personal, în conformitate cu articolul 9, sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale și infracțiuni, în conformitate cu articolul 10;
- (d) posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;
- (e) existența unor garanții adecvate, care pot include criptarea sau pseudonimizarea.

Articolul 7

Condiții privind consimțământul

(1) În cazul în care prelucrarea se bazează pe consimțământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal.

(2) În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Nicio parte a respectivei declarații care constituie o încălcare a prezentului regulament nu este obligatorie.

(3) Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimțământului se face la fel de simplu ca acordarea acestuia.

(4) Atunci când se evaluează dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

Articolul 8

Condiții aplicabile în ceea ce privește consimțământul copiilor în legătură cu serviciile societății informaționale

(1) În cazul în care se aplică articolul 6 alineatul (1) litera (a), în ceea ce privește oferirea de servicii ale societății informaționale în mod direct unui copil, prelucrarea datelor cu caracter personal ale unui copil este legală dacă copilul are cel puțin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului.

Statele membre pot prevedea prin lege o vârstă inferioară în aceste scopuri, cu condiția ca acea vârstă inferioară să nu fie mai mică de 13 ani.

(2) Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile.

(3) Alineatul (1) nu afectează dreptul general al contractelor aplicabil în statele membre, cum ar fi normele privind valabilitatea, încheierea sau efectele unui contract în legătură cu un copil.

Articolul 9

Prelucrarea de categorii speciale de date cu caracter personal

(1) Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

(2) Alineatul (1) nu se aplică în următoarele situații:

- (a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicția prevăzută la alineatul (1) să nu poată fi ridicată prin consimțământul persoanei vizate;
- (b) prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;
- (c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;
- (d) prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;
- (e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;
- (f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;
- (g) prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate;
- (h) prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la alineatul (3);
- (i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional; sau

- (j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate.
- (3) Datele cu caracter personal menționate la alineatul (1) pot fi prelucrate în scopurile menționate la alineatul (2) litera (h) în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naționale competente.
- (4) Statele membre pot menține sau introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea de date genetice, date biometrice sau date privind sănătatea.

Articolul 10

Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni

Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni sau la măsuri de securitate conexe în temeiul articolului 6 alineatul (1) se efectuează numai sub controlul unei autorități de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorități de stat.

Articolul 11

Prelucrarea care nu necesită identificare

- (1) În cazul în care scopurile pentru care un operator prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu are obligația de a păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizată în scopul unic al respectării prezentului regulament.
- (2) Dacă, în cazurile menționate la alineatul (1) din prezentul articol, operatorul poate demonstra că nu este în măsură să identifice persoana vizată, operatorul informează persoana vizată în mod corespunzător, în cazul în care este posibil. În astfel de cazuri, articolele 15-20 nu se aplică, cu excepția cazului în care persoana vizată, în scopul exercitării drepturilor sale în temeiul respectivelor articole, oferă informații suplimentare care permit identificarea sa.

CAPITOLUL III

Drepturile persoanei vizate

Secțiunea 1

Transparență și modalități

Articolul 12

Transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate

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

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

(3) Operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri în temeiul articolelor 15-22, fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.

(4) Dacă nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoana vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară.

(5) Informațiile furnizate în temeiul articolelor 13 și 14 și orice comunicare și orice măsuri luate în temeiul articolelor 15-22 și 34 sunt oferite gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate:

- (a) fie să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;
- (b) fie să refuze să dea curs cererii.

În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

(6) Fără a aduce atingere articolului 11, în cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea menționată la articolele 15-21, operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

(7) Informațiile care urmează să fie furnizate persoanelor vizate în temeiul articolelor 13 și 14 pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea trebuie să poată fi citite automat.

(8) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 92 în vederea determinării informațiilor care urmează să fie prezentate de pictograme și a procedurilor pentru furnizarea de pictograme standardizate.

Secțiunea 2

Informare și acces la date cu caracter personal

Articolul 13

Informații care se furnizează în cazul în care datele cu caracter personal sunt colectate de la persoana vizată

(1) În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obținerii acestor date cu caracter personal, furnizează persoanei vizate toate informațiile următoare:

- (a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
- (b) datele de contact ale responsabilului cu protecția datelor, după caz;
- (c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;

- (d) în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f), interesele legitime urmărite de operator sau de o parte terță;
- (e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- (f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menționate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.
- (2) În plus față de informațiile menționate la alineatul (1), în momentul în care datele cu caracter personal sunt obținute, operatorul furnizează persoanei vizate următoarele informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă:
- (a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- (b) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
- (c) atunci când prelucrarea se bazează pe articolul 6 alineatul (1) litera (a) sau pe articolul 9 alineatul (2) litera (a), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
- (d) dreptul de a depune o plângere în fața unei autorități de supraveghere;
- (e) dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;
- (f) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la articolul 22 alineatele (1) și (4), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.
- (3) În cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu alineatul (2).
- (4) Alineatele (1), (2) și (3) nu se aplică dacă și în măsura în care persoana vizată deține deja informațiile respective.

Articolul 14

Informații care se furnizează în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată

- (1) În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informații:
- (a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
- (b) datele de contact ale responsabilului cu protecția datelor, după caz;
- (c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- (d) categoriile de date cu caracter personal vizate;
- (e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;

- (f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menționate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.
- (2) Pe lângă informațiile menționate la alineatul (1), operatorul furnizează persoanei vizate următoarele informații necesare pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată:
- (a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
 - (b) în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f), interesele legitime urmărite de operator sau de o parte terță;
 - (c) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării și a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
 - (d) atunci când prelucrarea se bazează pe articolul 6 alineatul (1) litera (a) sau pe articolul 9 alineatul (2) litera (a), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
 - (e) dreptul de a depune o plângere în fața unei autorități de supraveghere;
 - (f) sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public;
 - (g) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la articolul 22 alineatele (1) și (4), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.
- (3) Operatorul furnizează informațiile menționate la alineatele (1) și (2):
- (a) într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;
 - (b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă; sau
 - (c) dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.
- (4) În cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obținute, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu alineatul (2).
- (5) Alineatele (1)-(4) nu se aplică dacă și în măsura în care:
- (a) persoana vizată deține deja informațiile;
 - (b) furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva condițiilor și a garanțiilor prevăzute la articolul 89 alineatul (1), sau în măsura în care obligația menționată la alineatul (1) din prezentul articol este susceptibilă să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective. În astfel de cazuri, operatorul ia măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate, inclusiv punerea informațiilor la dispoziția publicului;
 - (c) obținerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern sub incidența căruia intră operatorul și care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau
 - (d) în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligații legale de a păstra secretul.

Articolul 15

Dreptul de acces al persoanei vizate

- (1) Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații:
- (a) scopurile prelucrării;
 - (b) categoriile de date cu caracter personal vizate;
 - (c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale;
 - (d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
 - (e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;
 - (f) dreptul de a depune o plângere în fața unei autorități de supraveghere;
 - (g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;
 - (h) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la articolul 22 alineatele (1) și (4), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.
- (2) În cazul în care datele cu caracter personal sunt transferate către o țară terță sau o organizație internațională, persoana vizată are dreptul să fie informată cu privire la garanțiile adecvate în temeiul articolului 46 referitoare la transfer.
- (3) Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative. În cazul în care persoana vizată introduce cererea în format electronic și cu excepția cazului în care persoana vizată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent.
- (4) Dreptul de a obține o copie menționată la alineatul (3) nu aduce atingere drepturilor și libertăților altora.

Secțiunea 3

Rectificare și ștergere

Articolul 16

Dreptul la rectificare

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

Articolul 17

Dreptul la ștergerea datelor („dreptul de a fi uitat”)

- (1) Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:
- (a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

- (b) persoana vizată își retrace consimțământul pe baza căruia are loc prelucrarea, în conformitate cu articolul 6 alineatul (1) litera (a) sau cu articolul 9 alineatul (2) litera (a), și nu există niciun alt temei juridic pentru prelucrarea;
- (c) persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (1) și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (2);
- (d) datele cu caracter personal au fost prelucrate ilegal;
- (e) datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul;
- (f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la articolul 8 alineatul (1).

(2) În cazul în care operatorul a făcut publice datele cu caracter personal și este obligat, în temeiul alineatului (1), să le ștergă, operatorul, ținând seama de tehnologia disponibilă și de costul implementării, ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

(3) Alineatele (1) și (2a) nu se aplică în măsura în care prelucrarea este necesară:

- (a) pentru exercitarea dreptului la liberă exprimare și la informare;
- (b) pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este investit operatorul;
- (c) din motive de interes public în domeniul sănătății publice, în conformitate cu articolul 9 alineatul (2) literele (h) și (i) și cu articolul 9 alineatul (3);
- (d) în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în măsura în care dreptul menționat la alineatul (1) este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau
- (e) pentru constatarea, exercitarea sau apărarea unui drept în instanță.

Articolul 18

Dreptul la restricționarea prelucrării

(1) Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării în cazul în care se aplică unul din următoarele cazuri:

- (a) persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;
- (b) prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;
- (c) operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță; sau
- (d) persoana vizată s-a opus prelucrării în conformitate cu articolul 21 alineatul (1), pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

(2) În cazul în care prelucrarea a fost restricționată în temeiul alineatului (1), astfel de date cu caracter personal pot, cu excepția stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

(3) O persoană vizată care a obținut restricționarea prelucrării în temeiul alineatului (1) este informată de către operator înainte de ridicarea restricției de prelucrare.

Articolul 19

Obligația de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării

Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate în conformitate cu articolul 16, articolul 17 alineatul (1) și articolul 18, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

Articolul 20

Dreptul la portabilitatea datelor

(1) Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, în cazul în care:

- (a) prelucrarea se bazează pe consimțământ în temeiul articolului 6 alineatul (1) litera (a) sau al articolului 9 alineatul (2) litera (a) sau pe un contract în temeiul articolului 6 alineatul (1) litera (b); și
- (b) prelucrarea este efectuată prin mijloace automate.

(2) În exercitarea dreptului său la portabilitatea datelor în temeiul alineatului (1), persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic.

(3) Exercițarea dreptului menționat la alineatul (1) din prezentul articol nu aduce atingere articolului 17. Respectivul drept nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este investit operatorul.

(4) Dreptul menționat la alineatul (1) nu aduce atingere drepturilor și libertăților altora.

Secțiunea 4

Dreptul la opoziție și procesul decizional individual automatizat

Articolul 21

Dreptul la opoziție

(1) În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situația particulară în care se află, prelucrării în temeiul articolului 6 alineatul (1) litera (e) sau (f) sau al articolului 6 alineatul (1) a datelor cu caracter personal care o privesc, inclusiv creării de profiluri pe baza respectivelor dispoziții. Operatorul nu mai prelucrează datele cu caracter personal, cu excepția cazului în care operatorul demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

(2) Atunci când prelucrarea datelor cu caracter personal are drept scop marketingul direct, persoana vizată are dreptul de a se opune în orice moment prelucrării în acest scop a datelor cu caracter personal care o privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv.

(3) În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.

(4) Cel târziu în momentul primei comunicări cu persoana vizată, dreptul menționat la alineatele (1) și (2) este adus în mod explicit în atenția persoanei vizate și este prezentat în mod clar și separat de orice alte informații.

(5) În contextual utilizării serviciilor societății informaționale și în pofida Directivei 2002/58/CE, persoana vizată își poate exercita dreptul de a se opune prin mijloace automate care utilizează specificații tehnice.

(6) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică sau în scopuri statistice în conformitate cu articolul 89 alineatul (1), persoana vizată, din motive legate de situația sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepția cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

Articolul 22

Procesul decizional individual automatizat, inclusiv crearea de profiluri

(1) Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

(2) Alineatul (1) nu se aplică în cazul în care decizia:

- (a) este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date;
- (b) este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului și care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate; sau
- (c) are la bază consimțământul explicit al persoanei vizate.

(3) În cazurile menționate la alineatul (2) literele (a) și (c), operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia.

(4) Deciziile menționate la alineatul (2) nu au la bază categoriile speciale de date cu caracter personal menționate la articolul 9 alineatul (1), cu excepția cazului în care se aplică articolul 9 alineatul (2) litera (a) sau (g) și în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate.

Secțiunea 5

Restricții

Articolul 23

Restricții

(1) Dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la articolele 12-22 și 34, precum și la articolul 5 în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la articolele 12-22, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura:

- (a) securitatea națională;
- (b) apărarea;
- (c) securitatea publică;

- (d) prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;
 - (e) alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale;
 - (f) protejarea independenței judiciare și a procedurilor judiciare;
 - (g) prevenirea, investigarea, depistarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate;
 - (h) funcția de monitorizare, inspecție sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale în cazurile menționate la literele (a)-(e) și (g);
 - (i) protecția persoanei vizate sau a drepturilor și libertăților altora;
 - (j) punerea în aplicare a pretențiilor de drept civil.
- (2) În special, orice măsură legislativă menționată la alineatul (1) conține dispoziții specifice cel puțin, dacă este cazul, în ceea ce privește:
- (a) scopurile prelucrării sau ale categoriilor de prelucrare;
 - (b) categoriile de date cu caracter personal;
 - (c) domeniul de aplicare al restricțiilor introduse;
 - (d) garanțiile pentru a preveni abuzurile sau accesul sau transferul ilegal;
 - (e) menționarea operatorului sau a categoriilor de operatori;
 - (f) perioadele de stocare și garanțiile aplicabile având în vedere natura, domeniul de aplicare și scopurile prelucrării sau ale categoriilor de prelucrare;
 - (g) riscurile pentru drepturile și libertăților persoanelor vizate; și
 - (h) dreptul persoanelor vizate de a fi informate cu privire la restricție, cu excepția cazului în care acest lucru poate aduce atingere scopului restricției.

CAPITOLUL IV

Operatorul și persoana împuternicită de operator

Secțiunea 1

Obligații generale

Articolul 24

Responsabilitatea operatorului

- (1) Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivul măsuri se revizuiesc și se actualizează dacă este necesar.
- (2) Atunci când sunt proporționale în raport cu operațiunile de prelucrare, măsurile menționate la alineatul (1) includ punerea în aplicare de către operator a unor politici adecvate de protecție a datelor.
- (3) Aderarea la coduri de conduită aprobate, menționate la articolul 40, sau la un mecanism de certificare aprobat, menționat la articolul 42, poate fi utilizată ca element care să demonstreze respectarea obligațiilor de către operator.

*Articolul 25***Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit**

- (1) Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.
- (2) Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane.
- (3) Un mecanism de certificare aprobat în conformitate cu articolul 42 poate fi utilizat drept element care să demonstreze îndeplinirea cerințelor prevăzute la alineatele (1) și (2) ale prezentului articol.

*Articolul 26***Operatori asociați**

- (1) În cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați. Ei stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul prezentului regulament, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute la articolele 13 și 14, prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.
- (2) Acordul menționat la alineatul (1) reflectă în mod adecvat rolurile și raporturile respective ale operatorilor asociați față de persoanele vizate. Esența acestui acord este făcută cunoscută persoanei vizate.
- (3) Indiferent de clauzele acordului menționat la alineatul (1), persoana vizată își poate exercita drepturile în temeiul prezentului regulament cu privire la și în raport cu fiecare dintre operatori.

*Articolul 27***Reprezentanții operatorilor sau ai persoanelor împuternicite de operatori care nu își au sediul în Uniune**

- (1) În cazul în care se aplică articolul 3 alineatul (2), operatorul sau persoana împuternicită de operator desemnează în scris un reprezentant în Uniune.
- (2) Obligația prevăzută la alineatul (1) din prezentul articol nu se aplică:
- (a) prelucrării care are un caracter ocazional, care nu include, pe scară largă, prelucrarea unor categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau prelucrarea unor date cu caracter personal referitoare la condamnări penale și infracțiuni menționată la articolul 10, și care este puțin susceptibilă de a genera un risc pentru drepturile și libertățile persoanelor, ținând cont de natura, contextul, domeniul de aplicare și scopurile prelucrării; sau
 - (b) unei autorități sau unui organism public.

- (3) Reprezentantul își are sediul în unul dintre statele membre în care se află persoanele vizate ale căror date cu caracter personal sunt prelucrate în legătură cu furnizarea de bunuri și servicii sau al căror comportament este monitorizat.
- (4) Reprezentantul primește din partea operatorului sau a persoanei împuternicite de operator un mandat prin care autoritățile de supraveghere și persoanele vizate, în special, se pot adresa reprezentantului, în plus față de operator sau persoana împuternicită de operator sau în locul acestora, cu privire la toate chestiunile legate de prelucrarea, în scopul asigurării respectării prezentului regulament.
- (5) Desemnarea unui reprezentant de către operator sau persoana împuternicită de operator nu aduce atingere acțiunilor în justiție care ar putea fi introduse împotriva operatorului sau persoanei împuternicite de operator înseși.

Articolul 28

Persoana împuternicită de operator

- (1) În cazul în care prelucrarea urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate.
- (2) Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecții față de aceste modificări.
- (3) Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoană împuternicită de operator:
- (a) prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, inclusiv în ceea ce privește transferurile de date cu caracter personal către o țară terță sau o organizație internațională, cu excepția cazului în care această obligație îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;
 - (b) se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație statutară adecvată de confidențialitate;
 - (c) adoptă toate măsurile necesare în conformitate cu articolul 32;
 - (d) respectă condițiile menționate la alineatele (2) și (4) privind recrutarea unei alte persoane împuternicite de operator;
 - (e) ținând seama de natura prelucrării, oferă asistență operatorului prin măsuri tehnice și organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligației operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute în capitolul III;
 - (f) ajută operatorul să asigure respectarea obligațiilor prevăzute la articolele 32-36, ținând seama de caracterul prelucrării și informațiile aflate la dispoziția persoanei împuternicite de operator;
 - (g) la alegerea operatorului, șterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;
 - (h) pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute la prezentul articol, permite desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea.

În ceea ce privește primul paragraf litera (h), persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucțiune încalcă prezentul regulament sau alte dispoziții din dreptul intern sau din dreptul Uniunii referitoare la protecția datelor.

(4) În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator, astfel cum se prevede la alineatul (3), revin celei de a doua persoane împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul dreptului Uniunii sau al dreptului intern, în special furnizarea de garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentului regulament. În cazul în care această a doua persoană împuternicită nu își respectă obligațiile privind protecția datelor, persoana împuternicită inițială rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor acestei a doua persoane împuternicite.

(5) Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, menționat la articolul 40, sau la un mecanism de certificare aprobat, menționat la articolul 42, poate fi utilizată ca element prin care să se demonstreze existența garanțiilor suficiente menționate la alineatele (1) și (4) din prezentul articol.

(6) Fără a aduce atingere unui contract individual încheiat între operator și persoana împuternicită de operator, contractul sau celălalt act juridic menționat la alineatele (3) și (4) din prezentul articol se poate baza, integral sau parțial, pe clauze contractuale standard menționate la alineatele (7) și (8) din prezentul articol, inclusiv atunci când fac parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator în temeiul articolelor 42 și 43.

(7) Comisia poate să prevadă clauze contractuale standard pentru aspectele menționate la alineatele (3) și (4) din prezentul articol și în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2).

(8) O autoritate de supraveghere poate să adopte clauze contractuale standard pentru aspectele menționate la alineatele (3) și (4) din prezentul articol și în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 63.

(9) Contractul sau celălalt act juridic menționat la alineatele (3) și (4) se formulează în scris, inclusiv în format electronic.

(10) Fără a aduce atingere articolelor 82, 83 și 84, în cazul în care o persoană împuternicită de operator încalcă prezentul regulament, prin stabilirea scopurilor și mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă.

Articolul 29

Desfășurarea activității de prelucrare sub autoritatea operatorului sau a persoanei împuternicite de operator

Persoana împuternicită de operator și orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru.

Articolul 30

Evidențele activităților de prelucrare

(1) Fiecare operator și, după caz, reprezentantul acestuia păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor. Respectiva evidență cuprinde toate următoarele informații:

- (a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;
- (b) scopurile prelucrării;
- (c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;

- (d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
 - (e) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor menționate la articolul 49 alineatul (1) al doilea paragraf, documentația care dovedește existența unor garanții adecvate;
 - (f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
 - (g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1).
- (2) Fiecare operator și, după caz, persoana împuternicită de operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind:
- (a) numele și datele de contact ale persoanei sau persoanelor împuternicite de operator și ale fiecărui operator în numele căruia acționează această persoană (aceste persoane), precum și ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;
 - (b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;
 - (c) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor prevăzute la articolul 49 alineatul (1) al doilea paragraf, documentația care dovedește existența unor garanții adecvate;
 - (d) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1).
- (3) Evidențele menționate la alineatele (1) și (2) se formulează în scris, inclusiv în format electronic.
- (4) Operatorul sau persoana împuternicită de acesta, precum și, după caz, reprezentantul operatorului sau al persoanei împuternicite de operator pun evidențele la dispoziția autorității de supraveghere, la cererea acesteia.
- (5) Obligațiile menționate la alineatele 1 și 2 nu se aplică unei întreprinderi sau organizații cu mai puțin de 250 de angajați, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează la articolul 10.

Articolul 31

Cooperarea cu autoritatea de supraveghere

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

Secțiunea 2

Securitatea datelor cu caracter personal

Articolul 32

Securitatea prelucrării

(1) Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

- (a) pseudonimizarea și criptarea datelor cu caracter personal;

- (b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
 - (c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
 - (d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.
- (2) La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.
- (3) Aderarea la un cod de conduită aprobat, menționat la articolul 40, sau la un mecanism de certificare aprobat, menționat la articolul 42, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute la alineatul (1) din prezentul articol.
- (4) Operatorul și persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.

Articolul 33

Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal

- (1) În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere competente în temeiul articolului 55, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată din partea autorității de supraveghere în cazul în care.
- (2) Persoana împuternicită de operator înștiințează operatorul fără întârzieri nejustificate după ce ia cunoștință de o încălcare a securității datelor cu caracter personal.
- (3) Notificarea menționată la alineatul (1) cel puțin:
- (a) descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
 - (b) comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
 - (c) descrie consecințele probabile ale încălcării securității datelor cu caracter personal;
 - (d) descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.
- (4) Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.
- (5) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație permite autorității de supraveghere să verifice conformitatea cu prezentul articol.

Articolul 34

Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal

- (1) În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

- (2) În informarea transmisă persoanei vizate prevăzută la alineatul (1) din prezentul articol se include o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile și măsurile menționate la articolul 33 alineatul (3) literele (b), (c) și (d).
- (3) Informarea persoanei vizate menționată la alineatul (1) nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:
- (a) operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;
 - (b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate menționat la alineatul (1) nu mai este susceptibil să se materializeze;
 - (c) ar necesita un efort disproporționat. În această situație, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.
- (4) În cazul în care operatorul nu a comunicat deja încălcarea securității datelor cu caracter personal către persoana vizată, autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securității datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condițiile menționate la alineatul (3) sunt îndeplinite.

Secțiunea 3

Evaluarea impactului asupra protecției datelor și consultarea prealabilă

Articolul 35

Evaluarea impactului asupra protecției datelor

- (1) Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.
- (2) La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat.
- (3) Evaluarea impactului asupra protecției datelor menționată la alineatul (1) se impune mai ales în cazul:
- (a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;
 - (b) prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10; sau
 - (c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.
- (4) Autoritatea de supraveghere întocmește și publică o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor, în conformitate cu alineatul (1). Autoritatea de supraveghere comunică aceste liste comitetului menționat la articolul 68.
- (5) Autoritatea de supraveghere poate, de asemenea, să stabilească și să pună la dispoziția publicului o listă a tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor. Autoritatea de supraveghere comunică aceste liste comitetului.
- (6) Înainte de adoptarea listelor menționate la alineatele (4) și (5), autoritatea de supraveghere competentă aplică mecanismul pentru asigurarea coerenței menționat la articolul 63 în cazul în care aceste liste implică activități de prelucrare care presupun furnizarea de bunuri sau prestarea de servicii către persoane vizate sau monitorizarea comportamentului acestora în mai multe state membre ori care pot afecta în mod substanțial libera circulație a datelor cu caracter personal în cadrul Uniunii.

- (7) Evaluarea conține cel puțin:
- (a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;
 - (b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;
 - (c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la alineatul (1); și
 - (d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.
- (8) La evaluarea impactului operațiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevante, se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate menționate la articolul 40, în special în vederea unei evaluări a impactului asupra protecției datelor.
- (9) Operatorul solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.
- (10) Atunci când prelucrarea în temeiul articolului 6 alineatul (1) litera (c) sau (e) are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidența căruia intră operatorul, iar dreptul respectiv reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, alineatele (1)-(7) nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.
- (11) Acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

Articolul 36

Consultarea prealabilă

- (1) Operatorul consultă autoritatea de supraveghere înainte de prelucrarea atunci când evaluarea impactului asupra protecției datelor prevăzută la articolul 35 indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.
- (2) Atunci când consideră că prelucrarea prevăzută menționată la alineatul (1) ar încălca prezentul regulament, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris operatorului și, după caz, persoanei împuternicite de operator, în cel mult opt săptămâni de la primirea cererii de consultare, și își poate utiliza oricare dintre competențele menționate la articolul 58. Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute. Autoritatea de supraveghere informează operatorul și, după caz, persoana împuternicită de operator, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când autoritatea de supraveghere a obținut informațiile pe care le-a solicitat în scopul consultării.
- (3) Atunci când consultă autoritatea de supraveghere în conformitate cu alineatul (1), operatorul îi furnizează acesteia:
- (a) dacă este cazul, responsabilitățile respective ale operatorului, ale operatorilor asociați și ale persoanelor împuternicite de operator implicate în activitățile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;
 - (b) scopurile și mijloacele prelucrării preconizate;
 - (c) măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților persoanelor vizate, în conformitate cu prezentul regulament;
 - (d) dacă este cazul, datele de contact ale responsabilului cu protecția datelor;

- (e) evaluarea impactului asupra protecției datelor prevăzută la articolul 35; și
 - (f) orice alte informații solicitate de autoritatea de supraveghere.
- (4) Statele membre consultă autoritatea de supraveghere în cadrul procesului de pregătire a unei propuneri de măsură legislativă care urmează să fie adoptată de un parlament național sau a unei măsuri de reglementare întemeiate pe o astfel de măsură legislativă, care se referă la prelucrarea.
- (5) În pofida alineatului (1), dreptul intern poate impune operatorilor să se consulte cu autoritatea de supraveghere și să obțină în prealabil autorizarea din partea acesteia în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecția socială și sănătatea publică.

Secțiunea 4

Responsabilul cu protecția datelor

Articolul 37

Desemnarea responsabilului cu protecția datelor

- (1) Operatorul și persoana împuternicită de operator desemnează un responsabil cu protecția datelor ori de câte ori:
- (a) prelucrarea este efectuată de o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;
 - (b) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă; sau
 - (c) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date, menționată la articolul 9, sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10.
- (2) Un grup de întreprinderi poate numi un responsabil cu protecția datelor unic, cu condiția ca responsabilul cu protecția datelor să fie ușor accesibil din fiecare întreprindere.
- (3) În cazul în care operatorul sau persoana împuternicită de operator este o autoritate publică sau un organism public, poate fi desemnat un responsabil cu protecția datelor unic pentru mai multe dintre aceste autorități sau organisme, luând în considerare structura organizatorică și dimensiunea acestora.
- (4) În alte cazuri decât cele menționate la alineatul (1), operatorul sau persoana împuternicită de operator ori asociațiile și alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot desemna sau, acolo unde dreptul Uniunii sau dreptul intern solicită acest lucru, desemnează un responsabil cu protecția datelor. Responsabilul cu protecția datelor poate să acționeze în favoarea unor astfel de asociații și alte organisme care reprezintă operatori sau persoane împuternicite de operatori.
- (5) Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la articolul 39.
- (6) Responsabilul cu protecția datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să își îndeplinească sarcinile în baza unui contract de servicii.
- (7) Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecția datelor și le comunică autorității de supraveghere.

Articolul 38

Funcția responsabilului cu protecția datelor

- (1) Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal.

- (2) Operatorul și persoana împuternicită de operator sprijină responsabilul cu protecția datelor în îndeplinirea sarcinilor menționate la articolul 39, asigurându-i resursele necesare pentru executarea acestor sarcini, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate.
- (3) Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini. Acesta nu este demis sau sancționat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.
- (4) Persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentului regulament.
- (5) Responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.
- (6) Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese.

Articolul 39

Sarcinile responsabilului cu protecția datelor

- (1) Responsabilul cu protecția datelor are cel puțin următoarele sarcini:
- (a) informarea și consilierea operatorului, sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;
 - (b) monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
 - (c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu articolul 35;
 - (d) cooperarea cu autoritatea de supraveghere;
 - (e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.
- (2) În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.

Secțiunea 5

Coduri de conduită și certificare

Articolul 40

Coduri de conduită

- (1) Statele membre, autoritățile de supraveghere, comitetul și Comisia încurajează elaborarea de coduri de conduită menite să contribuie la buna aplicare a prezentului regulament, ținând seama de caracteristicile specifice ale diverselor sectoare de prelucrare și de nevoile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii.
- (2) Asociațiile și alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot pregăti coduri de conduită sau le pot modifica sau extinde pe cele existente, în scopul de a specifica modul de aplicare a prezentului regulament, cum ar fi în ceea ce privește:
- (a) prelucrarea în mod echitabil și transparent;

- (b) interesele legitime urmărite de operatori în contexte specifice;
- (c) colectarea datelor cu caracter personal;
- (d) pseudonimizarea datelor cu caracter personal;
- (e) informarea publicului și a persoanelor vizate;
- (f) exercitarea drepturilor persoanelor vizate;
- (g) informarea și protejarea copiilor și modalitatea în care trebuie obținut consimțământul titularilor răspunderii părintești asupra copiilor;
- (h) măsurile și procedurile menționate la articolele 24 și 25 și măsurile de asigurare a securității prelucrării, menționate la articolul 32;
- (i) notificarea autorităților de supraveghere cu privire la încălcările securității datelor cu caracter personal și informarea persoanelor vizate cu privire la aceste încălcări;
- (j) transferul de date cu caracter personal către țări terțe sau organizații internaționale; sau
- (k) proceduri extrajudiciare și alte proceduri de soluționare a litigiilor pentru soluționarea litigiilor între operatori și persoanele vizate în ceea ce privește prelucrarea, fără a aduce atingere drepturilor persoanelor vizate, în temeiul articolelor 77 și 79.

(3) La codurile de conduită aprobate în temeiul alineatului (5) din prezentul articol și care au o valabilitate generală în temeiul alineatului (9) din prezentul articol pot adera nu numai operatorii sau persoanele împuternicite de operatori care fac obiectul prezentului regulament, ci și operatorii sau persoanele împuternicite de operatori care nu fac obiectul prezentului regulament în temeiul articolului 3, în scopul de a oferi garanții adecvate în cadrul transferurilor de date cu caracter personal către țări terțe sau organizații internaționale în condițiile menționate la articolul 46 alineatul (2) litera (e). Acești operatori sau persoane împuternicite de operatori își asumă angajamente cu caracter obligatoriu și executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, în scopul aplicării garanțiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.

(4) Codul de conduită prevăzut la alineatul (2) din prezentul articol cuprinde mecanisme care permit organismului menționat la articolul 41 alineatul (1) să efectueze monitorizarea obligatorie a respectării dispozițiilor acestuia de către operatorii sau persoanele împuternicite de operatori care se angajează să îl aplice, fără a aduce atingere sarcinilor și competențelor autorităților de supraveghere care sunt competente în temeiul articolului 55 sau 56.

(5) Asociațiile și alte organisme menționate la alineatul (2) din prezentul articol care intenționează să pregătească un cod de conduită sau să modifice sau să extindă un cod existent transmit proiectul de cod, de modificare sau de extindere autorității de supraveghere care este competentă în temeiul articolului 55. Autoritatea de supraveghere emite un aviz cu privire la conformitatea cu prezentul regulament a proiectului de cod, de modificare sau de extindere și îl aprobă în cazul în care se constată că acesta oferă garanții adecvate suficiente.

(6) În cazul în care proiectul de cod, de modificare sau de extindere este aprobat în conformitate cu alineatul (5), iar codul de conduită în cauză nu are legătură cu activitățile de prelucrare din mai multe state membre, autoritatea de supraveghere înregistrează și publică codul.

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

(8) În cazul în care avizul menționat la alineatul (7) confirmă conformitatea cu prezentul regulament a proiectului de cod, de modificare sau de extindere sau în cazul în care, în situația menționată la alineatul (3), oferă garanții adecvate, comitetul transmite avizul său Comisiei.

(9) Comisia poate adopta acte de punere în aplicare pentru a decide că codul de conduită, modificarea sau extinderea aprobate care i-au fost prezentate în temeiul alineatului (8) din prezentul articol au valabilitate generală în Uniune. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 93 alineatul (2).

(10) Comisia asigură publicitatea adecvată pentru codurile aprobate asupra cărora s-a decis că au valabilitate generală în conformitate cu alineatul (9).

(11) Comitetul regrupează toate codurile de conduită, modificările și extinderile aprobate într-un registru și le pune la dispoziția publicului prin mijloace corespunzătoare.

Articolul 41

Monitorizarea codurilor de conduită aprobate

(1) Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente în temeiul articolelor 57 și 58, monitorizarea respectării unui cod de conduită în temeiul articolului 40 poate fi realizată de un organism care dispune de un nivel adecvat de expertiză în legătură cu obiectul codului și care este acreditat în acest scop de autoritatea de supraveghere competentă.

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

- (a) a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, independența și expertiza sa în legătură cu obiectul codului;
- (b) a instituit proceduri care îi permit să evalueze eligibilitatea operatorilor și a persoanelor împuternicite de operatori în vederea aplicării codului, să monitorizeze respectarea de către aceștia a dispozițiilor codului și să revizuiască periodic funcționarea acestuia;
- (c) a instituit proceduri și structuri pentru tratarea plângerilor privind încălcări ale codului sau privind modul în care codul a fost sau este pus în aplicare de un operator sau o persoană împuternicită de operator, precum și pentru asigurarea transparenței acestor proceduri și structuri pentru persoanele vizate și pentru public; și
- (d) a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, că sarcinile și atribuțiile sale nu creează conflicte de interese.

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

(4) Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente și dispozițiilor capitolului VIII, un organism menționat la alineatul (1) din prezentul articol ia măsuri corespunzătoare, sub rezerva unor garanții adecvate, în cazul încălcării codului de către un operator sau o persoană împuternicită de operator, inclusiv prin suspendarea sau excluderea respectivului operator sau a respectivei persoane din cadrul codului. Organismul în cauză informează autoritatea de supraveghere competentă cu privire la aceste măsuri și la motivele care le-au determinat.

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

(6) Prezentul articol nu se aplică prelucrării efectuate de autorități și organisme publice.

Articolul 42

Certificare

(1) Statele membre, autoritățile de supraveghere, comitetul și Comisia încurajează, în special la nivelul Uniunii, instituirea de mecanisme de certificare în domeniul protecției datelor, precum și de sigilii și mărci în acest domeniu, care să permită demonstrarea faptului că operațiunile de prelucrare efectuate de operatori și de persoanele împuternicite de operatori respectă prezentul regulament. Sunt luate în considerare necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii.

- (2) Mecanismele de certificare din domeniul protecției datelor, sigiliile sau mărcile aprobate în temeiul alineatului (5) din prezentul articol sunt instituite nu numai pentru a fi respectate de operatorii sau de persoanele împuternicite de operatori care fac obiectul prezentului regulament, ci și pentru a demonstra existența unor garanții adecvate oferite de operatorii sau de persoanele împuternicite de operatori care nu fac obiectul prezentului regulament, în temeiul articolului 3, în cadrul transferurilor de date cu caracter personal către țări terțe sau organizații internaționale în condițiile menționate la articolul 46 alineatul (2) litera (f). Acești operatori sau persoane împuternicite de operatori își asumă angajamente cu caracter obligatoriu și executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, în scopul aplicării garanțiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.
- (3) Certificarea este voluntară și disponibilă prin intermediul unui proces transparent.
- (4) Certificarea în conformitate cu prezentul articol nu reduce responsabilitatea operatorului sau a persoanei împuternicite de operator de a respecta prezentul regulament și nu aduce atingere sarcinilor și competențelor autorităților de supraveghere care sunt competente în temeiul articolului 55 sau 56.
- (5) Organismele de certificare menționate la articolul 43 sau autoritatea de supraveghere competentă emit o certificare în temeiul prezentului articol, pe baza criteriilor aprobate de către autoritatea de supraveghere competentă respectivă în temeiul articolului 58 alineatul (3), sau de către comitet în temeiul articolului 63. În cazul în care criteriile sunt aprobate de comitet, aceasta poate duce la o certificare comună, și anume sigiliul european privind protecția datelor.
- (6) Operatorul sau persoana împuternicită de operator care supune activitățile sale de prelucrare mecanismului de certificare oferă organismului de certificare menționat la articolul 43 sau, după caz, autorității de supraveghere competente, toate informațiile necesare pentru desfășurarea procedurii de certificare, precum și accesul la activitățile de prelucrare respective.
- (7) Certificarea este eliberată unui operator sau unei persoane împuternicite de operator pentru o perioadă maximă de trei ani și poate fi reînnoită în aceleași condiții, cu condiția ca cerințele relevante să fie îndeplinite în continuare. Certificarea este retrasă, după caz, de către organismele de certificare menționate la articolul 43 sau de către autoritatea de supraveghere competentă în cazul în care nu mai sunt îndeplinite cerințele pentru certificare.
- (8) Comitetul regroupează toate mecanismele de certificare și sigiliile și mărcile de protecție a datelor într-un registru și le pune la dispoziția publicului prin orice mijloc corespunzător.

Articolul 43

Organisme de certificare

- (1) Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente, prevăzute la articolele 57 și 58, organismele de certificare care dispun de un nivel adecvat de competență în domeniul protecției datelor, după ce informează autoritatea de supraveghere pentru a-i permite să își exercite competențele în temeiul articolului 58 alineatul (2) litera (h), emit și reînnoiesc certificarea. Statele membre se asigură că aceste organisme de certificare sunt acreditate de către una sau amândouă dintre următoarele entități:
- (a) autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56;
- (b) organismul național de acreditare desemnat în conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului ⁽¹⁾ în conformitate cu standardul EN-ISO/IEC 17065/2012 și cu cerințele suplimentare stabilite de autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56.
- (2) Un organism de certificare menționat la alineatul (1) este acreditat în conformitate cu alineatul respectiv numai dacă:
- (a) a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, independența și expertiza sa în legătură cu obiectul certificării;

⁽¹⁾ Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93 (JO L 218, 13.8.2008, p. 30)

- (b) s-a angajat să respecte criteriile menționate la articolul 42 alineatul (5) și aprobate de autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56, sau de către comitet în temeiul articolului 63;
- (c) a instituit proceduri pentru emiterea, revizuirea periodică și retragerea certificării, a sigiliilor și mărcilor din domeniul protecției datelor;
- (d) a instituit proceduri și structuri pentru tratarea plângerilor privind încălcări ale certificării sau privind modul în care certificarea a fost sau este pusă în aplicare de un operator sau o persoană împuternicită de operator, precum și pentru asigurarea transparenței acestor proceduri și structuri pentru persoanele vizate și pentru public; și
- (e) a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, că sarcinile și atribuțiile sale nu creează conflicte de interese.
- (3) Accreditarea organismelor de certificare menționate la alineatele (1) și (2) din prezentul articol se realizează pe baza criteriilor aprobate de către autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56, sau de către comitet în temeiul articolului 63. În cazul unei acreditări în conformitate cu alineatul (1) litera (b) din prezentul articol, aceste cerințe le completează pe cele prevăzute în Regulamentul (CE) nr. 765/2008 și normele tehnice care descriu metodele și procedurile organismelor de certificare.
- (4) Organismele de certificare menționate la alineatul (1) sunt responsabile cu realizarea unei evaluări adecvate în vederea certificării sau retragerii acestei certificări, fără a aduce atingere responsabilității operatorului sau a persoanei împuternicite de operator de a respecta prezentul regulament. Accreditarea se eliberează pentru o perioadă maximă de cinci ani și poate fi reînnoită în aceleași condiții, cu condiția ca organismul de certificare să îndeplinească cerințele prevăzute în prezentul articol.
- (5) Organismele de certificare menționate la alineatul (1) transmite autorităților de supraveghere competente motivele acordării sau retragerii certificării solicitate.
- (6) Cerințele menționate la alineatul (3) din prezentul articol și criteriile menționate la articolul 42 alineatul (5) se publică de către autoritatea de supraveghere într-o formă ușor de accesat. Autoritățile de supraveghere transmit, de asemenea, aceste cerințe și criterii comitetului. Comitetul regroupează toate mecanismele de certificare și sigiliile de protecție a datelor într-un registru și le pune la dispoziția publicului prin orice mijloc corespunzător.
- (7) Fără a aduce atingere dispozițiilor capitolului VIII, autoritatea de supraveghere competentă sau organismul național de acreditare revocă acreditarea acordată unui organism de certificare în temeiul alineatului (1) din prezentul articol în cazul în care nu sunt sau nu mai sunt îndeplinite condițiile pentru acreditare sau măsurile luate de organismul de acreditare încalcă prezentul regulament.
- (8) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 92, în scopul specificării cerințelor care trebuie luate în considerare pentru mecanismele de certificare din domeniul protecției datelor, menționate la articolul 42 alineatul (1).
- (9) Comisia poate adopta acte de punere în aplicare pentru a stabili standarde tehnice pentru mecanismele de certificare și pentru sigiliile și mărcile din domeniul protecției datelor, precum și mecanisme de promovare și recunoaștere a acelor mecanisme de certificare, sigilii și mărci. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2).

CAPITOLUL V

Transferurile de date cu caracter personal către țări terțe sau organizații internaționale

Articolul 44

Principiul general al transferurilor

Orice date cu caracter personal care fac obiectul prelucrării sau care urmează a fi prelucrate după ce sunt transferate într-o țară terță sau către o organizație internațională pot fi transferate doar dacă, sub rezerva celorlalte dispoziții ale prezentului regulament, condițiile prevăzute în prezentul capitol sunt respectate de operator și de persoana împuternicită de operator, inclusiv în ceea ce privește transferurile ulterioare de date cu caracter personal din țara terță sau de la organizația internațională către o altă țară terță sau către o altă organizație internațională. Toate dispozițiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice garantat prin prezentul regulament nu este subminat.

Articolul 45

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

(1) Transferul de date cu caracter personal către o țară terță sau o organizație internațională se poate realiza atunci când Comisia a decis că țara terță, un teritoriu ori unul sau mai multe sectoare specificate din acea țară terță sau organizația internațională în cauză asigură un nivel de protecție adecvat. Transferurile realizate în aceste condiții nu necesită autorizări speciale.

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

- (a) statul de drept, respectarea drepturilor omului și a libertăților fundamentale, legislația relevantă, atât generală, cât și sectorială, inclusiv privind securitatea publică, apărarea, securitatea națională și dreptul penal, precum și accesul autorităților publice la datele cu caracter personal, precum și punerea în aplicare a acestei legislații, normele de protecție a datelor, normele profesionale și măsurile de securitate, inclusiv normele privind transferul ulterior de date cu caracter personal către o altă țară terță sau organizație internațională, care sunt respectate în țara terță respectivă sau în organizația internațională respectivă, jurisprudența, precum și existența unor drepturi efective și opozabile ale persoanelor vizate și a unor reparații efective pe cale administrativă și judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate;
- (b) existența și funcționarea eficientă a uneia sau mai multor autorități de supraveghere independente în țara terță sau sub jurisdicția cărora intră o organizație internațională, cu responsabilitate pentru asigurarea și impunerea respectării normelor de protecție a datelor, incluzând competențe adecvate de asigurare a respectării aplicării, pentru acordarea de asistență și consiliere persoanelor vizate cu privire la exercitarea drepturilor acestora și pentru cooperarea cu autoritățile de supraveghere din statele membre; și
- (c) angajamentele internaționale la care a aderat țara terță sau organizația internațională în cauză sau alte obligații care decurg din convenții sau instrumente obligatorii din punct de vedere juridic, precum și din participarea acesteia la sisteme multilaterale sau regionale, mai ales în domeniul protecției datelor cu caracter personal.

(3) Comisia, după ce evaluează caracterul adecvat al nivelului de protecție, poate decide, printr-un act de punere în aplicare, că o țară terță, un teritoriu sau unul sau mai multe sectoare specificate dintr-o țară terță sau o organizație internațională asigură un nivel de protecție adecvat în sensul alineatului (2) din prezentul articol. Actul de punere în aplicare prevede un mecanism de revizuire periodică, cel puțin o dată la patru ani, care ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională. Actul de punere în aplicare menționează aplicarea geografică și sectorială, și, după caz, identifică autoritatea sau autoritățile de supraveghere menționate la alineatul (2) litera (b) din prezentul articol. Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2).

(4) Comisia monitorizează continuu evoluțiile din țările terțe și de la nivelul organizațiilor internaționale care ar putea afecta funcționarea deciziilor adoptate în temeiul alineatului (3) din prezentul articol și a deciziilor adoptate în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE.

(5) În cazul în care informațiile disponibile dezvăluie, în special în urma revizuirii menționate la alineatul (3) din prezentul articol, că o țară terță, un teritoriu sau un sector specificat din acea țară terță sau o organizație internațională nu mai asigură un nivel de protecție adecvat în sensul alineatului (2) din prezentul articol, Comisia, dacă este necesar, abrogă, modifică sau suspendă, prin intermediul unui act de punere în aplicare, decizia menționată la alineatul (3) din prezentul articol fără efect retroactiv. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2).

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

(6) Comisia inițiază consultări cu țara terță sau organizația internațională în vederea remedierii situației care a stat la baza deciziei luate în conformitate cu alineatul (5).

(7) O decizie luată în temeiul alineatului (5) din prezentul articol nu aduce atingere transferurilor de date cu caracter personal către țara terță, un teritoriu sau unul sau mai multe sectoare specificate din acea țară terță sau către organizația internațională în cauză în conformitate cu articolele 46-49.

(8) Comisia publică în *Jurnalul Oficial al Uniunii Europene* și pe site-ul său o listă a țărilor terțe, a teritoriilor și a sectoarelor specificate dintr-o țară terță și a organizațiilor internaționale în cazul cărora a decis că nivelul de protecție adecvat este asigurat sau nu mai este asigurat.

(9) Deciziile adoptate de Comisie în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE rămân în vigoare până când sunt modificate, înlocuite sau abrogate de o decizie a Comisiei adoptată în conformitate cu alineatul (3) sau (5) din prezentul articol.

Articolul 46

Transferuri în baza unor garanții adecvate

(1) În absența unei decizii în temeiul articolului 45 alineatul (3), operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o țară terță sau o organizație internațională numai dacă operatorul sau persoana împuternicită de operator a oferit garanții adecvate și cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate.

(2) Garanțiile adecvate menționate la alineatul 1 pot fi furnizate fără să fie nevoie de nicio autorizație specifică din partea unei autorități de supraveghere, prin:

(a) un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;

(b) reguli corporatiste obligatorii în conformitate cu articolul 47;

(c) clauze standard de protecție a datelor adoptate de Comisie în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2);

(d) clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisie în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2);

(e) un cod de conduită aprobat în conformitate cu articolul 40, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

(f) un mecanism de certificare aprobat în conformitate cu articolul 42, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

(3) Sub rezerva autorizării din partea autorității de supraveghere competente, garanțiile adecvate menționate la alineatul (1) pot fi furnizate de asemenea, în special, prin:

(a) clauze contractuale între operator sau persoana împuternicită de operator și operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din țara terță sau organizația internațională; sau

(b) dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate.

(4) Autoritatea de supraveghere aplică mecanismul pentru asigurarea coerenței menționat la articolul 63, în cazurile menționate la alineatul (3) din prezentul articol.

(5) Autorizațiile acordate de un stat membru sau de o autoritate de supraveghere în temeiul articolului 26 alineatul (2) din Directiva 95/46/CE sunt valabile până la data la care sunt modificate, înlocuite sau abrogate, dacă este necesar, de respectiva autoritate de supraveghere. Deciziile adoptate de Comisie în temeiul articolului 26 alineatul (4) din Directiva 95/46/CE rămân în vigoare până când sunt modificate, înlocuite sau abrogate, dacă este necesar, de o decizie a Comisiei adoptată în conformitate cu alineatul (2) din prezentul articol.

Articolul 47

Reguli corporatiste obligatorii

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

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

- (b) să confere, în mod expres, drepturi opozabile persoanelor vizate în ceea ce privește prelucrarea datelor lor cu caracter personal; și
 - (c) să îndeplinească cerințele prevăzute la alineatul (2).
- (2) Regulile corporatiste obligatorii menționate la alineatul (1) precizează cel puțin:
- (a) structura și datele de contact ale grupului de întreprinderi sau ale grupului de întreprinderi implicate într-o activitate economică comună și ale fiecăruia dintre membrii săi;
 - (b) transferurile de date sau setul de transferuri, inclusiv categoriile de date cu caracter personal, tipul prelucrării și scopurile prelucrării, tipurile de persoane vizate afectate și identificarea țării terțe sau a țărilor terțe în cauză;
 - (c) caracterul lor juridic obligatoriu, atât pe plan intern, cât și extern;
 - (d) aplicarea principiilor generale în materie de protecție a datelor, în special limitarea scopului, reducerea la minimum a datelor, perioadele de stocare limitate, calitatea datelor, protecția datelor începând cu momentul conceperii și protecția implicită, temeiul juridic pentru prelucrare, prelucrarea categoriilor speciale de date cu caracter personal, măsurile de asigurare a securității datelor, precum și cerințele referitoare la transferurile ulterioare către organisme care nu fac obiectul regulilor corporatiste obligatorii;
 - (e) drepturile persoanelor vizate în ceea ce privește prelucrarea și mijloacele de exercitare a acestor drepturi, inclusiv dreptul de a nu face obiectul unor decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, în conformitate cu articolul 22, dreptul de a depune o plângere în fața autorității de supraveghere competente și în fața instanțelor competente ale statelor membre, în conformitate cu articolul 79, precum și dreptul de a obține reparații și, după caz, despăgubiri pentru încălcarea regulilor corporatiste obligatorii;
 - (f) acceptarea de către operator sau de persoana împuternicită de operator, care își are sediul pe teritoriul unui stat membru, a răspunderii pentru orice încălcare a regulilor corporatiste obligatorii de către orice membru în cauză care nu își are sediul în Uniune; operatorul sau persoana împuternicită de operator este exonerat(ă) de această răspundere, integral sau parțial, numai dacă dovedește că membrul respectiv nu a fost răspunzător de evenimentul care a cauzat prejudiciul;
 - (g) modul în care informațiile privind regulile corporatiste obligatorii, în special privind dispozițiile menționate la literele (d), (e) și (f) de la prezentul alineat, sunt furnizate persoanelor vizate în completarea informațiilor menționate la articolele 13 și 14;
 - (h) sarcinile oricărui responsabil cu protecția datelor desemnat în conformitate cu articolul 37 sau ale oricărei alte persoane sau entități însărcinate cu monitorizarea respectării regulilor corporatiste obligatorii în cadrul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, a activităților de formare și a gestionării plângerilor;
 - (i) procedurile de formulare a plângerilor;
 - (j) mecanismele din cadrul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, menite să asigure verificarea conformității cu regulile corporatiste obligatorii. Aceste mecanisme includ auditurile privind protecția datelor și metodele de asigurare a acțiunilor corective menite să protejeze drepturile persoanei vizate. Rezultatele acestor verificări ar trebui să fie comunicate persoanei sau entității menționate la litera (h) și consiliului de administrație al întreprinderii care exercită controlul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună și ar trebui să fie puse la dispoziția autorității de supraveghere competente, la cerere;
 - (k) mecanismele de raportare și înregistrare a modificărilor aduse regulilor și de raportare a acestor modificări autorității de supraveghere;
 - (l) mecanismul de cooperare cu autoritatea de supraveghere în vederea asigurării respectării regulilor de către orice membru al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, în special prin punerea la dispoziția autorității de supraveghere a rezultatelor verificărilor cu privire la măsurile menționate la punctul (j);
 - (m) mecanismele de raportare către autoritatea de supraveghere competentă a oricăror cerințe legale impuse unui membru al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună într-o țară terță care pot avea un efect advers considerabil asupra garanțiilor furnizate prin regulile corporatiste obligatorii; și
 - (n) formarea corespunzătoare în domeniul protecției datelor a personalului care are un acces permanent sau periodic la date cu caracter personal.

(3) Comisia poate preciza formatul și procedurile pentru schimbul de informații între operatori, persoanele împuternicite de operatori și autoritățile de supraveghere pentru regulile corporatiste obligatorii în sensul prezentului articol. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 93 alineatul (2).

Articolul 48

Transferurile sau divulgările de informații neautorizate de dreptul Uniunii

Orice hotărâre a unei instanțe sau a unui tribunal și orice decizie a unei autorități administrative a unei țări terțe care impun unui operator sau persoanei împuternicite de operator să transfere sau să divulge date cu caracter personal poate fi recunoscută sau executată în orice fel numai dacă se bazează pe un acord internațional, cum ar fi un tratat de asistență judiciară reciprocă în vigoare între țara terță solicitantă și Uniune sau un stat membru, fără a se aduce atingere altor motive de transfer în temeiul prezentului capitol.

Articolul 49

Derogări pentru situații specifice

(1) În absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 45 alineatul (3) sau a unor garanții adecvate în conformitate cu articolul 46, inclusiv a regulilor corporatiste obligatorii, un transfer sau un set de transferuri de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc numai în una dintre condițiile următoare:

- (a) persoana vizată și-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a fost informată asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizată ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecție și a unor garanții adecvate;
- (b) transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;
- (c) transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;
- (d) transferul este necesar din considerente importante de interes public;
- (e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;
- (f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul;
- (g) transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau al dreptului intern, are scopul de a furniza informații publicului și care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în măsura în care sunt îndeplinite condițiile cu privire la consultare prevăzute de dreptul Uniunii sau de dreptul intern în acel caz specific.

În cazul în care un transfer nu ar putea să se întemeieze pe o dispoziție prevăzută la articolul 45 sau 46, inclusiv dispoziții privind reguli corporatiste obligatorii, și nu este aplicabilă niciuna dintre derogările pentru situații specifice prevăzute la primul paragraf din prezentul alineat, un transfer către o țară terță sau o organizație internațională poate avea loc numai în cazul în care transferul nu este repetitiv, se referă doar la un număr limitat de persoane vizate, este necesar în scopul realizării intereselor legitime majore urmărite de operator asupra căruia nu prevalează interesele sau drepturile și libertățile persoanei vizate și operatorul a evaluat toate circumstanțele aferente transferului de date și, pe baza acestei evaluări, a prezentat garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal. Operatorul informează autoritatea de supraveghere cu privire la transfer. Operatorul, în plus față de furnizarea informațiilor menționate la articolele 13 și 14, informează persoana vizată cu privire la transfer și la interesele legitime majore pe care le urmărește.

(2) Transferul în temeiul alineatului (1) primul paragraf litera (g) nu implică totalitatea datelor cu caracter personal sau ansamblul categoriilor de date cu caracter personal cuprinse în registru. Atunci când registrul urmează a fi consultat de către persoane care au un interes legitim, transferul se efectuează numai la cererea persoanelor respective sau în cazul în care acestea vor fi destinatarii.

- (3) Alineatul (1) primul paragraf literele (a), (b) și (c) și paragraful al doilea nu se aplică în cazul activităților desfășurate de autoritățile publice în exercitarea competențelor lor publice.
- (4) Interesul public prevăzut la alineatul (1) primul paragraf litera (d) este recunoscut în dreptul Uniunii sau în dreptul statului membru sub incidența căruia intră operatorul.
- (5) În absența unei decizii privind caracterul adecvat al nivelului de protecție, dreptul Uniunii sau dreptul intern poate, din considerente importante de interes public, să stabilească în mod expres limite asupra transferului unor categorii specifice de date cu caracter personal către o țară terță sau o organizație internațională. Statele membre notifică aceste dispoziții Comisiei.
- (6) Operatorul sau persoana împuternicită de operator consemnează evaluarea, precum și garanțiile adecvate prevăzute la paragraful al doilea al alineatului (1) din prezentul articol, în evidențele menționate la articolul 30.

Articolul 50

Cooperarea internațională în domeniul protecției datelor cu caracter personal

În ceea ce privește țările terțe și organizațiile internaționale, Comisia și autoritățile de supraveghere iau măsurile corespunzătoare pentru:

- (a) elaborarea de mecanisme de cooperare internațională pentru a facilita asigurarea aplicării efective a legislației privind protecția datelor cu caracter personal;
- (b) acordarea de asistență internațională reciprocă în asigurarea aplicării legislației din domeniul protecției datelor cu caracter personal, inclusiv prin notificare, transferul plângerilor, asistență în investigații și schimb de informații, sub rezerva unor garanții adecvate pentru protecția datelor cu caracter personal și a altor drepturi și libertăți fundamentale;
- (c) implicarea părților interesate relevante în discuțiile și activitățile care au ca scop intensificarea cooperării internaționale în domeniul aplicării legislației privind protecția datelor cu caracter personal;
- (d) promovarea schimbului reciproc și a documentației cu privire la legislația și practicile în materie de protecție a datelor cu caracter personal, inclusiv în ceea ce privește conflictele jurisdicționale cu țările terțe.

CAPITOLUL VI

Autorități de supraveghere independente

Secțiunea 1

Statutul independent

Articolul 51

Autoritatea de supraveghere

- (1) Fiecare stat membru se asigură că una sau mai multe autorități publice independente sunt responsabile de monitorizarea aplicării prezentului regulament, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea și în vederea facilitării liberei circulații a datelor cu caracter personal în cadrul Uniunii („autoritatea de supraveghere”).
- (2) Fiecare autoritate de supraveghere contribuie la aplicarea coerentă a prezentului regulament în întreaga Uniune. În acest scop, autoritățile de supraveghere cooperează atât între ele, cât și cu Comisia, în conformitate cu capitolul VII.
- (3) În cazul în care mai multe autorități de supraveghere sunt instituite într-un stat membru, acesta desemnează autoritatea de supraveghere care reprezintă autoritățile respective în cadrul comitetului și instituie un mecanism prin care să asigure respectarea de către celelalte autorități a normelor privind mecanismul pentru asigurarea coerenței prevăzut la articolul 63.
- (4) Fiecare stat membru notifică Comisiei dispozițiile de drept pe care le adoptă în temeiul prezentului capitol până la 25 mai 2018 și, fără întârziere, orice modificare ulterioară pe care o aduce acestor dispoziții.

*Articolul 52***Independență**

- (1) Fiecare autoritate de supraveghere beneficiază de independență deplină în îndeplinirea sarcinilor sale și exercitarea competențelor sale în conformitate cu prezentul regulament.
- (2) Membrul sau membrii fiecărei autorități de supraveghere, în cadrul îndeplinirii sarcinilor și al exercitării competențelor sale (lor) în conformitate cu prezentul regulament, rămâne (rămân) independent (independenți) de orice influență externă directă sau indirectă și nici nu solicită, nici nu acceptă instrucțiuni de la o parte externă.
- (3) Membrul sau membrii fiecărei autorități de supraveghere se abțin de la a întreprinde acțiuni incompatibile cu atribuțiile lor, iar pe durata mandatului, nu desfășoară activități incompatibile, remunerate sau nu.
- (4) Fiecare stat membru se asigură că fiecare autoritate de supraveghere beneficiază de resurse umane, tehnice și financiare, de un sediu și de infrastructura necesară pentru îndeplinirea sarcinilor și exercitarea efectivă a competențelor sale, inclusiv a celor care urmează să fie aplicate în contextul asistenței reciproce, al cooperării și al participării în cadrul comitetului.
- (5) Fiecare stat membru se asigură că fiecare autoritate de supraveghere își selectează personalul propriu și deține personal propriu aflat sub conducerea exclusivă a membrului sau membrilor autorității de supraveghere respective.
- (6) Fiecare stat membru se asigură că fiecare autoritate de supraveghere face obiectul unui control financiar care nu aduce atingere independenței sale și că dispune de bugete anuale distincte, publice, care pot face parte din bugetul general de stat sau național.

*Articolul 53***Condiții generale aplicabile membrilor autorității de supraveghere**

- (1) Statele membre se asigură că fiecare membru al autorității lor de supraveghere este numit prin intermediul unei proceduri transparente:
 - de parlament;
 - de guvern;
 - de șeful statului; sau
 - de un organism independent împuternicit să facă numiri în temeiul dreptului intern.
- (2) Fiecare membru în cauză are calificările, experiența și competențele necesare, în special în domeniul protecției datelor cu caracter personal, pentru a-și putea îndeplini atribuțiile și exercita competențele.
- (3) Atribuțiile unui membru încetează în cazul expirării mandatului, în cazul demisiei sau pensionării din oficiu în conformitate cu dreptul intern relevant.
- (4) Un membru poate fi demis doar în cazuri de abateri grave sau dacă nu mai îndeplinește condițiile necesare pentru îndeplinirea atribuțiilor sale.

*Articolul 54***Norme privind instituirea autorității de supraveghere**

- (1) Fiecare stat membru prevede, pe cale legislativă, următoarele:
 - (a) instituirea fiecărei autorități de supraveghere;

- (b) calificările și condițiile de eligibilitate necesare pentru a fi numit în calitate de membru al fiecărei autorități de supraveghere;
- (c) normele și procedurile pentru numirea membrului sau a membrilor fiecărei autorități de supraveghere;
- (d) durata mandatului membrului sau membrilor fiecărei autorități de supraveghere, de minimum patru ani, cu excepția primei numiri după 24 mai 2016, din care o parte poate fi pe o perioadă mai scurtă în cazul în care acest lucru este necesar pentru a proteja independența autorității de supraveghere printr-o procedură de numiri eșalonate;
- (e) dacă și de câte ori este eligibil pentru reînnoire mandatul membrului sau membrilor fiecărei autorități de supraveghere;
- (f) condițiile care reglementează obligațiile membrului sau membrilor și ale personalului fiecărei autorități de supraveghere, interdicții privind acțiunile, ocupațiile și beneficiile incompatibile cu acestea în cursul mandatului și după încetarea acestuia, precum și normele care reglementează încetarea contractului de angajare.

(2) Membrul sau membrii și personalul fiecărei autorități de supraveghere au obligația, în conformitate cu dreptul Uniunii sau cu dreptul intern, de a respecta atât pe parcursul mandatului, cât și după încetarea acestuia, secretul profesional în ceea ce privește informațiile confidențiale de care au luat cunoștință în cursul îndeplinirii sarcinilor sau al exercitării competențelor lor. Pe durata mandatului lor, această obligație de păstrare a secretului profesional se aplică în special în ceea ce privește raportarea de către persoane fizice a încălcărilor prezentului regulament.

Secțiunea 2

Abilitări, sarcini și competențe

Articolul 55

Competența

- (1) Fiecare autoritate de supraveghere are competența să îndeplinească sarcinile și să exercite competențele care îi sunt conferite în conformitate cu prezentul regulament pe teritoriul statului membru de care aparține.
- (2) În cazul în care prelucrarea este efectuată de autorități publice sau de organisme private care acționează pe baza literei (c) sau (e) de la articolul 6 alineatul (1), este autoritatea de supraveghere din statul membru respectiv. În astfel de cazuri, nu se aplică articolul 56.
- (3) Autoritățile de supraveghere nu sunt competente să supravegheze operațiunile de prelucrare ale instanțelor care acționează în exercițiul funcției lor judiciare.

Articolul 56

Competența autorității de supraveghere principale

- (1) Fără a aduce atingere articolului 55, autoritatea de supraveghere a sediului principal sau a sediului unic al operatorului sau al persoanei împuternicite de operator este competentă să acționeze în calitate de autoritate de supraveghere principală pentru prelucrarea transfrontalieră efectuată de respectivul operator sau respectiva persoană împuternicită în cauză în conformitate cu procedura prevăzută la articolul 60.
- (2) Prin derogare de la alineatul (1), fiecare autoritate de supraveghere este competentă să trateze o plângere depusă în atenția sa sau o eventuală încălcare a prezentului regulament, în cazul în care obiectul acesteia se referă numai la un sediu aflat în statul său membru sau afectează în mod semnificativ persoane vizate numai în statul său membru.
- (3) În cazurile menționate la alineatul (2) din prezentul articol, autoritatea de supraveghere informează fără întârziere autoritatea de supraveghere principală cu privire la această chestiune. În termen de trei săptămâni de la momentul informării, autoritatea de supraveghere principală decide dacă tratează sau nu cazul respectiv în conformitate cu procedura prevăzută la articolul 60, luând în considerare dacă există sau nu un sediu al operatorului sau al persoanei împuternicite de operator pe teritoriul statului membru a cărui autoritate de supraveghere a informat-o.

(4) În cazul în care autoritatea de supraveghere principală decide să trateze cazul, se aplică procedura prevăzută la articolul 60. Autoritatea de supraveghere care a informat autoritatea de supraveghere principală poate înainta un proiect de decizie acesteia din urmă. Autoritatea de supraveghere principală ține seama în cea mai mare măsură posibilă de proiectul respectiv atunci când pregătește proiectul de decizie prevăzut la articolul 60 alineatul (3).

(5) În cazul în care autoritatea de supraveghere principală decide să nu trateze cazul, autoritatea de supraveghere care a informat autoritatea de supraveghere principală tratează cazul în conformitate cu articolele 61 și 62.

(6) Autoritatea de supraveghere principală este singurul interlocutor al operatorului sau al persoanei împuternicite de operator în ceea ce privește prelucrarea transfrontalieră efectuată de respectivul operator sau de respectiva persoană împuternicită de operator.

Articolul 57

Sarcini

(1) Fără a aduce atingere altor sarcini stabilite în temeiul prezentului regulament, fiecare autoritate de supraveghere, pe teritoriul său:

- (a) monitorizează și asigură aplicarea prezentului regulament;
- (b) promovează acțiuni de sensibilizare și de înțelegere în rândul publicului a riscurilor, normelor, garanțiilor și drepturilor în materie de prelucrare. Se acordă atenție specială activităților care se adresează în mod specific copiilor;
- (c) oferă consiliere, în conformitate cu dreptul intern, parlamentului național, guvernului și altor instituții și organisme cu privire la măsurile legislative și administrative referitoare la protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea;
- (d) promovează acțiuni de sensibilizare a operatorilor și a persoanelor împuternicite de aceștia cu privire la obligațiile care le revin în temeiul prezentului regulament;
- (e) la cerere, furnizează informații oricărei persoane vizate în legătură cu exercitarea drepturilor sale în conformitate cu prezentul regulament și, dacă este cazul, cooperează cu autoritățile de supraveghere din alte state membre în acest scop;
- (f) tratează plângerile depuse de o persoană vizată, un organism, o organizație sau o asociație în conformitate cu articolul 80 și investighează într-o măsură adecvată obiectul plângerii și informează reclamantul cu privire la evoluția și rezultatul investigației, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigații mai amănunțite sau coordonarea cu o altă autoritate de supraveghere;
- (g) cooperează, inclusiv prin schimb de informații, cu alte autorități de supraveghere și își oferă asistență reciprocă pentru a asigura coerența aplicării și respectării prezentului regulament;
- (h) desfășoară investigații privind aplicarea prezentului regulament, inclusiv pe baza unor informații primite de la o altă autoritate de supraveghere sau de la o altă autoritate publică;
- (i) monitorizează evoluțiile relevante, în măsura în care acestea au impact asupra protecției datelor cu caracter personal, în special evoluția tehnologiilor informației și comunicațiilor și a practicilor comerciale;
- (j) adoptă clauze contractuale standard menționate la articolul 28 alineatul (8) și la articolul 46 alineatul (2) litera (d);
- (k) întocmește și menține la zi o listă în legătură cu cerința privind evaluarea impactului asupra protecției datelor, în conformitate cu articolul 35 alineatul (4);
- (l) oferă consiliere cu privire la operațiunile de prelucrare menționate la articolul 36 alineatul (2);
- (m) încurajează elaborarea de coduri de conduită în conformitate cu articolul 40 alineatul (1), își dă avizul cu privire la acestea și le aprobă pe cele care oferă suficiente garanții, în conformitate cu articolul 40 alineatul (5);
- (n) încurajează stabilirea unor mecanisme de certificare, precum și a unor sigilii și mărci în domeniul protecției datelor în conformitate cu articolul 42 alineatul (1) și aprobă criteriile de certificare în conformitate cu articolul 42 alineatul (5);
- (o) acolo unde este cazul, efectuează o revizuire periodică a certificărilor acordate, în conformitate cu articolul 42 alineatul (7);

- (p) elaborează și publică criteriile de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu articolul 41 și a unui organism de certificare în conformitate cu articolul 43;
 - (q) coordonează procedura de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu articolul 41 și a unui organism de certificare în conformitate cu articolul 43;
 - (r) autorizează clauzele și dispozițiile contractuale menționate la articolul 46 alineatul (3);
 - (s) aprobă regulile corporatiste obligatorii în conformitate cu articolul 47;
 - (t) contribuie la activitățile comitetului;
 - (u) menține la zi evidențe interne privind încălcările prezentului regulament și măsurile luate, în special avertismentele emise și sancțiunile impuse în conformitate cu articolul 58 alineatul (2); și
 - (v) îndeplinește orice alte sarcini legate de protecția datelor cu caracter personal.
- (2) Fiecare autoritate de supraveghere facilitează depunerea plângerilor menționate la alineatul (1) litera (f) prin măsuri precum punerea la dispoziție a unui formular de depunere a plângerii care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.
- (3) Îndeplinirea sarcinilor fiecărei autorități de supraveghere este gratuită pentru persoana vizată și, după caz, pentru responsabilul cu protecția datelor.
- (4) În cazul în care cererile sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, autoritatea de supraveghere poate percepe o taxă rezonabilă, bazată pe costurile administrative, sau poate refuza să le trateze. Sarcina de a demonstra caracterul evident nefondat sau excesiv al cererii revine autorității de supraveghere.

Articolul 58

Competențe

- (1) Fiecare autoritate de supraveghere are toate următoarele competențe de investigare:
- (a) de a da dispoziții operatorului și persoanei împuternicite de operator și, după caz, reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informații pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale;
 - (b) de a efectua investigații sub formă de audituri privind protecția datelor;
 - (c) de a efectua o revizuire a certificărilor acordate în temeiul articolului 42 alineatul (7);
 - (d) de a notifica operatorul sau persoana împuternicită de operator cu privire la presupusa încălcare a prezentului regulament;
 - (e) de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale;
 - (f) de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor, în conformitate cu dreptul Uniunii sau cu dreptul procesual intern.
- (2) Fiecare autoritate de supraveghere are toate următoarele competențe corective:
- (a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la posibilitatea ca operațiunile de prelucrare prevăzute să încalce dispozițiile prezentului regulament;
 - (b) de a emite muștrări adresate unui operator sau unei persoane împuternicite de operator în cazul în care operațiunile de prelucrare au încălcat dispozițiile prezentului regulament;
 - (c) de a da dispoziții operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-și exercita drepturile în temeiul prezentului regulament;

- (d) de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile prezentului regulament, specificând, după caz, modalitatea și termenul-limită pentru aceasta;
 - (e) de a obliga operatorul să informeze persoana vizată cu privire la o încălcare a protecției datelor cu caracter personal;
 - (f) de a impune o limitare temporară sau definitivă, inclusiv o interdicție asupra prelucrării;
 - (g) de a dispune rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării, în temeiul articolelor 16, 17 și 18, precum și notificarea acestor acțiuni destinatarilor cărora le-au fost divulgate datele cu caracter personal, în conformitate cu articolul 17 alineatul (2) și cu articolul 19;
 - (h) de a retrage o certificare sau de a obliga organismul de certificare să retragă o certificare eliberată în temeiul articolelor 42 și 43 sau de a obliga organismul de certificare să nu elibereze o certificare în cazul în care cerințele de certificare nu sunt sau nu mai sunt îndeplinite;
 - (i) de a impune amenzi administrative în conformitate cu articolul 83, în completarea sau în locul măsurilor menționate la prezentul alineat, în funcție de circumstanțele fiecărui caz în parte;
 - (j) de a dispune suspendarea fluxurilor de date către un destinatar dintr-o țară terță sau către o organizație internațională.
- (3) Fiecare autoritate de supraveghere are toate următoarele competențe de autorizare și de consiliere:
- (a) de a oferi consiliere operatorului în conformitate cu procedura de consultare prealabilă menționată la articolul 36;
 - (b) de a emite avize, din proprie inițiativă sau la cerere, parlamentului național, guvernului statului membru sau, în conformitate cu dreptul intern, altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal;
 - (c) de a autoriza prelucrarea menționată la articolul 36 alineatul (5), în cazul în care dreptul statului membru prevede o astfel de autorizare prealabilă;
 - (d) de a emite un aviz și de a aproba proiectele de coduri de conduită, în conformitate cu articolul 40 alineatul (5);
 - (e) de a acredita organismele de certificare în conformitate cu articolul 43;
 - (f) de a emite certificări și de a aproba criteriile de certificare în conformitate cu articolul 42 alineatul (5);
 - (g) de a adopta clauzele standard în materie de protecție a datelor menționate la articolul 28 alineatul (8) și la articolul 46 alineatul (2) litera (d);
 - (h) de a autoriza clauzele contractuale menționate la articolul 46 alineatul (3) litera (a);
 - (i) de a autoriza acordurile administrative menționate la articolul 46 alineatul (3) litera (b); și
 - (j) de a aproba reguli corporatiste obligatorii în conformitate cu articolul 47.
- (4) Exercitarea competențelor conferite autorității de supraveghere în temeiul prezentului articol face obiectul unor garanții adecvate, inclusiv căi de atac judiciare eficiente și procese echitabile, prevăzute în dreptul Uniunii și în dreptul intern în conformitate cu cartea.
- (5) Fiecare stat membru prevede, pe cale legislativă, faptul că autoritatea sa de supraveghere are competența de a aduce în fața autorităților judiciare cazurile de încălcare a prezentului regulament și, după caz, de a iniția sau de a se implica într-un alt mod în proceduri judiciare, în scopul de a asigura aplicarea dispozițiilor prezentului regulament.
- (6) Fiecare stat membru poate să prevadă în dreptul său faptul că autoritatea sa de supraveghere are competențe suplimentare, în afara celor menționate la alineatele (1), (2) și (3). Exercițarea acestor competențe nu afectează modul de operare eficientă a capitolului VII.

Articolul 59

Rapoarte de activitate

Fiecare autoritate de supraveghere întocmește un raport anual cu privire la activitățile sale, care poate include o listă a tipurilor de încălcări notificate și a tipurilor de măsuri luate în conformitate cu articolul 58 alineatul (2). Rapoartele se transmit parlamentului național, guvernului și altor autorități desemnate prin dreptul intern. Acestea se pun la dispoziția publicului, a Comisiei și a comitetului.

CAPITOLUL VII

Cooperare și coerență

Secțiunea 1

Cooperare

Articolul 60

Cooperarea dintre autoritatea de supraveghere principală și celelalte autorități de supraveghere vizate

- (1) Autoritatea de supraveghere principală cooperează cu celelalte autorități de supraveghere vizate, în conformitate cu prezentul articol, în încercarea de a ajunge la un consens. Autoritatea de supraveghere principală și autoritățile de supraveghere vizate își comunică reciproc toate informațiile relevante.
- (2) Autoritatea de supraveghere principală poate solicita în orice moment altor autorități de supraveghere vizate să ofere asistență reciprocă în temeiul articolului 61 și poate desfășura operațiuni comune în temeiul articolului 62, în special în vederea efectuării de investigații sau a monitorizării punerii în aplicare a unei măsuri referitoare la un operator sau o persoană împuternicită de operator, stabilit(ă) în alt stat membru.
- (3) Autoritatea de supraveghere principală comunică fără întârziere informațiile relevante referitoare la această chestiune celorlalte autorități de supraveghere vizate. Autoritatea de supraveghere principală transmite fără întârziere un proiect de decizie celorlalte autorități de supraveghere vizate, pentru a obține avizul lor, și ține seama în mod corespunzător de opiniile acestora.
- (4) În cazul în care oricare dintre celelalte autorități de supraveghere vizate exprimă, în termen de patru săptămâni după ce a fost consultată în conformitate cu alineatul (3) din prezentul articol, o obiecție relevantă și motivată la proiectul de decizie, autoritatea de supraveghere principală, în cazul în care nu dă curs obiecției relevante și motivate sau consideră că obiecția nu este relevantă sau motivată, sesizează mecanismul pentru asigurarea coerenței menționat la articolul 63.
- (5) În cazul în care intenționează să dea curs obiecției relevante și motivate formulate, autoritatea de supraveghere principală transmite celorlalte autorități de supraveghere vizate un proiect revizuit de decizie pentru a obține avizul acestora. Acest proiect revizuit de decizie face obiectul procedurii menționate la alineatul (4) pe parcursul unei perioade de două săptămâni.
- (6) În cazul în care niciuna dintre celelalte autorități de supraveghere vizate nu a formulat obiecții la proiectul de decizie transmis de autoritatea de supraveghere principală în termenul menționat la alineatele (4) și (5), se consideră că autoritatea de supraveghere principală și autoritățile de supraveghere vizate sunt de acord cu proiectul de decizie respectiv, care devine obligatoriu pentru acestea.
- (7) Autoritatea de supraveghere principală adoptă decizia și o notifică sediului principal sau sediului unic al operatorului sau al persoanei împuternicite de operator, după caz, și informează celelalte autorități de supraveghere vizate și comitetul cu privire la decizia în cauză, incluzând un rezumat al elementelor și motivelor relevante. Autoritatea de supraveghere la care a fost depusă plângerea informează reclamantul cu privire la decizie.
- (8) Prin derogare de la alineatul (7), în cazul în care o plângere este refuzată sau respinsă, autoritatea de supraveghere la care s-a depus plângerea adoptă decizia, o notifică reclamantului și informează operatorul cu privire la acest lucru.
- (9) În cazul în care autoritatea de supraveghere principală și autoritățile de supraveghere vizate sunt de acord să refuze sau să respingă anumite părți ale unei plângeri și să dea curs altor părți ale plângerii respective, se adoptă o decizie separată pentru fiecare dintre aceste părți. Autoritatea de supraveghere principală adoptă decizia pentru partea care vizează acțiunile referitoare la operator, o notifică sediului principal sau sediului unic al operatorului sau al persoanei împuternicite de operator de pe teritoriul statului membru în cauză și informează reclamantul cu privire la acest lucru, în timp ce autoritatea de supraveghere a reclamantului adoptă decizia pentru partea care vizează refuzarea sau respingerea plângerii respective, o notifică reclamantului și informează operatorul sau persoana împuternicită de operator cu privire la acest lucru.
- (10) În urma notificării deciziei autorității de supraveghere principale în temeiul alineatelor (7) și (9), operatorul sau persoana împuternicită de operator ia măsurile necesare pentru a se asigura că activitățile de prelucrare sunt în conformitate cu decizia în toate sediile sale din Uniune. Operatorul sau persoana împuternicită de operator notifică măsurile luate în vederea respectării deciziei autorității de supraveghere principale, care informează celelalte autorități de supraveghere vizate.

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

(12) Autoritatea de supraveghere principală și celelalte autorități de supraveghere vizate își furnizează reciproc informațiile solicitate în temeiul prezentului articol, pe cale electronică, utilizând un formular standard.

Articolul 61

Asistență reciprocă

(1) Autoritățile de supraveghere își furnizează reciproc informații relevante și asistență pentru a pune în aplicare prezentul regulament în mod coerent și instituie măsuri de cooperare eficace între ele. Asistența reciprocă se referă, în special, la cereri de informații și măsuri de supraveghere, cum ar fi cereri privind autorizări și consultări prealabile, inspecții și investigații.

(2) Fiecare autoritate de supraveghere ia toate măsurile corespunzătoare necesare pentru a răspunde unei cereri a unei alte autorități de supraveghere, fără întârzieri nejustificate și cel târziu în termen de o lună de la data primirii cererii. Aceste măsuri pot include, în special, transmiterea informațiilor relevante privind desfășurarea unei investigații.

(3) Cererile de asistență cuprind toate informațiile necesare, inclusiv scopul cererii și motivele care stau la baza acesteia. Informațiile care fac obiectul schimbului se utilizează numai în scopul în care au fost solicitate.

(4) Autoritatea de supraveghere solicitată nu poate refuza să dea curs cererii, cu excepția cazului în care:

- (a) nu are competență privind obiectul cererii sau măsurile pe care este solicitată să le execute; sau
- (b) a da curs cererii ar încălca prezentul regulament sau dreptul Uniunii sau dreptului intern sub incidența căruia intră autoritatea de supraveghere care a primit cererea.

(5) Autoritatea de supraveghere căreia i s-a adresat cererea informează autoritatea de supraveghere care a transmis cererea cu privire la rezultate sau, după caz, la progresele înregistrate ori măsurile întreprinse pentru a răspunde cererii. Autoritatea de supraveghere solicitată își motivează fiecare refuz de a da curs cererii în temeiul alineatului (4).

(6) Ca regulă, autoritățile de supraveghere solicitate furnizează informațiile solicitate de alte autorități de supraveghere pe cale electronică, utilizând un formular standard.

(7) Autoritățile de supraveghere solicitate nu percep nicio taxă pentru acțiunile întreprinse de acestea în temeiul unei cereri de asistență reciprocă. Autoritățile de supraveghere pot conveni asupra unor norme privind retribuițiile reciproce în cazul unor cheltuieli specifice rezultate în urma acordării de asistență reciprocă în situații excepționale.

(8) În cazul în care o autoritate de supraveghere nu furnizează informațiile menționate la alineatul (5) din prezentul articol în termen de o lună de la primirea cererii din partea altei autorități de supraveghere, aceasta din urmă poate adopta o măsură provizorie pe teritoriul propriului stat membru, în conformitate cu articolul 55 alineatul (1). În acest caz, necesitatea urgentă de a acționa în temeiul articolului 66 alineatul (1) este considerată a fi îndeplinită și necesită o decizie obligatorie urgentă din partea comitetului, în conformitate cu articolul 66 alineatul (2).

(9) Comisia, printr-un act de punere în aplicare, poate specifica forma și procedurile pentru asistența reciprocă menționată în prezentul articol, precum și modalitățile de schimb de informații pe cale electronică între autoritățile de supraveghere și între autoritățile de supraveghere și comitet, în special formularul standard menționat la alineatul (6) din prezentul articol. Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2).

Articolul 62

Operațiuni comune ale autorităților de supraveghere

(1) După caz, autoritățile de supraveghere desfășoară operațiuni comune, inclusiv investigații comune și măsuri comune de aplicare a legii, în care sunt implicați membri sau personal din autoritățile de supraveghere ale altor state membre.

(2) În cazul în care operatorul sau persoana împuternicită de operator deține sedii în mai multe state membre sau dacă un număr semnificativ de persoane vizate din mai multe state membre sunt susceptibile de a fi afectate în mod semnificativ de operațiuni de prelucrare, o autoritate de supraveghere din fiecare dintre statele membre respective are dreptul de a participa la operațiunile comune. Autoritatea de supraveghere care este competentă în conformitate cu articolul 56 alineatul (1) sau alineatul (4) invită autoritățile de supraveghere din fiecare dintre aceste state membre să ia parte la operațiunile comune respective și răspunde fără întârziere la cererea de participare a unei autorități de supraveghere.

(3) O autoritate de supraveghere poate, în conformitate cu dreptul intern și cu acordul autorității de supraveghere din statul membru de origine, să acorde competențe, inclusiv competențe de investigare, membrilor sau personalului autorității de supraveghere din statul membru de origine implicați în operațiuni comune sau, în măsura în care dreptul statului membru al autorității de supraveghere din statul membru de primire permite acest lucru, poate autoriza membrii sau personalul autorității de supraveghere din statul membru de origine să își exercite competențele de investigare în conformitate cu dreptul statului membru al acestei din urmă autorități. Astfel de competențe de investigare pot fi exercitate doar sub coordonarea și în prezența membrilor sau personalului autorității de supraveghere din statul membru de primire. Membrii sau personalul autorității de supraveghere din statul membru de origine sunt supuși dreptului intern sub incidența căruia intră autoritatea de supraveghere din statul membru de primire.

(4) În cazul în care, în conformitate cu alineatul (1), personalul unei autorități de supraveghere din statul membru de origine își desfășoară activitatea într-un alt stat membru, statul membru de primire își asumă responsabilitatea pentru acțiunile personalului respectiv, inclusiv răspunderea pentru eventualele prejudicii cauzate de membrii personalului respectiv în cursul operațiunilor acestora, în conformitate cu dreptul statului membru pe teritoriul căruia își desfășoară operațiunile.

(5) Statul membru pe teritoriul căruia s-au produs prejudiciile repară aceste prejudicii în condițiile aplicabile prejudiciilor cauzate de propriul său personal. Statul membru de origine al autorității de supraveghere al cărei personal a cauzat prejudicii unei persoane de pe teritoriul unui alt stat membru rambursează acestui alt stat membru totalitatea sumelor pe care le-a plătit persoanelor îndreptățite în numele acestora.

(6) Fără a aduce atingere exercitării drepturilor sale față de terțe părți și cu excepția alineatului (5), fiecare stat membru se abține, în cazul prevăzut la alineatul (1), de la a pretinde de la un alt stat membru rambursarea despăgubirilor pentru prejudiciile menționate la alineatul (4).

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

Secțiunea 2

Asigurarea coerenței

Articolul 63

Mecanismul pentru asigurarea coerenței

Pentru a contribui la aplicarea coerentă a prezentului regulament în întreaga Uniune, autoritățile de supraveghere cooperează între ele și, după caz, cu Comisia prin mecanismul pentru asigurarea coerenței, astfel cum se prevede în prezenta secțiune.

Articolul 64

Avizul comitetului

(1) Comitetul emite un aviz de fiecare dată când o autoritate de supraveghere competentă intenționează să adopte oricare dintre măsurile de mai jos. În acest scop, autoritatea de supraveghere competentă comunică proiectul de decizie comitetului, atunci când:

- (a) vizează adoptarea unei liste de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor, în conformitate cu articolul 35 alineatul (4);
- (b) în conformitate cu articolul 40 alineatul (7), se referă la conformitatea cu prezentul regulament a unui proiect de cod de conduită sau a unei modificări sau extinderi a unui cod de conduită;

- (c) vizează aprobarea criteriilor pentru acreditarea unui organism în conformitate cu articolul 41 alineatul (3) sau a unui organism de certificare în conformitate cu articolul 43 alineatul (3);
- (d) vizează determinarea clauzelor standard în materie de protecție a datelor menționate la articolul 46 alineatul (2) litera (d) sau la articolul 28 alineatul (8);
- (e) vizează autorizarea clauzelor contractuale menționate la articolul 46 alineatul (3) litera (a); sau
- (f) vizează aprobarea regulilor corporatiste obligatorii în sensul articolului 47.
- (2) Orice autoritate de supraveghere, președintele comitetului sau Comisia poate solicita ca orice chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru să fie examinată de comitet în vederea obținerii unui aviz, în special în cazul în care o autoritate de supraveghere competentă nu respectă obligațiile privind asistența reciprocă în conformitate cu articolul 61 sau privind operațiunile comune în conformitate cu articolul 62.
- (3) În cazurile menționate la alineatele (1) și (2), comitetul emite un aviz cu privire la chestiunea care îi este prezentată, cu condiția să nu fi emis deja un aviz cu privire la aceeași chestiune. Avizul respectiv este adoptat în termen de opt săptămâni cu majoritatea simplă a membrilor comitetului. Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea chestiunii. În ceea ce privește proiectul de decizie menționat la alineatul (1) transmis membrilor comitetului în conformitate cu alineatul (5), un membru care nu a emis obiecții într-un termen rezonabil indicat de președinte se consideră a fi de acord cu proiectul de decizie.
- (4) Autoritățile de supraveghere și Comisia comunică pe cale electronică comitetului, fără întârzieri nejustificate, printr-un formular standard, orice informație relevantă, inclusiv, după caz, o sinteză a faptelor, proiectul de decizie, motivele care fac necesară adoptarea unei astfel de măsuri, precum și opiniile altor autorități de supraveghere vizate.
- (5) Președintele comitetului informează pe cale electronică, fără întârzieri nejustificate:
- (a) membrii comitetului și Comisia cu privire la orice informație relevantă care i-a fost comunicată, utilizând un formular standard. Secretariatul comitetului furnizează traduceri ale informațiilor relevante, acolo unde este necesar; și
- (b) autoritatea de supraveghere menționată, după caz, la alineatele (1) și (2), și Comisia cu privire la aviz și îl publică.
- (6) Autoritatea de supraveghere competentă nu își adoptă proiectul de decizie menționat la alineatul (1) în termenul menționat la alineatul (3).
- (7) Autoritatea de supraveghere menționată la alineatul (1) ține seama pe deplin de avizul comitetului și comunică pe cale electronică președintelui comitetului, în termen de două săptămâni de la primirea avizului, dacă își va păstra sau își va modifica proiectul de decizie și, dacă este cazul, transmite proiectul de decizie modificat, utilizând un formular standard.
- (8) În cazul în care autoritatea de supraveghere vizată informează președintele comitetului, în termenul menționat la alineatul (7) din prezentul articol, că intenționează să nu se conformeze avizului comitetului, integral sau parțial, oferind motivele relevante, se aplică articolul 65 alineatul (1).

Articolul 65

Soluționarea litigiilor de către comitet

- (1) Pentru a asigura aplicarea corectă și coerentă a prezentului regulament în cazuri individuale, comitetul adoptă o decizie obligatorie în următoarele cazuri:
- (a) atunci când, în unul dintre cazurile menționate la articolul 60 alineatul (4), o autoritate de supraveghere vizată a formulat o obiecție relevantă și motivată la un proiect de decizie a autorității principale sau autoritatea principală a respins o astfel de obiecție ca nefiind relevantă sau motivată. Decizia obligatorie se referă la toate chestiunile vizate de obiecția relevantă și motivată, în special la chestiunea dacă prezentul regulament a fost încălcat;

- (b) în cazul în care există opinii divergente cu privire la care dintre autoritățile de supraveghere vizate deține competența pentru sediul principal;
- (c) în cazul în care o autoritate de supraveghere competentă nu solicită avizul comitetului în cazurile menționate la articolul 64 alineatul (1) sau nu ține seama de avizul comitetului emis în temeiul articolului 64. În acest caz, orice autoritate de supraveghere vizată sau Comisia poate comunica chestiunea comitetului.
- (2) Decizia menționată la alineatul (1) se adoptă în termen de o lună de la prezentarea chestiunii, cu o majoritate de două treimi a membrilor comitetului. Acest termen poate fi prelungit cu o lună, ținându-se seama de complexitatea chestiunii. Decizia menționată la alineatul (1) se motivează și se adresează autorității de supraveghere principale și tuturor autorităților de supraveghere vizate, fiind obligatorie pentru acestea.
- (3) În cazul în care comitetul nu a fost în măsură să adopte o decizie în termenele menționate la alineatul (2), acesta își adoptă decizia în termen de două săptămâni de la data expirării celei de a doua luni menționate la alineatul (2), cu o majoritate simplă a membrilor săi. În cazul în care membrii comitetului au opinii divergente în proporții egale, decizia se adoptă prin votul președintelui.
- (4) Autoritățile de supraveghere vizate nu adoptă o decizie asupra chestiunii prezentate comitetului în conformitate cu alineatul (1) în termenele menționate la alineatele (2) și (3).
- (5) Președintele comitetului notifică, fără întârzieri nejustificate, decizia menționată la alineatul (1) autorităților de supraveghere vizate. Comitetul informează Comisia cu privire la acest lucru. Decizia se publică pe site-ul comitetului, fără întârziere, după notificarea de către autoritatea de supraveghere a deciziei finale menționate la alineatul (6).
- (6) Autoritatea de supraveghere principală sau, dacă este cazul, autoritatea de supraveghere la care s-a depus plângerea își adoptă decizia finală pe baza deciziei menționate la alineatul (1) din prezentul articol, fără întârziere nejustificată și în termen de cel mult o lună de la notificarea de către comitet a deciziei sale. Autoritatea de supraveghere principală sau, dacă este cazul, autoritatea de supraveghere la care s-a depus plângerea informează comitetul cu privire la data la care decizia sa finală este notificată operatorului sau persoanei împuternicite de operator și, respectiv, persoanei vizate. Decizia finală a autorităților de supraveghere vizate se adoptă în conformitate cu condițiile prevăzute la articolul 60 alineatele (7), (8) și (9). Decizia finală se referă la decizia menționată la alineatul (1) din prezentul articol și precizează faptul că decizia menționată la respectivul alineat va fi publicată pe site-ul al comitetului, în conformitate cu alineatul (5). La decizia finală se anexează decizia menționată la alineatul (1) din prezentul articol.

Articolul 66

Procedura de urgență

- (1) În circumstanțe excepționale, atunci când o autoritate de supraveghere vizată consideră că există o necesitate urgentă de a acționa în scopul protejării drepturilor și libertăților persoanelor vizate, aceasta poate, prin derogare de la mecanismul pentru asigurarea coerenței menționat la articolele 63, 64 și 65 sau de la procedura menționată la articolul 60, să adopte de îndată măsuri provizorii menite să producă efecte juridice pe propriul său teritoriu, cu o perioadă de valabilitate determinată, care să nu depășească trei luni. Autoritatea de supraveghere comunică fără întârziere aceste măsuri și motivele adoptării lor celorlalte autorități de supraveghere vizate, comitetului și Comisiei.
- (2) În cazul în care o autoritate de supraveghere a adoptat o măsură în temeiul alineatului (1) și consideră că este necesară adoptarea de urgență a unor măsuri definitive, aceasta poate solicita un aviz de urgență sau o decizie obligatorie urgentă din partea comitetului, indicând motivele pentru această solicitare.
- (3) Orice autoritate de supraveghere poate solicita un aviz de urgență sau o decizie obligatorie urgentă, după caz, din partea comitetului în cazul în care o autoritate de supraveghere competentă nu a luat o măsură adecvată într-o situație în care există o necesitate urgentă de a acționa pentru a proteja drepturile și libertățile persoanelor vizate, indicând motivele pentru solicitarea unui astfel de aviz sau a unei astfel de decizii, inclusiv pentru necesitatea urgentă de a acționa.
- (4) Prin derogare de la articolul 64 alineatul (3) și de la articolul 65 alineatul (2), un aviz de urgență sau o decizie obligatorie urgentă menționat(ă) la alineatele (2) și (3) de la prezentul articol este adoptat(ă) în termen de două săptămâni cu majoritate simplă a membrilor comitetului.

*Articolul 67***Schimb de informații**

Comisia poate adopta acte de punere în aplicare cu un domeniu de aplicare general pentru a defini modalitățile de realizare a schimbului electronic de informații între autoritățile de supraveghere, precum și între autoritățile de supraveghere și comitet, în special formularul standard menționat la articolul 64.

Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2).

*Secțiunea 3***Comitetul european pentru protecția datelor***Articolul 68***Comitetul european pentru protecția datelor**

- (1) Comitetul european pentru protecția datelor („comitetul”) este instituit ca organ al Uniunii și are personalitate juridică.
- (2) Comitetul este reprezentat de președintele său.
- (3) Comitetul este alcătuit din șeful unei autorități de supraveghere din fiecare stat membru și din Autoritatea Europeană pentru Protecția Datelor sau reprezentanții respectivi ai acestora.
- (4) În cazul în care într-un stat membru mai multe autorități de supraveghere sunt responsabile de monitorizarea aplicării dispozițiilor adoptate în temeiul prezentului regulament, se numește un reprezentant comun în conformitate cu dreptul intern al statului membru respectiv.
- (5) Comisia are dreptul de a participa la activitățile și reuniunile comitetului fără a avea drept de vot. Comisia numește un reprezentant. Președintele comitetului comunică Comisiei activitățile comitetului.
- (6) În cazurile menționate la articolul 65, Autoritatea Europeană pentru Protecția Datelor deține drept de vot numai cu privire la deciziile care privesc principiile și normele aplicabile în ceea ce privește instituțiile, organismele, oficiile și agențiile Uniunii care corespund pe fond cu cele din prezentul regulament.

*Articolul 69***Independență**

- (1) Comitetul acționează independent în îndeplinirea sarcinilor sale sau în exercitarea competențelor sale în conformitate cu articolele 70 și 71.
- (2) Fără a aduce atingere solicitărilor din partea Comisiei menționate la articolul 70 alineatul (1) litera (b) și la articolul 70 alineatul (2), comitetul, în îndeplinirea sarcinilor sale sau în exercitarea competențelor sale, nu solicită și nu acceptă instrucțiuni de la nicio parte externă.

*Articolul 70***Sarcinile comitetului**

- (1) Comitetul asigură aplicarea coerentă a prezentului regulament. În acest scop, din proprie inițiativă sau, după caz, la solicitarea Comisiei, comitetul are, în special, următoarele sarcini:
 - (a) să monitorizeze și să asigure aplicarea corectă a prezentului regulament, în cazurile prevăzute la articolele 64 și 65, fără a aduce atingere sarcinilor autorităților naționale de supraveghere;

- (b) să ofere consiliere Comisiei cu privire la orice aspect legat de protecția datelor cu caracter personal în cadrul Uniunii, inclusiv cu privire la orice propunere de modificare a prezentului regulament;
- (c) să ofere consiliere Comisiei cu privire la formatul și procedurile pentru schimbul de informații între operatori, persoanele împuternicite de operatori și autoritățile de supraveghere pentru regulile corporatiste obligatorii;
- (d) să emită orientări, recomandări și bune practici privind procedurile de ștergere a linkurilor către datele cu caracter personal, a copiilor sau a reproducerilor acestora de care dispun serviciile de comunicații accesibile publicului, astfel cum se menționează la articolul 17 alineatul (2);
- (e) să examineze, din proprie inițiativă, la cererea unuia dintre membrii săi sau la cererea Comisiei, orice chestiune referitoare la aplicarea prezentului regulament și să emită orientări, recomandări și bune practici pentru a încuraja aplicarea coerentă a prezentului regulament;
- (f) să emită orientări, recomandări și bune practici în conformitate cu prezentul alineat litera (e) în vederea detalierii criteriilor și condițiilor pentru deciziile bazate pe crearea de profiluri menționate la articolul 22 alineatul (2);
- (g) să emită orientări, recomandări și bune practici în conformitate cu litera (e) din prezentul alineat pentru stabilirea încălcării securității datelor cu caracter personal și stabilirii întârzierilor nejustificate menționate la articolul 33 alineatele (1) și (2), precum și pentru circumstanțele speciale în care un operator sau o persoană împuternicită de către operator are obligația de a notifica încălcarea securității datelor cu caracter personal;
- (h) să emită orientări, recomandări și bune practici în conformitate cu litera (e) din prezentul alineat în ceea ce privește circumstanțele în care o încălcare a securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, menționate la articolul 34 alineatul (1);
- (i) să emită orientări, recomandări și bune practici în conformitate cu litera (e) din prezentul alineat în scopul detalierii criteriilor și cerințelor aplicabile transferurilor de date cu caracter personal bazate pe regulile corporatiste obligatorii care trebuie respectate de operatori și cele care trebuie respectate de persoanele împuternicite de operatori, precum și cu privire la cerințe suplimentare necesare pentru a asigura protecția datelor cu caracter personal ale persoanelor vizate menționate la articolul 47;
- (j) să emită orientări, recomandări și bune practici în conformitate cu litera (e) din prezentul alineat în vederea detalierii criteriilor și cerințelor pentru transferurile de date cu caracter personal menționate la articolul 49 alineatul (1);
- (k) să elaboreze orientări destinate autorităților de supraveghere, referitoare la aplicarea măsurilor menționate la articolul 58 alineatele (1), (2) și (3) și să stabilească amenzile administrative în conformitate cu articolul 83;
- (l) să revizuiască aplicarea practică a orientărilor, recomandărilor și bunelor practici menționate la literele (e) și (f);
- (m) să emită orientări, recomandări și bune practici în conformitate cu litera (e) din prezentul alineat în vederea stabilirii procedurilor comune de raportare de către persoanele fizice a încălcărilor prezentului regulament în conformitate cu articolul 54 alineatul (2);
- (n) să încurajeze elaborarea de coduri de conduită și stabilirea unor mecanisme de certificare, precum și a unor sigilii și mărci în domeniul protecției datelor, în conformitate cu articolele 40 și 42;
- (o) să efectueze acreditarea organismelor de certificare și revizuirea periodică a acreditării în conformitate cu articolul 43 și să țină un registru public al organismelor acreditate, în conformitate cu articolul 43 alineatul (6), și al operatorilor acreditați sau al persoanelor împuternicite de operator acreditate, stabiliți (stabilite) în țări terțe, în conformitate cu articolul 42 alineatul (7);
- (p) să precizeze cerințele menționate la articolul 43 alineatul (3), în vederea acreditării organismelor de certificare prevăzute la articolul 42;
- (q) să prezinte Comisiei un avis privind cerințele de certificare menționate la articolul 43 alineatul (8);
- (r) să prezinte Comisiei un avis privind pictogramele menționate la articolul 12 alineatul (7);
- (s) să prezinte Comisiei un avis pentru evaluarea caracterului adecvat al nivelului de protecție într-o țară terță sau o organizație internațională, inclusiv pentru a determina dacă o țară terță, un teritoriu, sau unul sau mai multe sectoare specificate din acea țară terță, sau o organizație internațională nu mai asigură un nivel de protecție adecvat. În acest scop, Comisia pune la dispoziția comitetului toată documentația necesară, inclusiv corespondența purtată cu autoritățile publice ale țării terțe, în ceea ce privește acea țară terță, acel teritoriu sau acel sector, sau cu organizația internațională;

- (t) să emită avize privind proiectele de decizii ale autorităților de supraveghere în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 64 alineatul (1) privind chestiunile prezentate în conformitate cu articolul 64 alineatul (2) și să emită decizii obligatorii în temeiul articolului 65, inclusiv în cazurile menționate la articolul 66;
 - (u) să promoveze cooperarea și schimbul eficient bilateral și multilateral de informații și bune practici între autoritățile de supraveghere;
 - (v) să promoveze programe comune de formare și să faciliteze schimburile de personal între autoritățile de supraveghere, precum și, după caz, cu autoritățile de supraveghere ale țărilor terțe sau organizațiilor internaționale;
 - (w) să promoveze schimbul de cunoștințe și de documente privind legislația și practicile în materie de protecție a datelor cu autoritățile de supraveghere a protecției datelor la nivel mondial;
 - (x) să emită avize privind codurile de conduită elaborate la nivelul Uniunii în temeiul articolului 40 alineatul (9); și
 - (y) să țină un registru electronic accesibil publicului cu deciziile luate de autoritățile de supraveghere și de instanțe cu privire la chestiuni tratate în cadrul mecanismului pentru asigurarea coerenței.
- (2) În cazul în care Comisia consultă comitetul, aceasta poate indica un termen limită, ținând seama de caracterul urgent al chestiunii.
- (3) Comitetul își transmite avizele, orientările, recomandările și bunele practici Comisiei și comitetului menționat la articolul 93 și le face publice.
- (4) Dacă este cazul, comitetul consultă părțile interesate și le oferă posibilitatea de a face observații într-un termen rezonabil. Fără a aduce atingere dispozițiilor articolului 76, comitetul publică rezultatele procedurii de consultare.

Articolul 71

Rapoarte

- (1) Comitetul întocmește un raport anual privind protecția persoanelor fizice cu privire la prelucrare în Uniune și, dacă este relevant, în țări terțe și organizații internaționale. Raportul este pus la dispoziția publicului și transmis Parlamentului European, Consiliului și Comisiei.
- (2) Raportul anual include o revizuire a aplicării practice a orientărilor, recomandărilor și bunelor practici menționate la articolul 70 alineatul (1) litera (l), precum și a deciziilor obligatorii menționate la articolul 65.

Articolul 72

Procedura

- (1) Comitetul adoptă decizii prin majoritate simplă a membrilor săi, cu excepția cazului când se prevede altfel în prezentul regulament.
- (2) Comitetul își adoptă propriul regulament de procedură cu o majoritate de două treimi a membrilor săi și își organizează propriile mecanisme de funcționare.

Articolul 73

Președintele

- (1) Comitetul alege un președinte și doi vicepreședinți din rândul membrilor săi, cu majoritate simplă.
- (2) Mandatul președintelui și al vicepreședinților este de cinci ani și poate fi reînnoit o singură dată.

*Articolul 74***Sarcinile președintelui**

- (1) Președintele are următoarele sarcini:
 - (a) să convoace reuniunile comitetului și să stabilească ordinea de zi;
 - (b) să notifice deciziile adoptate de comitet, în conformitate cu articolul 65, autorității de supraveghere principale și autorităților de supraveghere vizate;
 - (c) să asigure îndeplinirea la timp a sarcinilor comitetului, în special în ceea ce privește mecanismul pentru asigurarea coerenței menționat la articolul 63.
- (2) Comitetul stabilește în regulamentul său de procedură repartizarea sarcinilor între președinte și vicepreședinți.

*Articolul 75***Secretariatul**

- (1) Comitetul dispune de un secretariat, care este asigurat de Autoritatea Europeană pentru Protecția Datelor.
- (2) Secretariatul își îndeplinește sarcinile exclusiv pe baza instrucțiunilor președintelui comitetului.
- (3) Personalul Autorității Europene pentru Protecția Datelor implicat în îndeplinirea sarcinilor conferite comitetului în temeiul prezentului regulament face obiectul unor linii de raportare separate în raport cu personalul implicat în îndeplinirea sarcinilor conferite Autorității Europene pentru Protecția Datelor.
- (4) Dacă este oportun, comitetul și Autoritatea Europeană pentru Protecția Datelor elaborează și publică un memorandum de înțelegere pentru punerea în aplicare a prezentului articol, care să stabilească condițiile cooperării și să se aplice personalului Autorității Europene pentru Protecția Datelor implicat în îndeplinirea sarcinilor conferite comitetului în temeiul prezentului regulament.
- (5) Secretariatul oferă sprijin analitic, administrativ și logistic comitetului.
- (6) Secretariatul este responsabil în special de următoarele:
 - (a) gestionarea curentă a activității comitetului;
 - (b) comunicarea dintre membrii comitetului, președintele acestuia și Comisie;
 - (c) comunicarea cu alte instituții și cu publicul;
 - (d) utilizarea mijloacelor electronice pentru comunicarea internă și externă;
 - (e) traducerea informațiilor relevante;
 - (f) pregătirea și monitorizarea acțiunilor ulterioare reuniunilor comitetului;
 - (g) pregătirea, redactarea și publicarea avizelor, deciziilor privind soluționarea litigiilor dintre autoritățile de supraveghere și a altor texte adoptate de comitet.

*Articolul 76***Confidențialitate**

- (1) Discuțiile din cadrul comitetului sunt confidențiale în cazul în care comitetul consideră că acest lucru este necesar în conformitate cu regulamentul său de procedură.

(2) Accesul la documentele prezentate membrilor comitetului, experților și reprezentanților părților terțe este reglementat prin Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului ⁽¹⁾.

CAPITOLUL VIII

Căi de atac, răspundere și sancțiuni

Articolul 77

Dreptul de a depune o plângere la o autoritate de supraveghere

(1) Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prezentul regulament.

(2) Autoritatea de supraveghere la care s-a depus plângerea informează reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul articolului 78.

Articolul 78

Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere

(1) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană fizică sau juridică are dreptul de a exercita o cale de atac judiciară eficientă împotriva unei decizii obligatorii din punct de vedere juridic a unei autorități de supraveghere care o vizează.

(2) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care autoritatea de supraveghere care este competentă în temeiul articolelor 55 și 56 nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse în temeiul articolului 77.

(3) Acțiunile introduse împotriva unei autorități de supraveghere sunt aduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere.

(4) În cazul în care acțiunile sunt introduse împotriva unei decizii a unei autorități de supraveghere care a fost precedată de un aviz sau o decizie a comitetului în cadrul mecanismului pentru asigurarea coerenței, autoritatea de supraveghere transmite curții avizul respectiv sau decizia respectivă.

Articolul 79

Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau unei persoane împuternicite de operator

(1) Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere în temeiul articolului 77, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal fără a se respecta prezentul regulament.

(2) Acțiunile introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în fața instanțelor din statul membru unde operatorul sau persoana împuternicită de operator își are un sediu. Alternativ, o astfel de acțiune poate fi prezentată în fața instanțelor din statul membru în care persoana vizată își are reședința obișnuită, cu excepția cazului în care operatorul sau persoana împuternicită de operator este o autoritate publică a unui stat membru ce acționează în exercitarea competențelor sale publice.

⁽¹⁾ Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO L 145, 31.5.2001, p. 43).

*Articolul 80***Reprezentarea persoanelor vizate**

- (1) Persoana vizată are dreptul de a mandata un organism, o organizație sau o asociație fără scop lucrativ, care au fost constituite în mod corespunzător în conformitate cu dreptul intern, ale căror obiective statutare sunt de interes public, care sunt active în domeniul protecției drepturilor și libertăților persoanelor vizate în ceea ce privește protecția datelor lor cu caracter personal, să depună plângerea în numele său, să exercite în numele său drepturile menționate la articolele 77, 78 și 79, precum și să exercite dreptul de a primi despăgubiri menționat la articolul 82 în numele persoanei vizate, dacă acest lucru este prevăzut în dreptul intern.
- (2) Statele membre pot prevedea că orice organism, organizație sau asociație menționată la alineatul (1) din prezentul articol, independent de mandatul unei persoane vizate, are dreptul de a depune în statul membru respectiv o plângere la autoritatea de supraveghere care este competentă în temeiul articolului 77 și de a exercita drepturile menționate la articolele 78 și 79, în cazul în care consideră că drepturile unei persoane vizate în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării.

*Articolul 81***Suspendarea procedurilor**

- (1) În cazul în care o instanță competentă a unui stat membru are informații că pe rolul unei instanțe dintr-un alt stat membru se află o acțiune având același obiect în ceea ce privește activitățile de prelucrare ale aceluiași operator sau ale aceleași persoane împuternicite de operator, instanța respectivă contactează instanța din celălalt stat membru pentru a confirma existența unor astfel de acțiuni.
- (2) Atunci când pe rolul unei instanțe dintr-un alt stat membru se află o acțiune având același obiect în ceea ce privește activitățile de prelucrare ale aceluiași operator sau ale aceleași persoane împuternicite de operator, orice altă instanță competentă decât instanța sesizată inițial poate suspenda acțiunea aflată la ea pe rol.
- (3) În cazul în care o astfel de acțiune se judecă în primă instanță, orice instanță sesizată ulterior poate, de asemenea, la cererea uneia dintre părți, să-și decline competența, cu condiția ca respectiva acțiune să fie de competența primei instanțe sesizate și ca dreptul aplicabil acestuia să permită conexarea acțiunilor.

*Articolul 82***Dreptul la despăgubiri și răspunderea**

- (1) Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a prezentului regulament are dreptul să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.
- (2) Orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă prezentul regulament. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligațiile din prezentul regulament care revin în mod specific persoanelor împuternicite de operator sau a acționat în afara sau în contradicție cu instrucțiunile legale ale operatorului.
- (3) Operatorul sau persoana împuternicită de operator este exonerat(ă) de răspundere în temeiul alineatului (2) dacă dovedește că nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul.
- (4) În cazul în care mai mulți operatori sau mai multe persoane împuternicite de operator, sau un operator și o persoană împuternicită de operator sunt implicați (implicate) în aceeași operațiune de prelucrare și răspund, în temeiul alineatelor (2) și (3), pentru orice prejudiciu cauzat de prelucrare, fiecare operator sau persoană împuternicită de operator este răspunzător (răspunzătoare) pentru întregul prejudiciu pentru a asigura despăgubirea efectivă a persoanei vizate.
- (5) În cazul în care un operator sau o persoană împuternicită de operator a plătit, în conformitate cu alineatul (4), în totalitate despăgubirile pentru prejudiciul ocazionat, respectivul operator sau respectiva persoană împuternicită de operator are dreptul să solicite de la ceilalți operatori sau celelalte persoane împuternicite de operator implicate în aceeași operațiune de prelucrare recuperarea acelei părți din despăgubiri care corespunde părții lor de răspundere pentru prejudiciu, în conformitate cu condițiile stabilite la alineatul (2).

(6) Acțiunile în exercitarea dreptului de recuperare a despăgubirilor plătite se introduc la instanțele competente în temeiul dreptului statului membru menționat la articolul 79 alineatul (2).

Articolul 83

Condiții generale pentru impunerea amenzilor administrative

(1) Fiecare autoritate de supraveghere asigură faptul că impunerea unor amenzi administrative în conformitate cu prezentul articol pentru încălcările prezentului regulament menționate la alineatele (4), (5) și, (6) este, în fiecare caz, eficace, proporțională și disuasivă.

(2) În funcție de circumstanțele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menționate la articolul 58 alineatul (2) literele (a)-(h) și (j). Atunci când se ia decizia dacă să se impună o amendă administrativă și decizia cu privire la valoarea amenzii administrative în fiecare caz în parte, se acordă atenția cuvenită următoarelor aspecte:

- (a) natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea;
- (b) dacă încălcarea a fost comisă intenționat sau din neglijență;
- (c) orice acțiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;
- (d) gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ținându-se seama de măsurile tehnice și organizatorice implementate de aceștia în temeiul articolelor 25 și 32;
- (e) eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;
- (f) gradul de cooperare cu autoritatea de supraveghere pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării;
- (g) categoriile de date cu caracter personal afectate de încălcare;
- (h) modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;
- (i) în cazul în care măsurile menționate la articolul 58 alineatul (2) au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la același obiect, respectarea respectivelor măsuri;
- (j) aderarea la coduri de conduită aprobate, în conformitate cu articolul 40, sau la mecanisme de certificare aprobate, în conformitate cu articolul 42; și
- (k) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

(3) În cazul în care un operator sau o persoană împuternicită de operator încalcă în mod intenționat sau din neglijență, pentru aceeași operațiune de prelucrare sau pentru operațiuni de prelucrare conexe, mai multe dispoziții din prezentul regulament, cuantumul total al amenzii administrative nu poate depăși suma prevăzută pentru cea mai gravă încălcare.

(4) Pentru încălcările dispozițiilor următoare, în conformitate cu alineatul (2), se aplică amenzi administrative de până la 10 000 000 EUR sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare:

- (a) obligațiile operatorului și ale persoanei împuternicite de operator în conformitate cu articolele 8, 11, 25-39, 42 și 43;
- (b) obligațiile organismului de certificare în conformitate cu articolele 42 și 43;
- (c) obligațiile organismului de monitorizare în conformitate cu articolul 41 alineatul (4).

(5) Pentru încălcările dispozițiilor următoare, în conformitate cu alineatul (2), se aplică amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare:

- (a) principiile de bază pentru prelucrare, inclusiv condițiile privind consimțământul, în conformitate cu articolele 5, 6, 7 și 9;
- (b) drepturile persoanelor vizate în conformitate cu articolele 12-22;
- (c) transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu articolele 44-49;
- (d) orice obligații în temeiul legislației naționale adoptate în temeiul capitolului IX;
- (e) nerespectarea unui ordin sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării fluxurilor de date, emisă de către autoritatea de supraveghere în temeiul articolului 58 alineatul (2), sau neacordarea accesului, încălcând articolul 58 alineatul (1).

(6) Pentru încălcarea unui ordin emis de autoritatea de supraveghere în conformitate cu articolul 58 alineatul (2) se aplică, în conformitate cu alineatul (2) din prezentul articol, amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare.

(7) Fără a aduce atingere competențelor corective ale autorităților de supraveghere menționate la articolul 58 alineatul (2), fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi impuse amenzi administrative autorităților publice și organismelor publice stabilite în statul membru respectiv.

(8) Exercițarea de către autoritatea de supraveghere a competențelor sale în temeiul prezentului articol are loc cu condiția existenței unor garanții procedurale adecvate în conformitate cu dreptul Uniunii și cu dreptul intern, inclusiv căi de atac judiciare eficiente și dreptul la un proces echitabil.

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

Articolul 84

Sancțiuni

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

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

CAPITOLUL IX

Dispoziții referitoare la situații specifice de prelucrare

Articolul 85

Prelucrarea și libertatea de exprimare și de informare

(1) Prin intermediul dreptului intern, statele membre asigură un echilibru între dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament și dreptul la libertatea de exprimare și de informare, inclusiv prelucrarea în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare.

(2) Pentru prelucrarea efectuată în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare, statele membre prevăd exonerări sau derogări de la dispozițiile capitolului II (principii), ale capitolului III (drepturile persoanei vizate), ale capitolului IV (operatorul și persoana împuternicită de operator), ale capitolului V (transferul datelor cu caracter personal către țări terțe sau organizații internaționale), ale capitolului VI (autorități de supraveghere independente), ale capitolului VII (cooperare și coerență) și ale capitolului IX (situații specifice de prelucrare a datelor) în cazul în care acestea sunt necesare pentru a asigura un echilibru între dreptul la protecția datelor cu caracter personal și libertatea de exprimare și de informare.

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

Articolul 86

Prelucrarea și accesul public la documente oficiale

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

Articolul 87

Prelucrarea unui număr de identificare național

Statele membre pot detalia în continuare condițiile specifice de prelucrare a unui număr de identificare național sau a oricărui alt identificator cu aplicabilitate generală. În acest caz, numărul de identificare național sau orice alt identificator cu aplicabilitate generală este folosit numai în temeiul unor garanții corespunzătoare pentru drepturile și libertățile persoanei vizate în temeiul prezentului regulament.

Articolul 88

Prelucrarea în contextul ocupării unui loc de muncă

(1) Prin lege sau prin acorduri colective, statele membre pot prevedea norme mai detaliate pentru a asigura protecția drepturilor și a libertăților cu privire la prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii, al egalității și diversității la locul de muncă, al asigurării sănătății și securității la locul de muncă, al protejării proprietății angajatorului sau a clientului, precum și în scopul exercitării și beneficierii, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și pentru încetarea raporturilor de muncă.

(2) Aceste norme includ măsuri corespunzătoare și specifice pentru garantarea demnității umane, a intereselor legitime și a drepturilor fundamentale ale persoanelor vizate, în special în ceea ce privește transparența prelucrării, transferul de date cu caracter personal în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună și sistemele de monitorizare la locul de muncă.

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

Articolul 89

Garanții și derogări privind prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice

(1) Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice are loc cu condiția existenței unor garanții corespunzătoare, în conformitate cu prezentul regulament, pentru drepturile și libertățile persoanelor vizate. Respectivul garanții asigură faptul că au fost instituite măsuri tehnice și

organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor. Respectivile măsuri pot include pseudonimizarea, cu condiția ca respectivile scopuri să fie îndeplinite în acest mod. Atunci când respectivile scopuri pot fi îndeplinite printr-o prelucrare ulterioară care nu permite sau nu mai permite identificarea persoanelor vizate, scopurile respective sunt îndeplinite în acest mod.

(2) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică ori în scopuri statistice, dreptul Uniunii sau dreptul intern poate să prevadă derogări de la drepturile menționate la articolele 15, 16, 18 și 21, sub rezerva condițiilor și a garanțiilor prevăzute la alineatul (1) din prezentul articol, în măsura în care drepturile respective sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri.

(3) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare în interes public, dreptul Uniunii sau dreptul intern poate să prevadă derogări de la drepturile menționate la articolele 15, 16, 18, 19, 20 și 21, sub rezerva condițiilor și a garanțiilor prevăzute la alineatul (1) din prezentul articol, în măsura în care drepturile respective sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri.

(4) În cazul în care prelucrarea menționată la alineatele (2) și (3) servește în același timp și altui scop, derogările se aplică numai prelucrării în scopurile menționate la alineatele respective.

Articolul 90

Obligații privind păstrarea confidențialității

(1) Statele membre pot adopta norme specifice pentru a stabili competențele autorităților de supraveghere, prevăzute la articolul 58 alineatul (1) literele (e) și (f), în legătură cu operatori sau cu persoane împuternicite de operatori care, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organismele naționale competente, au obligația de a păstra secretul profesional sau alte obligații echivalente de confidențialitate, în cazul în care acest lucru este necesar și proporțional pentru a stabili un echilibru între dreptul la protecția datelor cu caracter personal și obligația păstrării confidențialității. Respectivile norme se aplică doar în ceea ce privește datele cu caracter personal pe care operatorul sau persoana împuternicită de operator le-a primit în urma sau în contextul unei activități care intră sub incidența acestei obligații de păstrare a confidențialității.

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

Articolul 91

Normele existente în domeniul protecției datelor pentru biserici și asociații religioase

(1) În cazul în care, într-un stat membru, bisericile și asociațiile sau comunitățile religioase aplică, la data intrării în vigoare a prezentului regulament, un set cuprinzător de norme de protecție a persoanelor fizice cu privire la prelucrare, aceste norme pot continua să se aplice, cu condiția să fie aliniate la prezentul regulament.

(2) Bisericile și asociațiile religioase care aplică un set cuprinzător de norme în conformitate cu alineatul (1) din prezentul articol sunt supuse supravegherii unei autorități de supraveghere independente care poate fi specifică, cu condiția să îndeplinească condițiile stabilite în capitolul VI din prezentul regulament.

CAPITOLUL X

Acte delegate și acte de punere în aplicare

Articolul 92

Exercitarea delegării

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

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

(3) Delegarea de competențe menționată la articolul 12 alineatul (8) și la articolul 43 alineatul (8) poate fi revocată în orice moment de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificată în decizia respectivă. Decizia produce efecte din ziua următoare datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere validității actelor delegate care sunt deja în vigoare.

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

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

Articolul 93

Procedura comitetului

(1) Comisia este asistată de un comitet. Comitetul respectiv este un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

(3) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 8 din Regulamentul (UE) nr. 182/2011 coroborat cu articolul 5 din respectivul regulament.

CAPITOLUL XI

Dispoziții finale

Articolul 94

Abrogarea Directivei 95/46/CE

(1) Decizia 95/46/CE se abrogă cu efect de la 25 mai 2018.

(2) Trimiterile la directiva abrogată se interpretează ca trimiteri la prezentul regulament. Trimiterile la Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal instituit prin articolul 29 din Directiva 95/46/CE se interpretează ca trimiteri la Comitetul european pentru protecția datelor instituit prin prezentul regulament.

Articolul 95

Relația cu Directiva 2002/58/CE

Prezentul regulament nu impune obligații suplimentare pentru persoanele fizice sau juridice în ceea ce privește prelucrarea în legătură cu furnizarea de servicii de comunicații electronice destinate publicului în rețelele de comunicații publice din Uniune, cu privire la aspectele pentru care acestora le revin obligații specifice cu același obiectiv prevăzut în Directiva 2002/58/CE.

*Articolul 96***Relația cu acordurile încheiate anterior**

Acordurile internaționale care implică transferul de date cu caracter personal către țări terțe sau organizații internaționale, care au fost încheiate de statele membre înainte de 24 mai 2016 și care sunt în conformitate cu dreptul Uniunii aplicabil înainte de data respectivă, rămân în vigoare până când vor fi modificate, înlocuite sau revocate.

*Articolul 97***Rapoartele Comisiei**

(1) Până la 25 mai 2020 și, ulterior, la fiecare patru ani, Comisia transmite Parlamentului European și Consiliului un raport privind evaluarea și revizuirea prezentului regulament. Rapoartele sunt făcute publice.

(2) În contextul evaluărilor și revizuirilor menționate la alineatul (1), Comisia examinează în special aplicarea și funcționarea:

(a) capitolului V privind transferul datelor cu caracter personal către țări terțe sau organizații internaționale, având în vedere în special deciziile adoptate în temeiul articolului 45 alineatul (3) din prezentul regulament și deciziile adoptate în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE;

(b) capitolul VII privind cooperarea și coerența.

(3) În scopul alineatului (1), Comisia poate solicita informații de la statele membre și de la autoritățile de supraveghere.

(4) La efectuarea evaluărilor și a revizuirilor menționate la alineatele (1) și (2), Comisia ia în considerare pozițiile și constatările Parlamentului European, ale Consiliului, precum și ale altor organisme sau surse relevante.

(5) Comisia transmite, dacă este necesar, propuneri corespunzătoare de modificare a prezentului regulament, în special ținând seama de evoluțiile din domeniul tehnologiei informației și având în vedere progresele societății informaționale.

*Articolul 98***Revizuirea altor acte juridice ale Uniunii în materie de protecție a datelor**

Dacă este cazul, Comisia prezintă propuneri legislative în vederea modificării altor acte juridice ale Uniunii privind protecția datelor cu caracter personal, în vederea asigurării unei protecții uniforme și consecvente a persoanelor fizice în ceea ce privește prelucrarea. Acest lucru privește în special normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea de către instituțiile, organismele, oficiile și agențiile Uniunii, precum și normele referitoare la libera circulație a acestor date.

*Articolul 99***Intrare în vigoare și aplicare**

(1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

(2) Prezentul regulament se aplică de la 25 mai 2018.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 27 aprilie 2016.

Pentru Parlamentul European

Președintele

M. SCHULZ

Pentru Consiliu

Președintele

J.A. HENNIS-PLASSCHAERT

DIRECTIVE

DIRECTIVA (UE) 2016/680 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

din 27 aprilie 2016

privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16 alineatul (2),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Regiunilor ⁽¹⁾,

hotărând în conformitate cu procedura legislativă ordinară ⁽²⁾,

întrucât:

- (1) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal reprezintă un drept fundamental. Articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene (Carta) și articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc.
- (2) Principiile și normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal ar trebui, indiferent de cetățenia sau de locul de reședință al persoanelor fizice, să respecte drepturile și libertățile fundamentale ale acestora, în special dreptul la protecția datelor cu caracter personal. Prezenta directivă urmărește să contribuie la realizarea unui spațiu de libertate, securitate și justiție.
- (3) Evoluțiile tehnologice rapide și globalizarea au generat noi provocări pentru protecția datelor cu caracter personal. Amploarea colectării și a schimbului de date cu caracter personal a crescut în mod semnificativ. Tehnologia permite prelucrarea datelor cu caracter personal la un nivel fără precedent în cadrul activităților precum prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor ori executarea pedepselor.
- (4) Libera circulație a datelor cu caracter personal între autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora în cadrul Uniunii, și transferul de astfel de date cu caracter personal către țări terțe și organizații internaționale, ar trebui facilitate asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal. Aceste evoluții impun realizarea unui cadru solid și mai coerent în materie de protecție a datelor cu caracter personal în Uniune, însoțit de o aplicare riguroasă a normelor.
- (5) Directiva 95/46/CE a Parlamentului European și a Consiliului ⁽³⁾ se aplică oricărei prelucrări de date cu caracter personal în statele membre, atât în sectorul public, cât și în cel privat. Cu toate acestea, directiva menționată nu se aplică prelucrării datelor cu caracter personal în cursul exercitării unei activități care nu se înscrie în domeniul de aplicare a dreptului comunitar, cum sunt activitățile în domeniul cooperării judiciare în materie penală și al cooperării polițienești.

⁽¹⁾ JO C 391, 18.12.2012, p. 127.

⁽²⁾ Poziția Parlamentului European din 12 martie 2014 (nepublicată încă în Jurnalul Oficial) și Poziția în primă lectură a Consiliului din 8 aprilie 2016 (nepublicată încă în Jurnalul Oficial). Poziția Parlamentului European din 14 aprilie 2016.

⁽³⁾ Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO L 281, 23.11.1995, p. 31).

- (6) Decizia-cadru 2008/977/JAI a Consiliului ⁽¹⁾ se aplică în domeniul cooperării judiciare în materie penală și al cooperării polițienești. Domeniul de aplicare a deciziei-cadru menționate este limitat la prelucrarea datelor cu caracter personal transmise sau puse la dispoziție între statele membre.
- (7) Asigurarea unui nivel omogen și ridicat de protecție a datelor cu caracter personal ale persoanelor fizice și facilitarea schimbului de date cu caracter personal între autoritățile competente ale statelor membre sunt esențiale pentru a se garanta eficacitatea cooperării judiciare în materie penală și a cooperării polițienești. În acest scop, nivelul de protecție a drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora, ar trebui să fie echivalent în toate statele membre. Protecția efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea drepturilor persoanelor vizate și a obligațiilor celor care prelucrează date cu caracter personal, ci și competențe echivalente pentru monitorizarea și asigurarea conformității cu normele în materie de protecție a datelor cu caracter personal în statele membre.
- (8) Articolul 16 alineatul (2) din TFUE mandatează Parlamentul European și Consiliul să stabilească normele privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal, precum și normele privind libera circulație a acestor date.
- (9) Pe această bază, Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ⁽²⁾ stabilește normele generale pentru protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și garantarea liberei circulații a acestor date în cadrul Uniunii.
- (10) În Declarația nr. 21 cu privire la protecția datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești, anexată la actul final al Conferinței interguvernamentale care a adoptat Tratatul de la Lisabona, conferința a recunoscut că s-ar putea dovedi necesare norme specifice privind protecția datelor cu caracter personal și libera circulație a datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești în temeiul articolului 16 din TFUE, având în vedere natura specifică a acestor domenii.
- (11) Prin urmare, domeniile menționate ar trebui să fie reglementate printr-o directivă care să stabilească norme specifice privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora, cu respectarea naturii speciale a activităților în cauză. Pot reprezenta astfel de autorități competente nu numai autoritățile publice, precum autoritățile judiciare, poliția sau alte autorități de aplicare a legii, ci și orice alt organism sau altă entitate însărcinată prin dreptul intern să exercite autoritatea publică și competențe publice în sensul prezentei directive. În cazul în care un astfel de organism sau de entitate prelucrează date cu caracter personal în alte scopuri decât cele urmărite de prezenta directivă, se aplică Regulamentul (UE) 2016/679. Regulamentul (UE) 2016/679 se aplică, prin urmare, în cazurile în care un organism sau o entitate colectează date cu caracter personal în alte scopuri și ulterior prelucrează datele cu caracter personal respective în vederea respectării unei obligații legale care îi revine. De exemplu, în scopul depistării, investigării sau urmăririi infracțiunilor, instituțiile financiare păstrează anumite date cu caracter personal care sunt prelucrate de către acestea și furnizează datele cu caracter personal respective numai autorităților naționale competente în cazuri specifice și în conformitate cu dreptul intern. Unui organism sau entități care prelucrează date cu caracter personal în numele acestor autorități, în cadrul domeniului de aplicare al prezentei directive, ar trebui să îi revină obligații în temeiul unui contract sau al altui act juridic și al dispozițiilor aplicabile persoanelor împuternicite de către operatori în conformitate cu prezenta directivă, fără ca prin aceasta să se aducă atingere aplicării Regulamentului (UE) 2016/679 în ceea ce privește prelucrarea datelor cu caracter personal de către persoana împuternicită de către operator, atunci când această prelucrare nu intră sub incidența prezentei directive.
- (12) Activitățile desfășurate de poliție sau de alte autorități de aplicare a legii, inclusiv activitățile polițienești desfășurate fără a cunoaște dinainte dacă un incident constituie o infracțiune, se concentrează în principal asupra prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor. Activitățile respective pot include, de asemenea, exercitarea autorității prin aplicarea unor măsuri coercitive, precum activitățile polițienești desfășurate cu ocazia unor manifestații, evenimente sportive majore și revolte. De asemenea, activitățile menționate includ

⁽¹⁾ Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală (JO L 350, 30.12.2008, p. 60).

⁽²⁾ Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (a se vedea pagina 1 din prezentul Jurnal Oficial).

menținerea legii și ordinii ca atribuții ale poliției sau ale altor autorități de aplicare a legii atunci când aceasta se impune pentru a se asigura protecția împotriva amenințărilor la adresa securității publice și la adresa intereselor fundamentale ale societății protejate prin lege și pentru prevenirea acestor amenințări, care pot conduce la o infracțiune. Statele membre pot încredința autorităților competente alte sarcini care nu sunt neapărat îndeplinite în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora, astfel încât prelucrarea datelor cu caracter personal în aceste alte scopuri, în măsura în care se circumscriu domeniului de aplicare al dreptului Uniunii, intră sub incidența Regulamentului (UE) 2016/679.

- (13) Noțiunea de infracțiune, în sensul prezentei directive, ar trebui să constituie o noțiune autonomă de drept al Uniunii astfel cum este interpretat de Curtea de Justiție a Uniunii Europene („Curtea de Justiție”).
- (14) Având în vedere că prezenta directivă nu ar trebui să se aplice prelucrării datelor cu caracter personal în cadrul unei activități care nu intră sub incidența dreptului Uniunii, activitățile privind securitatea națională, activitățile agențiilor sau ale unităților specializate pe probleme de securitate națională și prelucrarea datelor cu caracter personal de către statele membre atunci când acestea desfășoară activități circumscrise domeniului de aplicare al titlului V capitolul 2 din Tratatul privind Uniunea Europeană (TUE) nu ar trebui să fie considerate activități care se încadrează în domeniul de aplicare al prezentei directive.
- (15) În vederea asigurării aceluiași nivel de protecție pentru persoanele fizice prin drepturi garantate din punct de vedere juridic în întreaga Uniune și a preîntâmpinării discrepanțelor care împiedică schimbul de date cu caracter personal între autoritățile competente, prezenta directivă ar trebui să prevadă norme armonizate pentru protecția și libera circulație a datelor cu caracter personal prelucrate în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. Armonizarea drepturilor statelor membre nu ar trebui să aibă ca rezultat diminuarea nivelului de protecție a datelor cu caracter personal pe care îl oferă statele respective, ci ar trebui, dimpotrivă, să urmărească să asigure un înalt nivel de protecție în cadrul Uniunii. Statele membre nu ar trebui să fie împiedicate să prevadă garanții mai mari decât cele stabilite în prezenta directivă pentru protecția drepturilor și libertăților persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente.
- (16) Prezenta directivă nu aduce atingere principiului accesului publicului la documente oficiale. În temeiul Regulamentului (UE) 2016/679, datele cu caracter personal din documentele oficiale deținute de o autoritate publică sau de un organism public sau privat pentru îndeplinirea unei atribuții de interes public pot fi divulgate de autoritatea sau organismul respectiv în conformitate cu dreptul Uniunii sau cu dreptul intern sub incidența căruia intră autoritatea sau organismul, pentru a stabili un echilibru între accesul public la documente oficiale și dreptul la protecția datelor cu caracter personal.
- (17) Protecția conferită de prezenta directivă ar trebui să vizeze persoanele fizice, indiferent de cetățenia sau de locul de reședință al acestora, în ceea ce privește prelucrarea datelor cu caracter personal ale acestora.
- (18) Pentru a preîntâmpina un risc serios de eludare, protecția persoanelor fizice ar trebui să fie neutră din punct de vedere tehnologic și nu ar trebui să depindă de tehnicile utilizate. Protecția persoanelor fizice ar trebui să se aplice în ceea ce privește prelucrarea datelor cu caracter personal prin mijloace automate, precum și prelucrarea manuală, în cazul în care datele cu caracter personal sunt cuprinse sau destinate să fie cuprinse într-un sistem de evidență. Dosarele sau seturile de dosare, precum și copertele acestora, care nu sunt structurate în conformitate cu criteriile specifice, nu ar trebui să intre sub incidența prezentei directive.
- (19) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ⁽¹⁾ se aplică prelucrării datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii. Regulamentul (CE) nr. 45/2001 și alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal ar trebui adaptate la principiile și normele stabilite prin Regulamentul (UE) 2016/679.
- (20) Prezenta directivă nu împiedică statele membre să precizeze operațiunile și procedurile de prelucrare în normele naționale privind procedurile penale în ceea ce privește prelucrarea datelor cu caracter personal de către instanțe și alte autorități judiciare, în special în ceea ce privește datele cu caracter personal conținute într-o hotărâre judecătorească sau în înregistrările legate de proceduri penale.

⁽¹⁾ Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

- (21) Principiile protecției datelor ar trebui să se aplice oricărei informații referitoare la o persoană fizică identificată sau identificabilă. Pentru a se determina dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană în scopul identificării, în mod direct sau indirect, a persoanei fizice respective. Pentru a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace în scopul identificării persoanei fizice, ar trebui luați în considerare toți factorii obiectivi, precum costurile și intervalul de timp necesare pentru identificare, ținându-se seama de tehnologia disponibilă la momentul prelucrării și de dezvoltarea tehnologică. Principiile protecției datelor ar trebui, prin urmare, să nu se aplice informațiilor anonime, adică informațiilor care nu sunt legate de o persoană fizică identificată sau identificabilă, sau datelor cu caracter personal care sunt anonimizate astfel încât persoana vizată nu mai este identificabilă.
- (22) Autoritățile publice cărora le sunt divulgate date cu caracter personal în conformitate cu o obligație legală pentru exercitarea misiunii lor oficiale, cum ar fi autoritățile fiscale și vamale, unitățile de investigare financiară, autoritățile administrative independente sau autoritățile piețelor financiare, responsabile de reglementarea și de supravegherea piețelor valorilor mobiliare, nu ar trebui să fie considerate drept destinatari în cazul în care primesc date cu caracter personal care sunt necesare pentru desfășurarea unei anumite anchete de interes general, în conformitate cu dreptul Uniunii sau cu dreptul intern. Cererile de divulgare transmise de autoritățile publice ar trebui să se facă întotdeauna în scris, să fie motivate și ocazionale și nu ar trebui să se refere la totalitatea unui sistem de evidență sau să conducă la interconectarea sistemelor de evidență. Prelucrarea datelor cu caracter personal de către respectivele autorități publice ar trebui să respecte normele aplicabile privind protecția datelor, în conformitate cu scopurile prelucrării.
- (23) Datele genetice ar trebui definite drept date cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice despre fiziologia sau starea de sănătate a persoanei respective, și care rezultă în urma unei analize a unei mostre de material biologic al persoanei fizice în cauză, în special a analizei cromozomiale, a unei analize a acidului dezoxiribonucleic (ADN) sau a acidului ribonucleic (ARN) sau în urma analizei oricărui alt element care permite obținerea unor informații echivalente. Având în vedere complexitatea și sensibilitatea informațiilor genetice, există un risc ridicat de utilizare abuzivă și de reutilizare în diverse scopuri neautorizate de către operator. Orice discriminare bazată pe caracteristici genetice ar trebui să fie, în principiu, interzisă.
- (24) Datele cu caracter personal privind sănătatea ar trebui să includă toate datele având legătură cu starea de sănătate a persoanei vizate, care să dezvăluie informații despre starea de sănătate fizică sau mentală trecută, prezentă sau viitoare a persoanei vizate. Acestea includ informații privind persoana fizică colectate în cursul înscrierii acesteia la serviciile de asistență medicală sau în cadrul acordării serviciilor respective persoanei fizice în cauză, astfel cum sunt menționate în Directiva 2011/24/UE a Parlamentului European și a Consiliului (⁽¹⁾); un număr, un simbol sau un semn distinctiv atribuit unei persoane fizice pentru identificarea singulară a acesteia în scopuri medicale; informații rezultate din testarea sau examinarea unei părți a corpului sau a unei substanțe corporale, inclusiv din date genetice și eșantioane de material biologic; precum și orice informații privind, de exemplu, o boală, un handicap, un risc de îmbolnăvire, istoricul medical, tratamentul clinic sau starea fiziologică sau biomedicală a persoanei vizate, indiferent de sursa acestora, ca de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro.
- (25) Toate statele membre sunt afiliate la Organizația Internațională de Poliție Criminală (Interpol). Pentru a-și îndeplini misiunea, Interpol primește, stochează și difuzează date cu caracter personal pentru a ajuta autoritățile competente să prevină și să combată criminalitatea internațională. Prin urmare, este adecvat să se consolideze cooperarea dintre Uniune și Interpol prin promovarea unui schimb eficient de date cu caracter personal, asigurând, în același timp, respectarea drepturilor și libertăților fundamentale în ceea ce privește prelucrarea automată a datelor cu caracter personal. Atunci când se transferă date cu caracter personal din Uniune către Interpol și către țările care au membri delegați la Interpol, ar trebui să se aplice prezenta directivă, în special dispozițiile privind transferurile internaționale. Prezenta directivă nu ar trebui să aducă atingere normelor specifice stabilite în Poziția comună 2005/69/JAI a Consiliului (⁽²⁾) și în Decizia 2007/533/JAI a Consiliului (⁽³⁾).
- (26) Orice prelucrare a datelor cu caracter personal trebuie să fie legală, echitabilă și transparentă față de persoanele fizice în cauză, iar prelucrarea trebuie să fie făcută numai pentru scopuri specifice prevăzute de lege. Acest lucru nu împiedică, în sine, autoritățile de aplicare a legii să desfășoare activități precum investigațiile sub acoperire sau supravegherea video. Aceste activități pot fi întreprinse în scopul prevenirii, depistării, investigării sau urmăririi

(¹) Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere (JO L 88, 4.4.2011, p. 45).

(²) Poziția comună 2005/69/JAI a Consiliului din 24 ianuarie 2005 privind schimbul de anumite date cu Interpol (JO L 27, 29.1.2005, p. 61).

(³) Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II) (JO L 205, 7.8.2007, p. 63).

penale a infracțiunilor sau al executării sancțiunilor penale, inclusiv al protecției împotriva fraudei și al prevenirii amenințărilor la adresa securității publice, în măsura în care sunt prevăzute de lege și constituie o măsură necesară și proporțională într-o societate democratică, ținându-se seama în mod corespunzător de interesele legitime ale respectivei persoane fizice. Principiul prelucrării echitabile a datelor din domeniul protecției datelor cu caracter personal este o noțiune distinctă de dreptul la un proces echitabil, astfel cum este definit la articolul 47 din Cartă și la articolul 6 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale (CEDO). Persoanele fizice ar trebui să fie informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor acestora cu caracter personal și cu privire la modul în care să își exercite drepturile respective. În special, scopurile specifice în care datele cu caracter personal sunt prelucrate ar trebui să fie explicite și legitime și să fie determinate la momentul colectării datelor. Datele cu caracter personal ar trebui să fie adecvate și relevante pentru scopurile în care sunt prelucrate. În special, ar trebui să se asigure faptul că datele cu caracter personal colectate nu sunt excesive și că nu sunt stocate mai mult timp decât este necesar pentru îndeplinirea scopului în care sunt prelucrate. Datele cu caracter personal ar trebui prelucrate doar în cazul în care scopul prelucrării nu poate fi îndeplinit, în mod rezonabil, prin alte mijloace. În vederea asigurării faptului că datele nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ștergere sau revizuire periodică. Statele membre ar trebui să stabilească garanții adecvate pentru datele cu caracter personal care sunt stocate pe o perioadă mai lungă, în scopuri de arhivare în interes public sau în scopuri științifice, statistice sau istorice.

- (27) Pentru prevenirea, investigarea și urmărirea penală a infracțiunilor, autoritățile competente trebuie să prelucreze datele cu caracter personal colectate în contextul prevenirii, depistării, investigării sau urmării penale a anumitor infracțiuni dincolo de acest context pentru a înțelege mai bine activitățile infracționale și pentru a face legături între diferitele infracțiuni detectate.
- (28) În vederea menținerii securității în ceea ce privește prelucrarea și a prevenirii prelucrărilor care nu respectă prezenta directivă, datele cu caracter personal ar trebui prelucrate într-un mod care să asigure un nivel corespunzător de securitate și confidențialitate, inclusiv prin prevenirea accesului neautorizat la acestea sau a utilizării neautorizate a datelor și a echipamentului utilizat pentru prelucrare și luând în considerare stadiul actual al tehnologiei disponibile, costurile punerii acestora în aplicare în raport cu riscurile și natura datelor cu caracter personal a căror protecție trebuie asigurată.
- (29) Colectarea datelor cu caracter personal ar trebui să fie efectuată în scopuri determinate, explicite și legitime în cadrul domeniului de aplicare al prezentei directive, iar prelucrarea acestora nu ar trebui să se facă în scopuri care sunt incompatibile cu obiectivele prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau ale executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. În cazul în care datele cu caracter personal sunt prelucrate de către același sau de către un alt operator într-un scop care se încadrează în domeniul de aplicare al prezentei directive, dar este diferit de scopul în care au fost colectate, o astfel de prelucrare ar trebui să fie permisă cu condiția ca o astfel de prelucrare să fie autorizată în conformitate cu dispozițiile legale aplicabile și este necesară și proporțională în raport cu acest alt scop.
- (30) Principiul exactității datelor ar trebui aplicat luând în considerare natura și scopul prelucrării în cauză. În special în cadrul procedurilor judiciare, declarațiile care conțin date cu caracter personal se bazează pe o percepție subiectivă a persoanelor fizice și nu sunt întotdeauna verificabile. În consecință, acest principiu nu ar trebui să se aplice exactității unei declarații, ci doar faptului că o anumită declarație a fost făcută.
- (31) Prelucrarea datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești presupune prelucrarea datelor cu caracter personal referitoare la diferite categorii de persoane. Prin urmare, ar trebui să se facă o distincție clară, după caz și în măsura posibilului, între datele cu caracter personal ale diferitelor categorii de persoane vizate, cum ar fi suspecții, persoanele condamnate pentru comiterea unei infracțiuni, victimele și alte părți, cum ar fi martorii, persoanele care dețin informații sau contacte relevante și complicii suspecților și ai infractorilor condamnați. Acest lucru nu ar trebui să împiedice aplicarea dreptului la prezumția de nevinovăție, astfel cum este garantat de Cartă și de CEDO, după cum a fost interpretat de jurisprudența Curții de Justiție și, respectiv, a Curții Europene a Drepturilor Omului.
- (32) Autoritățile competente ar trebui să se asigure că nu se transmit sau nu se pun la dispoziție date cu caracter personal care sunt inexacte, incomplete sau nu mai sunt actuale. Pentru a asigura protecția persoanelor fizice și exactitatea, caracterul integral sau gradul de actualitate și fiabilitatea datelor cu caracter personal transmise sau puse la dispoziție, autoritățile competente ar trebui, pe cât posibil, să adauge informațiile necesare în toate transmișerile de date cu caracter personal.
- (33) Atunci când prezenta directivă face trimitere la dreptul intern, la un temei juridic sau la o măsură legislativă, aceasta nu necesită neapărat un act legislativ adoptat de către un parlament, fără a aduce atingere cerințelor care

decurg din ordinea constituțională a statului membru în cauză. Cu toate acestea, dreptul intern, temeiul juridic sau măsura legislativă în cauză ar trebui să fie clare și precise, iar aplicarea să fie previzibilă destinatarilor, în conformitate cu jurisprudența Curții de Justiție și a Curții Europene a Drepturilor Omului. Dreptul intern care reglementează prelucrarea datelor cu caracter personal din domeniul de aplicare al prezentei directive ar trebui să precizeze cel puțin obiectivele, datele cu caracter personal care urmează a fi prelucrate, scopurile prelucrării și procedurile de păstrare a integrității și a confidențialității datelor cu caracter personal și procedurile de distrugere a acestora, oferind astfel garanții suficiente împotriva riscurilor de abuzuri și de arbitrar.

- (34) Prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora, ar trebui să acopere orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal sau seturilor de date cu caracter personal în aceste scopuri efectuată prin mijloace automate sau în alt mod, precum colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, alinierea sau combinarea, restricționarea prelucrării, ștergerea sau distrugerea. În special, normele din prezenta directivă ar trebui să se aplice transmiterii datelor cu caracter personal în sensul prezentei directive către un destinatar care nu face obiectul prezentei directive. Un astfel de destinatar ar trebui să includă o persoană fizică sau juridică, o autoritate publică, o agenție sau orice alt organ căruia îi sunt divulgate în mod legal datele cu caracter personal de către autoritățile competente. În cazul în care datele cu caracter personal au fost inițial colectate de către o autoritate competentă în unul dintre scopurile prezentei directive, Regulamentul (UE) 2016/679 ar trebui să se aplice prelucrării acestor date în alte scopuri decât cele ale prezentei directive atunci când o astfel de prelucrare este autorizată de dreptul Uniunii sau de dreptul intern. În special, normele din Regulamentul (UE) 2016/679 ar trebui să se aplice la transmiterea de date cu caracter personal în scopuri care nu intră sub incidența prezentei directive. Prelucrarea datelor cu caracter personal de către un destinatar care nu este sau nu acționează în calitate de autoritate competentă în sensul prezentei directive și căruia îi sunt divulgate în mod legal datele cu caracter personal de către o autoritate competentă, ar trebui să intre sub incidența Regulamentului (UE) 2016/679. La punerea în aplicare a prezentei directive, statele membre ar trebui, de asemenea, să poată aduce precizări suplimentare cu privire la aplicarea normelor din Regulamentul (UE) 2016/679, sub rezerva condițiilor prevăzute în regulamentul respectiv.
- (35) Pentru a fi legală, prelucrarea datelor cu caracter personal în temeiul prezentei directive ar trebui să fie necesară pentru îndeplinirea unei atribuții de interes public de către o autoritate competentă în temeiul dreptului Uniunii sau al dreptului intern, în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. Aceste activități ar trebui să acopere protejarea intereselor vitale ale persoanei vizate. Îndeplinirea sarcinilor de prevenire, depistare, investigare sau urmărire penală a infracțiunilor, conferită în mod instituțional prin lege autorităților competente, le permite acestora să solicite sau să impună persoanelor fizice să respecte cerințele formulate. În acest caz, consimțământul persoanei vizate, astfel cum este definit în Regulamentul (UE) 2016/679, nu ar trebui să constituie un temei juridic pentru prelucrarea datelor cu caracter personal de către autoritățile competente. În cazul în care i se solicită persoanei vizate să respecte o obligație legală, persoana vizată nu dispune cu adevărat de libertatea de alegere, astfel încât reacția persoanei vizate nu poate fi considerată ca o manifestare liberă a voinței sale. Acest lucru nu ar trebui să împiedice statele membre să prevadă prin lege că persoana vizată poate accepta prelucrarea datelor sale cu caracter personal în scopurile prezentei directive, cum ar fi testele ADN în anchetele penale sau monitorizarea localizării persoanei vizate prin dispozitive electronice pentru executarea pedepselor.
- (36) Statele membre ar trebui să prevadă că, în cazul în care dreptul Uniunii sau dreptul intern aplicabil autorității competente care a transmis datele prevede condiții specifice aplicabile în situații specifice prelucrării datelor cu caracter personal, cum ar fi folosirea unor coduri de utilizare, autoritatea competentă care a transmis datele ar trebui să informeze destinatarul respectivelor date cu caracter personal cu privire la astfel de condiții și obligația de a le respecta. Astfel de condiții ar putea include, de exemplu, interdicția de a transmite datele cu caracter personal altor destinatari sau de a le utiliza în alte scopuri decât cele pentru care au fost transmise destinatarului, sau de a informa persoana vizată în cazul unei limitări a dreptului la informare fără aprobarea prealabilă a autorității competente care a transmis datele. Obligațiile menționate ar trebui să se aplice, de asemenea, transferurilor realizate de autoritatea competentă care a transmis datele către destinatari din țări terțe sau către organizații internaționale. Statele membre ar trebui să garanteze neaplicarea de către autoritatea competentă care a transmis datele nu aplică în cazul destinatarilor din alte state membre sau în cazul agențiilor, oficiilor și organelor instituite în conformitate cu titlul V capitolele 4 și 5 din TFUE, alte condiții decât cele aplicabile transmiterii similare de date în statul membru al autorității competente respective.
- (37) Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale necesită o protecție specifică, deoarece contextul prelucrării acestora ar putea genera riscuri considerabile la adresa drepturilor și libertăților fundamentale. Aceste date cu caracter personal ar trebui să includă datele cu caracter personal care dezvăluie originea rasială sau etnică, utilizarea termenului „origine rasială”

în prezenta directivă neimplicând o acceptare de către Uniune a teoriilor care urmăresc să stabilească existența unor rase umane separate. Asemenea date cu caracter personal nu ar trebui prelucrate, cu excepția cazului în care prelucrarea face obiectul unor garanții adecvate pentru drepturile și libertățile persoanei vizate prevăzute de lege și este autorizată în cazuri prevăzute de lege; dacă nu este deja autorizată de o astfel de lege, prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane; sau prelucrarea se referă la date care sunt făcute publice în mod manifest de către persoana vizată. Garanțiile adecvate pentru drepturile și libertățile persoanei vizate ar putea include posibilitatea de a colecta aceste date numai în legătură cu alte date referitoare la persoana fizică respectivă, posibilitatea de a garanta în mod adecvat datele colectate, reguli mai stricte privind accesul la date al personalului autorității competente și interzicerea transmiterii datelor respective. Prelucrarea unor astfel de date ar trebui, de asemenea, să fie permisă de lege, atunci când persoana vizată a fost de acord în mod explicit, în cazurile în care prelucrarea este deosebit de intruzivă pentru aceasta. Cu toate acestea, consimțământul persoanei vizate nu ar trebui să constituie, în sine, un temei juridic pentru prelucrarea unor astfel de date sensibile cu caracter personal de către autoritățile competente.

- (38) Persoana vizată ar trebui să aibă dreptul de a nu face obiectul unei decizii care evaluează aspecte cu caracter personal referitoare la propria persoană, care se bazează exclusiv pe prelucrarea automată și care produce efecte juridice negative care privesc propria persoană sau o afectează în mod semnificativ. În orice caz, o astfel de prelucrare ar trebui să facă obiectul unor garanții corespunzătoare, inclusiv o informare specifică a persoanei vizate și dreptul acesteia de a obține intervenție umană, în special de a-și exprima punctul de vedere, de a primi o explicație privind decizia luată în urma unei astfel de evaluări sau de a contesta decizia. Crearea de profiluri care are drept rezultat discriminarea persoanelor fizice pe baza datelor cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale este interzisă în condițiile prevăzute la articolele 21 și 52 din Cartă.
- (39) Pentru ca persoana vizată să își poată exercita drepturile, toate informațiile adresate persoanei vizate ar trebui să fie ușor accesibile, inclusiv pe site-ul internet al operatorului, și ușor de înțeles, fiind necesar ca limbajul folosit să fie simplu și clar. Respectivul informații ar trebui să fie adaptate la nevoile persoanelor vulnerabile, cum ar fi copiii.
- (40) Ar trebui să fie prevăzute modalități de facilitare a exercitării de către persoana vizată a drepturilor care îi sunt conferite prin dispozițiile adoptate în temeiul prezentei directive, inclusiv mecanismele prin care aceasta poate solicita și, după caz obține, în mod gratuit, în special, acces la datele cu caracter personal, precum și rectificarea sau ștergerea acestora și restricționarea prelucrării. Operatorul ar trebui să aibă obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate, cu excepția cazului în care operatorul aplică limitări ale drepturilor persoanelor vizate în conformitate cu prezenta directivă. În plus, în cazul în care cererile sunt în mod vădit nefondate sau excesive, de exemplu atunci când persoana vizată solicită informații în mod nejustificat și repetat sau atunci când persoana vizată abuzează de dreptul său de a primi informații, de exemplu prin furnizarea de informații false sau înșelătoare în momentul efectuării cererii, operatorul ar trebui să poată percepe o taxă rezonabilă sau să refuze să dea curs cererii.
- (41) Atunci când operatorul solicită furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate, respectivul informații ar trebui să fie prelucrate numai în acest scop specific și nu ar trebui să fie stocate pentru o perioadă mai lungă decât cea necesară în acest scop specific.
- (42) Cel puțin următoarele informații ar trebui să fie puse la dispoziția persoanei vizate: identitatea operatorului, existența operațiunii de prelucrare, scopurile prelucrării, dreptul de a înainta o plângere și existența dreptului de a solicita operatorului accesul la prelucrare, precum și rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării. Acest lucru ar putea să se realizeze pe site-ul internet al autorității competente. În plus, în cazuri specifice și pentru a-i permite persoanei vizate să își exercite drepturile, persoana vizată ar trebui să fie informată cu privire la temeiul juridic al prelucrării și cu privire la cât timp vor fi stocate datele, în măsura în care astfel de informații suplimentare sunt necesare, având în vedere circumstanțele specifice în care sunt prelucrate datele, pentru a garanta o prelucrare echitabilă în ceea ce privește persoana vizată.
- (43) O persoană fizică ar trebui să aibă drept de acces la datele colectate care o privesc și ar trebui să își exercite acest drept cu ușurință și la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia. Orice persoană vizată ar trebui, prin urmare, să aibă dreptul de a cunoaște și de a i se comunica în ce scopuri sunt prelucrate datele, pentru ce perioadă sunt acestea prelucrate și care este identitatea destinatarilor datelor, inclusiv din țările terțe. Când respectiva comunicare include informații cu privire la originea datelor cu caracter personal, astfel de informații nu ar trebui să dezvăluie identitatea persoanelor fizice, în special a surselor confidențiale. Pentru ca acest drept să fie respectat, este suficient ca persoana vizată să dețină o sinteză completă a respectivelor date într-o formă inteligibilă, adică o formă care să permită persoanei vizate să ia cunoștință de aceste date și să verifice că acestea sunt exacte și prelucrate în conformitate cu prezenta directivă,

astfel încât persoana vizată să poată să își exercite drepturile care îi sunt conferite prin prezenta directivă. O astfel de sinteză ar putea fi furnizată sub forma unei copii a datelor cu caracter personal care sunt în curs de prelucrare.

- (44) Statele membre ar trebui să aibă posibilitatea de a adopta măsuri legislative în vederea amânării, a restricționării sau a omiterii informării persoanelor vizate sau în vederea restricționării, integrale sau parțiale, a accesului la datele lor cu caracter personal, în măsura în care și atât timp cât o astfel de măsură constituie o măsură necesară și proporțională într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice în cauză, pentru a se evita obstrucționarea cercetărilor, a anchetelor sau a procedurilor oficiale sau judiciare, pentru a nu se afecta prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea pedepselor, pentru a se apăra securitatea publică sau securitatea națională ori pentru a se apăra drepturile și libertățile altor persoane. Operatorul ar trebui să evalueze, prin intermediul unei examinări concrete și individuale a fiecărui caz în parte, dacă dreptul de acces ar trebui să fie limitat parțial sau complet.
- (45) Orice refuz sau limitare a accesului ar trebui, în principiu, să fie prezentată în scris persoanei vizate și ar trebui să includă motivele de fapt și de drept pe care se bazează decizia.
- (46) Orice limitare a drepturilor persoanei vizate trebuie să fie în conformitate cu Carta și cu CEDO, după cum a fost interpretată de jurisprudența Curții de Justiție și, respectiv, a Curții Europene a Drepturilor Omului și, îndeosebi, trebuie să respecte esența drepturilor și libertăților respective.
- (47) O persoană fizică ar trebui să aibă dreptul de a obține rectificarea datelor cu caracter personal inexacte care o privesc, mai ales când acestea se referă la fapte, precum și dreptul la ștergerea datelor în cazul în care prelucrarea datelor respective nu respectă prezenta directivă. Cu toate acestea, dreptul la rectificare nu ar trebui să afecteze, de exemplu, conținutul depozițiilor martorilor. O persoană fizică ar trebui să aibă, de asemenea, dreptul la restricționarea prelucrării atunci când această persoană contestă exactitatea datelor cu caracter personal și nu se poate stabili exactitatea sau inexactitatea lor sau în cazul în care datele cu caracter personal trebuie să fie păstrate ca mijloace de probă. În special, în loc ca datele cu caracter personal să fie șterse, prelucrarea ar trebui să fie restricționată dacă într-un caz specific există motive întemeiate să se considere că ștergerea lor ar putea afecta interesele legitime ale persoanei vizate. În acest caz, datele restricționate ar trebui să fie prelucrate doar în scopul care a împiedicat ștergerea lor. Metodele de restricționare a prelucrării ar putea include, printre altele, transferul datelor selectate în alt sistem de prelucrare, de exemplu în scopuri de arhivare, sau anularea accesului utilizatorilor la datele selectate. În ceea ce privește sistemele automatizate de evidență a datelor, restricționarea prelucrării de date cu caracter personal ar trebui, în principiu, asigurată prin mijloace tehnice; faptul că prelucrarea datelor cu caracter personal este restricționată ar trebui indicat în sistem în așa fel încât să se înțeleagă clar că această restricționare are loc. O astfel de rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării ar trebui să fie comunicată destinatarilor cărora le-au fost divulgate datele și autorităților competente de la care provin datele inexacte. Operatorii ar trebui, de asemenea, să nu comunice mai departe astfel de date.
- (48) În cazul în care operatorul refuză unei persoane vizate drepturile acesteia la informare, acces ori la rectificarea sau ștergerea datelor cu caracter personal sau la restricționarea prelucrării, persoana vizată ar trebui să aibă dreptul de a solicita ca autoritatea națională de supraveghere să verifice legalitatea prelucrării. Persoana vizată ar trebui să fie informată cu privire la acest drept. Atunci când autoritatea de supraveghere acționează în numele persoanei vizate, persoana vizată ar trebui să fie informată de către autoritatea de supraveghere cel puțin cu privire la faptul că toate verificările sau revizuirile necesare au fost efectuate de către autoritatea de supraveghere. Autoritatea de supraveghere ar trebui, de asemenea, să informeze persoana vizată în legătură cu dreptul de a introduce o cale de atac.
- (49) În cazul în care datele cu caracter personal sunt prelucrate în cadrul unei anchete penale și al unor acțiuni în instanță în materie penală, statele membre ar trebui să poată garanta exercitarea drepturilor la informare, acces și de rectificare sau ștergere a datelor cu caracter personal și de restricționare a prelucrării în conformitate cu normele naționale privind procedurile judiciare.
- (50) Ar trebui să se stabilească responsabilitatea și răspunderea operatorului pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său. În special, operatorul ar trebui să fie obligat să pună în aplicare măsuri adecvate și eficiente și să fie în măsură să demonstreze că activitățile de prelucrare respectă prezenta directivă. Măsurile respective ar trebui să țină seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul la adresa drepturilor și libertăților persoanelor fizice. Măsurile luate de operator ar trebui să includă elaborarea și punerea în aplicare a unor garanții specifice cu privire la tratamentul datelor cu caracter personal ale persoanelor vulnerabile, în special ale copiilor.
- (51) Riscurile la adresa drepturilor și libertăților persoanelor fizice, prezentând grade diferite de probabilitate și gravitate, pot fi rezultatul unei prelucrări a datelor care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care: prelucrarea poate genera discriminare, furtul sau uzurparea identității, prejudiciu financiar, compromiterea reputației, pierderea confidențialității datelor protejate prin secret profesional,

inversarea neautorizată a pseudonimizării sau la orice alt prejudiciu semnificativ de natură economică sau socială; persoanele vizate ar putea fi private de drepturile și libertățile lor sau de capacitatea de a-și exercita controlul asupra datelor lor cu caracter personal; datele cu caracter personal prelucrate sunt date care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, ori apartenența sindicală; sunt prelucrate date genetice sau date biometrice pentru identificarea singulară a unei persoane sau date privind sănătatea sau date privind viața sexuală și orientarea sexuală sau condamnările penale și infracțiunile sau măsurile de securitate conexe; sunt evaluate aspecte de natură personală, de exemplu analizarea și previzionarea unor aspecte privind randamentul la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, localizarea sau deplasările, în scopul de a se crea sau de a se utiliza profiluri personale; sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale copiilor; sau prelucrarea implică un volum mare de date cu caracter personal și afectează un număr larg de persoane vizate.

- (52) Probabilitatea și gravitatea riscului ar trebui să fie determinate în raport de natura, domeniul de aplicare, contextul și scopurile prelucrării. Riscul ar trebui să facă obiectul unei evaluări obiective, prin care să se stabilească dacă operațiunile de prelucrare a datelor prezintă un risc ridicat. Un risc ridicat este un risc deosebit de prejudiciere a drepturilor și libertăților persoanelor vizate.
- (53) Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare pentru a se asigura îndeplinirea cerințelor din prezenta directivă. Punerea în aplicare a unor astfel de măsuri nu ar trebui să se întemeieze doar pe considerente economice. Pentru a fi în măsură să demonstreze respectarea prezentei directive, operatorul ar trebui să adopte politici interne și să pună în aplicare măsuri care să adere, în special, la principiul protecției datelor începând cu momentul conceperii și al protecției implicite a datelor. În cazul în care operatorul a realizat o evaluare a impactului asupra protecției datelor în temeiul prezentei directive, ar trebui să se țină cont de rezultatele acesteia la elaborarea măsurilor și procedurilor respective. Măsurile ar putea consta, printre altele, în utilizarea pseudonimizării, cât mai curând posibil. Utilizarea pseudonimizării în sensul prezentei directive poate servi ca instrument care ar putea facilita, în special, libera circulație a datelor cu caracter personal în cadrul spațiului de libertate, securitate și justiție.
- (54) Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și a persoanelor împuternicite de către operator, inclusiv în ceea ce privește monitorizarea de către autoritățile de supraveghere și măsurile adoptate de acestea, necesită o atribuire clară a responsabilităților stabilite prin prezenta directivă, inclusiv în cazul în care un operator stabilește scopurile și mijloacele prelucrării împreună cu alți operatori sau în cazul în care o operațiune de prelucrare este efectuată în numele unui operator.
- (55) Efectuarea prelucrării de către o persoană împuternicită de către un operator ar trebui să fie reglementată printr-un act juridic care să includă un contract care creează obligații pentru persoana împuternicită de către operator în raport cu operatorul și care să stipuleze, în special, că persoana împuternicită de către operator ar trebui să acționeze numai la instrucțiunile operatorului. Persoana împuternicită de către operator ar trebui să țină cont de principiul protecției datelor începând cu momentul conceperii și al protecției implicite a datelor.
- (56) În vederea demonstrării conformității cu prezenta directivă, operatorul sau persoana împuternicită de către operator ar trebui să păstreze evidențe ale tuturor categoriilor de activități de prelucrare aflate în responsabilitatea sa. Fiecare operator și fiecare persoană împuternicită de către operator ar trebui să aibă obligația de a coopera cu autoritatea de supraveghere și de a pune la dispoziția acesteia, la cerere, aceste evidențe, pentru a putea fi utilizate în scopul monitorizării respectivelor operațiuni de prelucrare. Operatorul sau persoana împuternicită de către operator care prelucrează date cu caracter personal în sisteme de prelucrare neautomată ar trebui să dispună de metode eficiente pentru a demonstra legalitatea prelucrării, a permite monitorizarea proprie și a garanta integritatea și securitatea datelor, precum înregistrări sau alte forme de evidențe.
- (57) Înregistrările ar trebui păstrate cel puțin pentru operațiunile din cadrul sistemelor de prelucrare automată, precum colectarea, modificarea, consultarea, divulgarea, inclusiv transferurile, combinarea sau ștergerea. Identificarea persoanei care a consultat sau divulgat date cu caracter personal ar trebui să fie înregistrată și, plecând de la identificarea respectivă, ar putea fi posibil să se stabilească justificarea operațiunilor de prelucrare. Înregistrările ar trebui să fie utilizate numai pentru verificarea legalității prelucrării, monitorizarea proprie, asigurarea integrității și securității datelor și pentru proceduri penale. Monitorizarea proprie include, de asemenea, proceduri disciplinare interne ale autorităților competente.
- (58) Operatorul ar trebui să realizeze o evaluare a impactului asupra protecției datelor în cazurile în care operațiunile de prelucrare pot avea drept rezultat, prin natura, domeniul de aplicare sau scopurile lor, un risc ridicat la adresa drepturilor și libertăților persoanelor vizate, evaluare care ar trebui să includă în special măsurile, garanțiile și mecanismele preconizate în vederea asigurării protecției datelor cu caracter personal și a atestării conformității cu prezenta directivă. Evaluările impactului ar trebui să acopere sistemele și procesele relevante aferente operațiunilor de prelucrare, și nu cazuri individuale.

- (59) Pentru a garanta protecția eficientă a drepturilor și libertăților persoanelor vizate, operatorul sau persoana împuternicită de către operator ar trebui să se consulte cu autoritatea de supraveghere în anumite cazuri, înainte de prelucrare.
- (60) În vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezenta directivă, operatorul sau persoana împuternicită de către operator ar trebui să evalueze riscurile inerente prelucrării și să pună în aplicare măsuri pentru atenuarea acestor riscuri, precum criptarea. Măsurile respective ar trebui să asigure un nivel corespunzător de securitate, inclusiv de confidențialitate, luând în considerare stadiul actual al tehnologiei, costurile punerii lor în aplicare în raport cu riscurile și natura datelor cu caracter personal a căror protecție trebuie asigurată. La evaluarea riscurilor la adresa securității datelor, ar trebui să se acorde atenție riscurilor pe care le prezintă prelucrarea datelor, cum ar fi distrugerea, pierderea sau modificarea accidentală sau ilegală, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, care pot duce în special la prejudicii fizice, materiale sau morale. Operatorul și persoana împuternicită de către operator ar trebui să se asigure că prelucrarea datelor cu caracter personal nu se realizează de către persoane neautorizate.
- (61) Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate genera prejudicii fizice, materiale sau morale persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau uzurpare de identitate, prejudiciu financiar, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt prejudiciu important de natură economică sau socială cauzat acelei persoane fizice. Prin urmare, de îndată ce a luat cunoștință de producerea unei încălcări a securității datelor cu caracter personal, operatorul ar trebui să notifice încălcarea securității datelor cu caracter personal autorității de supraveghere fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore după ce a luat cunoștință de existența acesteia, cu excepția cazului în care operatorul este în măsură să demonstreze, în conformitate cu principiul responsabilității, că încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. Atunci când notificarea nu se poate realiza în termen de 72 de ore, aceasta ar trebui să cuprindă motivele întârzierii, iar informațiile pot fi furnizate treptat, fără altă întârziere.
- (62) Persoanele fizice ar trebui să fie notificate fără întârziere în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, pentru a le permite acestora să ia măsurile de precauție necesare. Notificarea ar trebui să descrie natura încălcării securității datelor cu caracter personal și să formuleze recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative. Notificarea persoanelor vizate ar trebui să fie efectuate în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu autoritatea de supraveghere și în conformitate cu orientările furnizate de aceasta sau de alte autorități relevante. De exemplu, necesitatea de a atenua un risc imediat de producere a unor prejudicii ar presupune notificarea cu promptitudine a persoanelor vizate, în timp ce necesitatea de a pune în aplicare măsuri corespunzătoare împotriva încălcării în continuare a securității datelor sau împotriva unor încălcări similare ale securității datelor ar putea justifica un termen mai îndelungat. În cazul în care evitarea obstrucționării cercetărilor, a anchetelor sau a procedurilor oficiale sau judiciare, evitarea aducerii de prejudicii la adresa prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau a executării pedepselor, a protejării securității publice, a protejării securității naționale sau a apărării drepturilor și libertăților altora nu pot fi obținute prin amânarea sau restricționarea comunicării unei încălcări a securității datelor cu caracter personal către persoana fizică în cauză, o astfel de comunicare ar putea fi omisă în circumstanțe excepționale.
- (63) Operatorul ar trebui să desemneze o persoană care să îi acorde asistență pentru a monitoriza respectarea, la nivel intern, a dispozițiilor adoptate în temeiul prezentei directive, cu excepția cazului în care un stat membru decide să exonereze instanțele și alte autorități judiciare independente atunci când acționează în exercițiul funcției lor judiciare. Persoana respectivă ar putea fi un membru al personalului existent al operatorului care a beneficiat de o formare specială în materie de legislație și practici privind protecția datelor pentru a dobândi cunoștințe de specialitate în domeniul respectiv. Nivelul necesar al cunoștințelor de specialitate ar trebui să se stabilească în special în funcție de prelucrarea efectuată asupra datelor și de gradul de protecție impus pentru datele cu caracter personal prelucrate de către operator. Îndeplinirea sarcinilor sale poate fi efectuată cu normă întreagă sau cu fracțiune de normă. Un responsabil cu protecția datelor poate fi numit în comun de mai mulți operatori, ținând seama de structura organizatorică și de dimensiunea acestora, de exemplu în caz de resurse comune în unitățile centrale. Persoana respectivă poate fi, de asemenea, numită în posturi diferite în cadrul structurii operatorilor relevanți. Persoana respectivă ar trebui să îl ajute pe operator și pe angajații care prelucrează date cu caracter personal, prin informarea și consilierea acestora cu privire la respectarea obligațiilor relevante ale acestora în materie de protecție a datelor. Astfel de responsabili cu protecția datelor ar trebui să fie în măsură să își îndeplinească îndatoririle și sarcinile în mod independent, în conformitate cu dreptul intern.
- (64) Statele membre ar trebui să asigure că transferul către o țară terță sau către o organizație internațională are loc numai în cazul în care acest transfer este necesar pentru prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau pentru executarea pedepselor, inclusiv pentru protejarea împotriva amenințărilor la adresa

securității publice și prevenirea acestora, iar operatorul din țara terță sau din organizația internațională este o autoritate competentă în sensul prezentei directive. Un transfer ar trebui să poată fi efectuat numai de către autoritățile competente, acționând în calitate de operatori, cu excepția cazului în care persoanele împuternicite de către operatori primesc instrucțiuni în mod expres să transfere în numele operatorilor. Un astfel de transfer poate avea loc în cazul în care Comisia decide că țara terță sau organizația internațională în cauză asigură un nivel adecvat de protecție, atunci când se asigură garanții corespunzătoare ori când se aplică derogări pentru situații speciale. În cazul în care se transferă date cu caracter personal din Uniune către operatori, persoane împuternicite de către operatori sau alți destinatari din țări terțe sau organizații internaționale, nivelul de protecție a persoanelor fizice garantat în Uniune prin prezenta directivă nu ar trebui să fie diminuat, inclusiv în cazurile de transferuri ulterioare de date cu caracter personal dinspre țara terță sau organizația internațională către operatori sau persoane împuternicite de către operatori din aceeași sau dintr-o altă țară terță sau organizație internațională.

- (65) În cazul transferului de date cu caracter personal de la un stat membru către țări terțe sau către organizații internaționale, un astfel de transfer ar trebui să aibă loc, în principiu, numai după ce statul membru de la care au fost obținute datele a acordat o autorizație în ceea ce privește transferul. Interesele unei cooperări eficiente în domeniul aplicării legii impun ca, în cazul în care natura unei amenințări la adresa securității publice a unui stat membru sau a unei țări terțe sau la adresa intereselor fundamentale ale unui stat membru este atât de urgentă încât să facă imposibilă obținerea unei autorizații prealabile în timp util, autoritatea competentă ar trebui să poată transfera datele cu caracter personal relevante către țara terță sau organizația internațională în cauză fără o astfel de autorizație prealabilă. Statele membre ar trebui să prevadă că orice condiții specifice pentru transfer ar trebui să fie comunicate țărilor terțe sau organizațiilor internaționale. Transferurile ulterioare de date cu caracter personal ar trebui să facă obiectul autorizării prealabile de către autoritatea competentă care a realizat transferul inițial. Atunci când decide cu privire la o cerere de autorizare a unui transfer ulterior, autoritatea competentă care a realizat transferul inițial ar trebui să țină seama în mod corespunzător de toți factorii relevanți, inclusiv de gravitatea infracțiunii, de condițiile specifice transferului și de scopul pentru care datele au fost transferate inițial, de natura și condițiile executării pedepsei, precum și de nivelul de protecție a datelor cu caracter personal din țara terță sau dintr-o organizație internațională către care datele cu caracter personal sunt transferate ulterior. Autoritatea competentă care a realizat transferul inițial ar trebui, de asemenea, să poată aplica transferului ulterior condiții specifice. Astfel de condiții specifice pot fi descrise, de exemplu, în coduri de utilizare.
- (66) Comisia ar trebui să poată decide, cu efect în întreaga Uniune, că anumite țări terțe, un teritoriu ori unul sau mai multe sectoare determinate dintr-o țară terță sau o organizație internațională oferă un nivel adecvat de protecție a datelor, furnizând astfel securitate juridică și uniformitate în întreaga Uniune în ceea ce privește țările terțe sau organizațiile internaționale care sunt considerate a furniza un astfel de nivel de protecție. În astfel de cazuri, transferurile de date cu caracter personal către țările respective ar trebui să se poată realiza fără a fi necesară obținerea unei autorizații speciale, cu excepția cazului în care un alt stat membru de la care au fost obținute datele trebuie să își dea autorizația pentru transfer.
- (67) În conformitate cu valorile fundamentale pe care se întemeiază Uniunea, în special apărarea drepturilor omului, Comisia ar trebui, în evaluarea sa referitoare la țara terță sau la un teritoriu sau la un sector determinat dintr-o țară terță, să ia în considerare modul în care o anumită țară terță respectă statul de drept, accesul la justiție, precum și normele și standardele internaționale în materie de drepturi ale omului și legislația sa generală și sectorială, inclusiv legislația privind securitatea publică, apărarea și securitatea națională, precum și ordinea publică și dreptul penal. Adoptarea unei decizii privind caracterul adecvat al nivelului de protecție în ceea ce privește un teritoriu sau un sector determinat dintr-o țară terță ar trebui să țină seama de criterii clare și obiective, cum ar fi activitățile specifice de prelucrare și domeniul de aplicare al standardelor juridice aplicabile și legislația în vigoare în țara terță respectivă. Țara terță ar trebui să garanteze un nivel adecvat de protecție, echivalent în esență celui asigurat în cadrul Uniunii, în special atunci când datele sunt prelucrate în unul sau mai multe sectoare specifice. În special, țara terță ar trebui să asigure o supraveghere efectivă independentă în materie de protecție a datelor și să prevadă mecanisme de cooperare cu autoritățile de protecție a datelor din statele membre, iar persoanele vizate ar trebui să beneficieze de drepturi efective și opozabile și de reparații efective pe cale administrativă și judiciară.
- (68) Pe lângă angajamentele internaționale asumate de țara terță sau de organizația internațională, Comisia ar trebui să țină seama și de obligațiile care decurg din participarea țării terțe sau a organizației internaționale la sistemele multilaterale sau regionale, în special în ceea ce privește protecția datelor cu caracter personal, precum și de punerea în aplicare a unor astfel de obligații. În special, ar trebui să fie luată în considerare aderarea țării terțe la Convenția Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal și la protocolul adițional la aceasta. Comisia ar trebui să consulte

Comitetul european pentru protecția datelor instituit prin Regulamentul (UE) 2016/679 („comitetul”) atunci când evaluează nivelul de protecție din țările terțe sau din organizațiile internaționale. De asemenea, Comisia ar trebui să țină seama de orice decizie relevantă a Comisiei privind caracterul adecvat al nivelului de protecție, adoptată în conformitate cu articolul 45 din Regulamentul (UE) 2016/679.

- (69) Comisia ar trebui să monitorizeze funcționarea deciziilor privind nivelul de protecție dintr-o țară terță, un teritoriu sau un sector determinat dintr-o țară terță sau dintr-o organizație internațională. În ceea ce privește deciziile sale privind caracterul adecvat al nivelului de protecție, Comisia ar trebui să prevadă un mecanism de revizuire periodică a funcționării acestora. Această revizuire periodică ar trebui să se realizeze în consultare cu țara terță sau cu organizația internațională în cauză și ar trebui să ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională.
- (70) Comisia ar trebui, de asemenea, să fie în măsură să constate faptul că o țară terță, un teritoriu sau un sector determinat dintr-o țară terță ori o organizație internațională nu mai asigură un nivel corespunzător de protecție a datelor. În consecință, transferul de date cu caracter personal către țara terță sau organizația internațională respectivă ar trebui să fie interzis, cu excepția cazului când sunt îndeplinite cerințele prevăzute în prezenta directivă referitoare la transferul de date sub rezerva unor garanții adecvate și a unor derogări în situații specifice. Ar trebui să se prevadă proceduri de consultare între Comisie și astfel de țări terțe sau organizații internaționale. Comisia ar trebui ca, în timp util, să informeze țara terță sau organizația internațională cu privire la aceste motive și să inițieze consultări cu aceasta pentru remedierea situației.
- (71) Transferurile care nu se întemeiază pe o astfel de decizie privind caracterul adecvat al nivelului de protecție ar trebui să fie permise numai în cazul în care au fost prezentate garanții corespunzătoare într-un instrument cu caracter juridic obligatoriu, care să asigure protecția datelor cu caracter personal, sau în cazul în care operatorul a evaluat toate circumstanțele legate de datele transferate și, pe baza acestei evaluări, consideră că există garanții adecvate în ceea ce privește protecția datelor cu caracter personal. Astfel de instrumente cu caracter juridic obligatoriu ar putea fi, de exemplu, acorduri bilaterale cu caracter juridic obligatoriu care au fost încheiate de statele membre și puse în aplicare în ordinea juridică a acestora și a căror respectare poate fi impusă de către persoanele vizate din respectivele state membre, asigurând respectarea cerințelor în materie de protecție a datelor și drepturile persoanelor vizate, inclusiv dreptul de a obține reparații efective pe cale administrativă sau judiciară. Operatorul ar trebui să ia în considerare acordurile de cooperare încheiate între Europol sau Eurojust și țări terțe care permit schimbul de date cu caracter personal atunci când se efectuează evaluarea tuturor circumstanțelor legate de transferul de date. Operatorul ar trebui, de asemenea, să poată lua în considerare faptul că transferul de date cu caracter personal va fi supus obligațiilor de confidențialitate și principiului specificității, asigurându-se că datele nu vor fi prelucrate în alte scopuri decât cel al transferului. În plus, operatorul ar trebui să ia în considerare faptul că datele cu caracter personal nu vor fi folosite pentru a solicita, a pronunța sau a executa pedeapsa cu moartea sau orice altă formă de tratament crud și inuman. Chiar dacă aceste condiții ar putea fi considerate garanții adecvate care să permită transferul de date, operatorul ar trebui să poată solicita garanții suplimentare.
- (72) În cazul în care nu există nicio decizie privind caracterul adecvat al nivelului de protecție sau nicio garanție adecvată, un transfer sau o categorie de transferuri poate avea loc numai în situații specifice, dacă este necesar în scopul protejării intereselor vitale ale persoanei vizate sau ale unei alte persoane sau al protejării intereselor legitime ale persoanei vizate, în cazul în care se prevede astfel în dreptul statului membru care transferă datele cu caracter personal; pentru prevenirea unei amenințări imediate și grave la adresa securității publice a unui stat membru sau a unei țări terțe; într-un caz specific, în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv în scopul protejării împotriva amenințărilor la adresa securității publice; sau, într-un caz specific, pentru constatarea, exercitarea sau apărarea unui drept în instanță. Aceste derogări ar trebui interpretate restrictiv și nu ar trebui să permită transferuri frecvente, masive și structurale de date cu caracter personal sau transferuri la scară largă de date, ci ar trebui să se limiteze la datele strict necesare. Astfel de transferuri ar trebui să fie documentate și să fie puse la dispoziția autorității de supraveghere la cerere, în scopul monitorizării legalității transferului.
- (73) Autoritățile competente ale statelor membre aplică acordurile internaționale bilaterale sau multilaterale în vigoare, încheiate cu țări terțe în domeniul cooperării judiciare în materie penală și al cooperării polițienești, în schimbul obținerii de informații relevante care să le permită să își îndeplinească sarcinile atribuite în mod legal. În principiu, acest lucru are loc prin intermediul sau cel puțin cu cooperarea autorităților competente din țările terțe implicate în scopul prezentei directive, uneori chiar în absența unui acord internațional bilateral sau multilateral. Cu toate acestea, în anumite cazuri individuale, procedurile obișnuite care necesită contactarea autorității din țara terță pot fi ineficiente sau inadecvate, în special din cauza faptului că transferul nu poate fi efectuat în timp util sau din cauza faptului că autoritatea din țara terță nu respectă statul de drept sau normele și standardele internaționale în materie de drepturi ale omului, astfel încât autoritățile competente ale statelor membre ar putea decide să transfere datele cu caracter personal direct beneficiarilor stabiliți în țări terțe. Acesta ar putea fi cazul atunci când există o nevoie urgentă de a transfera date cu caracter personal pentru a salva viața unei persoane care se află în pericol de a deveni victimă a unei infracțiuni sau în interesul prevenirii săvârșirii iminente a unei infracțiuni, inclusiv a terorismului. Chiar dacă acest transfer între autoritățile competente și destinatarii stabiliți în

țări terțe ar trebui să aibă loc numai în anumite cazuri individuale, prezenta directivă ar trebui să prevadă condițiile pentru reglementarea unor astfel de cazuri. Aceste dispoziții nu ar trebui să fie considerate derogări de la niciun acord internațional bilateral sau multilateral existent în domeniul cooperării judiciare în materie penală și al cooperării polițienești. Aceste norme ar trebui să se aplice în completarea altor norme din directivă, în special cele cu privire la legalitatea prelucrării și cele din capitolul V.

- (74) Fluxul transfrontalier de date cu caracter personal poate expune unui risc sporit capacitatea persoanelor fizice de a-și exercita drepturile în materie de protecție a datelor pentru a se proteja împotriva utilizării sau a divulgării ilegale a acestor date. În același timp, autoritățile de supraveghere pot constata că se află în imposibilitatea de a da curs unor plângeri sau de a efectua investigații referitoare la activitățile desfășurate în afara frontierelor lor. Eforturile lor de a conlucra în context transfrontalier pot fi, de asemenea, îngreunate de insuficiența competențelor de prevenire sau remediere și de caracterul eterogen al regimurilor juridice. Prin urmare, este necesar să se promoveze o cooperare mai strânsă între autoritățile de supraveghere a protecției datelor pentru a le ajuta să facă schimb de informații cu omologii lor străini.
- (75) Instituirea în statele membre a unor autorități de supraveghere capabile să își exercite atribuțiile în deplină independență reprezintă un element esențial al protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Autoritățile de supraveghere ar trebui să monitorizeze aplicarea dispozițiilor adoptate în temeiul prezentei directive și ar trebui să contribuie la aplicarea ei consecventă în întreaga Uniune, în scopul asigurării protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. În acest scop, autoritățile de supraveghere ar trebui să coopereze între ele și cu Comisia.
- (76) Statele membre pot încredința unei autorități de supraveghere deja înființate în temeiul Regulamentului (UE) 2016/679 responsabilitatea pentru sarcinile care urmează să fie îndeplinite de către autoritățile naționale de supraveghere care urmează a fi înființate în temeiul prezentei directive.
- (77) Statele membre ar trebui să aibă posibilitatea de a institui mai multe autorități de supraveghere, pentru a reflecta structura lor constituțională, organizatorică și administrativă. Fiecare autoritate de supraveghere ar trebui să beneficieze de resurse financiare și umane, de localuri și de infrastructura necesare pentru îndeplinirea cu eficacitate a sarcinilor lor, inclusiv a celor legate de asistența reciprocă și cooperarea cu alte autorități de supraveghere în întreaga Uniune. Fiecare autoritate de supraveghere ar trebui să aibă un buget public anual distinct, care poate face parte din bugetul general de stat sau național.
- (78) Autoritățile de supraveghere ar trebui să facă obiectul unui control independent sau al unor mecanisme de monitorizare în ceea ce privește cheltuielile lor financiare, cu condiția ca acest control financiar să nu le afecteze independența.
- (79) Condițiile generale pentru membrul sau membrii autorității de supraveghere ar trebui stabilite prin dreptul intern și ar trebui, în special, să prevadă că respectivii membri ar trebui să fie numiți de parlamentul și/sau de guvernul ori de șeful de stat al statului membru în cauză, pe baza unei propuneri din partea guvernului sau a unui membru al guvernului ori din partea parlamentului sau camerei acestuia, ori de către un organism independent împuternicit prin dreptul intern să facă numirea prin intermediul unei proceduri transparente. În vederea asigurării independenței autorității de supraveghere, membrul sau membrii acesteia ar trebui să dea dovadă de integritate, nu ar trebui să întreprindă acțiuni incompatibile cu îndatoririle lor, iar, pe durata mandatului, nu ar trebui să desfășoare activități incompatibile, remunerate sau nu. În vederea asigurării independenței autorității de supraveghere, personalul ar trebui să fie ales de autoritatea de supraveghere, ceea ce poate include o intervenție din partea unui organism independent împuternicit în acest sens prin dreptul intern.
- (80) Cu toate că prezenta directivă se aplică, de asemenea, activităților instanțelor naționale și ale altor autorități judiciare, prelucrarea datelor cu caracter personal nu ar trebui să fie de competența autorităților de supraveghere atunci când instanțele acționează în exercițiul funcției lor judiciare, în scopul asigurării independenței judecătorilor în îndeplinirea sarcinilor lor judiciare. Această derogare ar trebui să se limiteze la activități judiciare în cadrul acțiunilor în instanță și să nu se aplice altor activități în care judecătorii ar putea fi implicați, în conformitate cu dreptul intern. Statele membre ar trebui, de asemenea, să poată să prevadă faptul că nu este de competența autorității de supraveghere prelucrarea datelor cu caracter personal ale altor autorități judiciare independente care acționează în exercițiul funcției lor judiciare, de exemplu ministerul public. În orice caz, respectarea normelor prezentei directive de către instanțe și alte autorități judiciare independente face întotdeauna obiectul unei supravegheri independente în conformitate cu articolul 8 alineatul (3) din Cartă.

- (81) Fiecare autoritate de supraveghere ar trebui să trateze plângerile depuse de orice persoană vizată și ar trebui să investigheze cazul sau să-l transmită autorității de supraveghere competente. Investigația în urma unei plângeri ar trebui să fie efectuată, sub rezerva controlului jurisdicțional, în măsura necesară fiecărui caz. Autoritatea de supraveghere ar trebui să informeze persoana vizată cu privire la evoluția și soluționarea plângerii într-un termen rezonabil. În eventualitatea în care cazul necesită o investigație suplimentară sau coordonarea cu o altă autoritate de supraveghere, ar trebui să se furnizeze informații intermediare persoanei vizate.
- (82) Pentru a se asigura eficacitatea, fiabilitatea și consecvența monitorizării respectării și a aplicării prezentei directive în întreaga Uniune, în conformitate cu TFUE, astfel cum a fost interpretat de Curtea de Justiție, autorităților de supraveghere din fiecare stat membru ar trebui să le revină aceleași sarcini și competențe efective, inclusiv competențe de investigare, corective și de consiliere, care constituie mijloace necesare pentru îndeplinirea sarcinilor lor. Cu toate acestea, competențele acestora nu ar trebui să afecteze normele speciale de procedură penală, inclusiv cele referitoare la investigarea și urmărirea penală a infracțiunilor, sau independența justiției. Fără a aduce atingere competențelor autorităților de urmărire penală în temeiul dreptului intern, autoritățile de supraveghere ar trebui să aibă, de asemenea, competența de a aduce în atenția autorităților judiciare cazurile de încălcare a prezentei directive sau de a desfășura proceduri judiciare. Competențele autorităților de supraveghere ar trebui să fie exercitate în conformitate cu garanțiile procedurale adecvate prevăzute în dreptul Uniunii și în dreptul intern, în mod imparțial, echitabil și într-un termen rezonabil. În special, fiecare măsură ar trebui să fie adecvată, necesară și proporțională în scopul de a asigura conformitatea cu prezenta directivă, luând în considerare circumstanțele fiecărui caz în parte, să respecte dreptul oricărei persoane de a fi ascultată înainte de a fi luată orice măsură individuală care ar putea să îi aducă atingere și să evite costurile inutile și inconveniente excesive pentru persoanele în cauză. Competențele de investigare în ceea ce privește accesul în incinte ar trebui exercitate în conformitate cu cerințele specifice din dreptul intern, cum ar fi obligația de a obține în prealabil o autorizare judiciară. Adoptarea unei decizii obligatorii din punct de vedere juridic ar trebui să facă obiectul controlului jurisdicțional în statul membru al autorității de supraveghere care a adoptat decizia.
- (83) Autoritățile de supraveghere ar trebui să se sprijine reciproc în îndeplinirea sarcinilor care le revin și ar trebui să își acorde asistență reciprocă, pentru a se asigura aplicarea consecventă a dispozițiilor adoptate în temeiul prezentei directive.
- (84) Comitetul, ar trebui să contribuie la aplicarea coerentă a prezentei directive în întreaga Uniune, inclusiv prin consilierea Comisiei și prin promovarea cooperării autorităților de supraveghere în întreaga Uniune.
- (85) Orice persoană vizată ar trebui să aibă dreptul de a depune o plângere la o singură autoritate de supraveghere și la o cale de atac eficientă în conformitate cu articolul 47 din Cartă, în cazul în care persoana vizată consideră că sunt încălcate drepturile care îi revin în conformitate cu dispozițiile adoptate în temeiul prezentei directive sau în cazul în care autoritatea de supraveghere nu dă curs unei plângeri, respinge sau refuză parțial sau total o plângere sau nu acționează atunci când o astfel de acțiune este necesară pentru asigurarea protecției drepturilor persoanei vizate. Investigația în urma unei plângeri ar trebui să fie efectuată, făcând obiectul controlului jurisdicțional, în măsura în care este necesar, în funcție de caz. Autoritatea de supraveghere competentă ar trebui să informeze persoana vizată cu privire la evoluția și soluționarea plângerii într-un termen rezonabil. În eventualitatea în care cazul necesită o investigație suplimentară sau coordonarea cu o altă autoritate de supraveghere, ar trebui să se furnizeze informații intermediare persoanei vizate. În vederea facilitării depunerii plângerilor, fiecare autoritate de supraveghere ar trebui să ia măsuri precum punerea la dispoziție a unui formular de depunere a plângerii, care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.
- (86) Orice persoană fizică sau juridică ar trebui să aibă dreptul la o cale de atac eficientă în fața instanței naționale competente, împotriva unei decizii a unei autorități de supraveghere care produce efecte juridice privind persoana respectivă. O astfel de decizie se referă în special la exercitarea competențelor de investigare, corective și de autorizare de către autoritatea de supraveghere sau la refuzul sau respingerea plângerilor. Cu toate acestea, dreptul respectiv nu privește alte măsuri ale autorităților de supraveghere care nu sunt obligatorii din punct de vedere juridic, cum ar fi avizele emise de autoritatea de supraveghere sau consultanța furnizată de aceasta. Acțiunile inițiate împotriva unei autorități de supraveghere ar trebui să fie aduse în fața instanțelor statului membru în care este stabilită autoritatea de supraveghere și ar trebui să se desfășoare în conformitate cu dreptul intern al statului membru respectiv. Respectivele instanțe ar trebui să își exercite competența deplină, care ar trebui să includă competența de a examina toate aspectele de fapt sau de drept care au relevanță pentru litigiul cu care acestea sunt sesizate.
- (87) În cazul în care persoana vizată consideră că drepturile sale în temeiul prezentei directive sunt încălcate, aceasta ar trebui să aibă dreptul să mandateze un organism care are drept obiectiv asigurarea protecției drepturilor și a

intereselor persoanelor vizate în ceea ce privește protecția datelor acestora cu caracter personal și este constituit în conformitate cu dreptul intern, să depună o plângere în numele persoanei vizate la o autoritate de supraveghere sau să exercite dreptul la o cale de atac. Dreptul de reprezentare a persoanelor vizate ar trebui să nu aducă atingere dreptului procedural intern care poate impune reprezentarea în mod obligatoriu a persoanelor vizate de un avocat, astfel cum este definit în Directiva 77/249/CEE a Consiliului ⁽¹⁾, în fața instanțelor naționale.

- (88) Orice daună pe care o persoană o poate suferi ca urmare a unei prelucrări care încalcă dispozițiile adoptate în temeiul prezentei directive ar trebui să fie despăgubită de operator sau de orice altă autoritate competentă în conformitate cu dreptul intern respectiv. Conceptul de „prejudiciu” ar trebui interpretat, în sens larg, din perspectiva jurisprudenței Curții de Justiție, într-un mod care să reflecte pe deplin obiectivele prezentei directive. Prezenta dispoziție nu aduce atingere niciunei acțiuni în despăgubire care rezultă din încălcarea altor norme din dreptul Uniunii sau din dreptul intern. Atunci când se face trimitere la o prelucrare care este ilegală sau care încalcă dispozițiile adoptate în temeiul prezentei directive, trimiterea vizează și prelucrarea care nu respectă actele de punere în aplicare adoptate în temeiul prezentei directive. Persoanele vizate ar trebui să primească despăgubiri integrale și efective pentru prejudiciile suferite.
- (89) Ar trebui să se aplice sancțiuni oricărei persoane fizice sau juridice, de drept privat sau public, care încalcă prezenta directivă. Statele membre ar trebui să se asigure că sancțiunile sunt eficace, proporționale și disuasive și ar trebui să adopte toate măsurile pentru aplicarea sancțiunilor.
- (90) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentei directive, Comisiei ar trebui să i confere competențe de executare referitor la nivelul adecvat de protecție oferit de o țară terță, de un teritoriu sau de un sector determinat din țara terță respectivă sau de o organizație internațională, formatul și procedurile pentru asistență reciprocă și modalitățile de schimb de informații prin mijloace electronice între autoritățile de supraveghere, precum și între autoritățile de supraveghere și comitet. Competențele respective ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ⁽²⁾.
- (91) Procedura de examinare ar trebui să fie utilizată pentru adoptarea actelor de punere în aplicare privind nivelul adecvat de protecție oferit de o țară terță, de un teritoriu sau de un sector determinat din țara terță respectivă sau de o organizație internațională, precum și privind formatul și procedurile pentru asistență reciprocă și modalitățile de schimb de informații prin mijloace electronice între autoritățile de supraveghere și între autoritățile de supraveghere și comitet, ținând seama de faptul că actele respective au un caracter general.
- (92) Comisia ar trebui să adopte acte de punere în aplicare imediat aplicabile atunci când acest lucru se impune din motive imperative de urgență, în cazuri justificate în mod corespunzător referitoare la o țară terță, la un teritoriu sau la un sector determinat din țara terță respectivă sau la o organizație internațională care nu mai asigură un nivel de protecție adecvat.
- (93) Întrucât obiectivele prezentei directive, și anume protejarea drepturilor și a libertăților fundamentale ale persoanelor fizice, în special dreptul acestora la protecția datelor cu caracter personal și asigurarea liberului schimb de date cu caracter personal de către autoritățile competente în cadrul Uniunii, nu pot fi realizate în mod satisfăcător de către statele membre ci, datorită amplitudinii sau a efectelor acțiunii, pot fi realizate mai bine la nivelul Uniunii, Uniunea poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este definit la articolul 5 din TUE. În conformitate cu principiul proporționalității, astfel cum este definit la articolul respectiv, prezenta directivă nu depășește ceea ce este necesar pentru realizarea obiectivelor menționate.
- (94) Dispozițiile speciale din actele Uniunii adoptate în domeniul cooperării judiciare în materie penală și al cooperării polițienești, care au fost adoptate înainte de data adoptării prezentei directive, care reglementează prelucrarea datelor cu caracter personal între statele membre sau accesul autorităților desemnate ale statelor membre la

⁽¹⁾ Directiva 77/249/CEE a Consiliului din 22 martie 1977 de facilitare a exercitării efective a libertății de a presta servicii de către avocați (JO L 78, 26.3.1977, p. 17).

⁽²⁾ Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

sistemele de informații stabilite în conformitate cu tratatele, ar trebui să rămână neatinse, cum ar fi, de exemplu, dispozițiile speciale referitoare la protecția datelor cu caracter personal aplicate în conformitate cu Decizia 2008/615/JAI a Consiliului ⁽¹⁾, sau articolul 23 din Convenția privind asistența judiciară reciprocă în materie penală între statele membre ale Uniunii Europene ⁽²⁾. Întrucât articolul 8 din Cartă și articolul 16 din TFUE prevăd că dreptul fundamental la protecția datelor cu caracter personal trebuie să fie asigurat în mod consecvent în întreaga Uniune, Comisia ar trebui să evalueze situația în ceea ce privește relația dintre prezenta directivă și actele adoptate înainte de data adoptării prezentei directive care reglementează prelucrarea datelor cu caracter personal între statele membre și accesul autorităților desemnate de statele membre la sistemele de informații instituite în conformitate cu tratatele, pentru a evalua necesitatea alinierii acestor dispoziții specifice cu prezenta directivă. Dacă este cazul, Comisia ar trebui să prezinte propuneri cu scopul de a asigura norme juridice coerente privind prelucrarea datelor cu caracter personal.

- (95) În vederea asigurării unei protecții globale și consecvente a datelor cu caracter personal în cadrul Uniunii, acordurile internaționale care au fost încheiate de către statele membre înainte de data intrării în vigoare a prezentei directive și care respectă dispozițiile relevante din dreptul Uniunii aplicabil înainte de data respectivă ar trebui să rămână în vigoare până la data la care sunt modificate, înlocuite sau revocate.
- (96) Statelor membre ar trebui să le fie acordat un termen de cel mult doi ani de la data intrării în vigoare a prezentei directive în vederea transpunerii sale. Prelucrările în derulare la data menționată ar trebui să fie aduse în conformitate cu prezenta directivă în termen de doi ani de la data intrării în vigoare a prezentei directive. Cu toate acestea, în cazul în care o astfel de prelucrare respectă dreptul Uniunii aplicabil înainte de data intrării în vigoare a prezentei directive, cerințele din prezenta directivă cu privire la consultarea prealabilă a autorității de supraveghere nu ar trebui să se aplice operațiunilor de prelucrare aflate deja în derulare la data menționată, având în vedere că respectivele cerințe, prin însăși natura lor, trebuie să fie îndeplinite înainte de prelucrare. În cazul în care statele membre aplică termenul mai lung pentru punerea în aplicare, care expiră după șapte ani de la data intrării în vigoare a prezentei directive, pentru îndeplinirea obligațiilor de înregistrare pentru sistemele de prelucrare automată instituite înainte de data respectivă, operatorul sau persoana împuternicită de către operator ar trebui să dispună de metode eficiente pentru a demonstra legalitatea prelucrării datelor, a permite monitorizarea proprie și a garanta integritatea și securitatea datelor, precum înregistrări sau alte forme de evidențe.
- (97) Prezenta directivă se aplică fără a aduce atingere normelor privind combaterea abuzului sexual, a exploatării sexuale a copiilor și a pornografiei infantile, astfel cum se prevede în Directiva 2011/93/UE a Parlamentului European și a Consiliului ⁽³⁾.
- (98) Decizia-cadru 2008/977/JAI a Consiliului ar trebui, prin urmare, să fie abrogată.
- (99) În conformitate cu articolul 6a din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei în ceea ce privește spațiul de libertate, securitate și justiție, anexat la TUE și la TFUE, Regatului Unit și Irlandei nu le revin obligații în temeiul normelor stabilite în prezenta directivă referitoare la prelucrarea datelor cu caracter personal de către statele membre în exercitarea activităților care intră în domeniul de aplicare al părții a treia titlul V capitolul 4 sau 5 din TFUE, atât timp cât Regatului Unit sau Irlandei nu le revin obligații în temeiul normelor Uniunii privind formele de cooperare judiciară în materie penală sau de cooperare polițienească care necesită respectarea dispozițiilor stabilite în temeiul articolului 16 din TFUE.
- (100) În conformitate cu articolele 2 și 2a din Protocolul nr. 22 privind poziția Danemarcei, astfel cum a fost anexat la TUE și la TFUE, Danemarcei nu îi revin obligații în temeiul normelor stabilite în prezenta directivă și acestea nu i se aplică în ceea ce privește prelucrarea datelor cu caracter personal de către statele membre în exercitarea activităților care intră sub incidența părții a treia titlul V capitolul 4 sau 5 din TFUE. Având în vedere faptul că prezenta directivă constituie o dezvoltare a acquis-ului Schengen, în temeiul părții a treia titlul V din TFUE, Danemarca decide, în conformitate cu articolul 4 din protocolul respectiv, în termen de șase luni de la adoptarea prezentei directive, dacă o va pune în aplicare în dreptul său intern.
- (101) În ceea ce privește Islanda și Norvegia, prezenta directivă constituie o dezvoltare a dispozițiilor acquis-ului Schengen, în conformitate cu Acordul încheiat între Consiliul Uniunii Europene și de Republica Islanda și Regatul Norvegiei în ceea ce privește asocierea acestor două state la implementarea, aplicarea și dezvoltarea acquis-ului Schengen ⁽⁴⁾.

⁽¹⁾ Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008, p. 1).

⁽²⁾ Actul Consiliului din 29 mai 2000 de elaborare, în temeiul articolului 34 din Tratatul privind Uniunea Europeană, a Convenției privind asistența judiciară reciprocă în materie penală între statele membre ale Uniunii Europene (JO C 197, 12.7.2000, p. 1).

⁽³⁾ Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului (JO L 335, 17.12.2011, p. 1).

⁽⁴⁾ JO L 176, 10.7.1999, p. 36.

- (102) În ceea ce privește Elveția, prezenta directivă constituie o dezvoltare a dispozițiilor acquis-ului Schengen, în conformitate cu Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen ⁽¹⁾.
- (103) În ceea ce privește Liechtenstein, prezenta directivă reprezintă o dezvoltare a dispozițiilor acquis-ului Schengen, astfel cum se prevede în Protocolul dintre Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen ⁽²⁾.
- (104) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de cartă, astfel cum sunt consacrate în TFUE, în special dreptul la respectarea vieții private și de familie, dreptul la protecția datelor cu caracter personal, dreptul la o cale de atac eficientă și la un proces echitabil. Limitările aduse acestor drepturi sunt în conformitate cu articolul 52 alineatul (1) din Cartă întrucât sunt necesare pentru atingerea obiectivelor de interes general recunoscute de Uniune sau pentru a proteja drepturile și libertățile celorlalți.
- (105) În conformitate cu Declarația politică comună a statelor membre și a Comisiei din 28 septembrie 2011 privind documentele explicative, statele membre s-au angajat să însoțească, în cazurile justificate, notificarea măsurilor de transpunere cu unul sau mai multe documente care să explice relația dintre componentele unei directive și părțile corespunzătoare din măsurile naționale de transpunere. În ceea ce privește prezenta directivă, legiuitorul consideră că este justificată transmiterea unor astfel de documente.
- (106) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 și a emis un aviz la data de 7 martie 2012 ⁽³⁾.
- (107) Prezenta directivă nu ar trebui să împiedice statele membre să pună în aplicare exercitarea, în cadrul procedurilor penale, a drepturilor persoanelor vizate cu privire la informare, acces și rectificarea sau ștergerea datelor cu caracter personal și restricționare a prelucrării, precum și eventualele limitări ale acestor drepturi în normele procedurale penale de drept intern,

ADOPTĂ PREZENTA DIRECTIVĂ:

CAPITOLUL I

Dispoziții generale

Articolul 1

Obiect și obiective

(1) Prezenta directivă stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora.

(2) În conformitate cu prezenta directivă, statele membre:

- (a) protejează drepturile și libertățile fundamentale ale persoanelor fizice, în special dreptul acestora la protecția datelor cu caracter personal; și
- (b) se asigură că schimbul de date cu caracter personal de către autoritățile competente în cadrul Uniunii, în cazul în care schimbul respectiv de informații este impus de dreptul Uniunii sau de dreptul intern, nu este limitat sau interzis din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

⁽¹⁾ JO L 53, 27.2.2008, p. 52.

⁽²⁾ JO L 160, 18.6.2011, p. 21.

⁽³⁾ JO C 192, 30.6.2012, p. 7.

(3) Prezenta directivă nu împiedică statele membre să prevadă garanții sporite față de cele stabilite în prezenta directivă pentru protecția drepturilor și libertăților persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente.

Articolul 2

Domeniul de aplicare

(1) Prezenta directivă se aplică prelucrării datelor cu caracter personal de către autoritățile competente în scopurile prevăzute la articolul 1 alineatul (1).

(2) Prezenta directivă se aplică prelucrării datelor cu caracter personal realizate integral sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care urmează să facă parte dintr-un sistem de evidență a datelor.

(3) Prezenta directivă nu se aplică prelucrării datelor cu caracter personal:

- (a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii;
- (b) de către instituțiile, organele, oficiile și agențiile Uniunii.

Articolul 3

Definiții

În sensul prezentei directive:

1. „date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.
2. „prelucrare” înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau 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, dezvoltarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;
3. „restricționarea prelucrării” înseamnă marcarea datelor cu caracter personal stocate, cu scopul de a limita prelucrarea viitoare a acestora;
4. „creare de profiluri” înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau a preconiza aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, localizarea sau deplasările respectivei persoane fizice;
5. „pseudonimizare” înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, în măsura în care aceste informații suplimentare sunt stocate separat și fac obiectul unor măsuri de natură tehnică și organizatorică destinate să garanteze neatribuirea unei persoane fizice identificate sau identificabile;
6. „sistem de evidență a datelor” înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;
7. „autoritate competentă” înseamnă:
 - (a) orice autoritate publică competentă în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor sau de executare a pedepselor, inclusiv în materie de protejare împotriva amenințărilor la adresa securității publice și de prevenire a acestora; sau
 - (b) orice alt organism sau entitate împuternicit(ă) de dreptul intern să exercite autoritate publică și competențe publice în scopul în prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora;

8. „operator” înseamnă autoritatea competentă care, singură sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele de prelucrare sunt stabilite prin dreptul Uniunii sau prin dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi stabilite prin dreptul Uniunii sau prin dreptul intern;
9. „persoană împuternicită de către operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
10. „destinatar” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau un alt organism căruia îi sunt transmise datele cu caracter personal, fie că aceasta este sau nu o parte terță; sunt exceptate, cu toate acestea, autoritățile publice care pot primi date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul intern, iar prelucrarea datelor cu caracter personal respective de către acestea respectă normele aplicabile în materie de protecție a datelor în conformitate cu scopurile prelucrării;
11. „încălcarea securității datelor cu caracter personal” înseamnă o încălcare a securității, care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod;
12. „date genetice” înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice care oferă informații unice privind fiziologia sau sănătatea respectivei persoane fizice, astfel cum rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la acea persoană fizică;
13. „date biometrice” înseamnă 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 fizice, cum ar fi imaginile faciale sau datele dactiloscopice;
14. „date privind sănătatea” înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv acordarea de servicii de asistență medicală, care dezvoltă informații despre starea de sănătate a acesteia;
15. „autoritate de supraveghere” înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 41;
16. „organizație internațională” înseamnă o organizație și organismele sale subordonate reglementate de dreptul internațional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe țări sau în temeiul unui astfel de acord.

CAPITOLUL II

Principii

Articolul 4

Principii referitoare la prelucrarea datelor cu caracter personal

- (1) Statele membre garantează că datele cu caracter personal:
 - (a) sunt prelucrate în mod legal și echitabil;
 - (b) sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate într-un mod incompatibil cu aceste scopuri;
 - (c) sunt adecvate, relevante și neexcesive în ceea ce privește scopurile în care sunt prelucrate;
 - (d) sunt exacte și, dacă este necesar, sunt actualizate; trebuie să se ia toate măsurile rezonabile pentru a asigura faptul că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, să fie șterse sau rectificate fără întârziere;
 - (e) sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor pentru care sunt prelucrate datele respective;
 - (f) sunt prelucrate într-un mod care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

- (2) Prelucrarea de către același operator sau de către un altul, în oricare dintre scopurile stabilite la articolul 1 alineatul (1), altele decât cele pentru care datele cu caracter personal au fost colectate, este permisă în măsura în care:
- (a) operatorul este autorizat să prelucreze astfel de date cu caracter personal în scopul respectiv, în conformitate cu dreptul Uniunii sau cu dreptul intern; și
 - (b) prelucrarea este necesară și proporțională în raport cu respectivul alt scop, în conformitate cu dreptul Uniunii sau cu dreptul intern.
- (3) Prelucrarea de către același operator sau de către un altul poate include arhivarea în interes public sau în scopuri științifice, statistice sau istorice pentru scopurile stabilite la articolul 1 alineatul (1), cu condiția unor garanții adecvate pentru drepturile și libertățile persoanelor vizate.
- (4) Operatorul este responsabil de respectarea alineatelor (1), (2) și (3) și poate demonstra acest lucru.

Articolul 5

Termene pentru stocare și revizuire

Statele membre garantează stabilirea unor termene corespunzătoare pentru ștergerea datelor cu caracter personal sau pentru o revizuire periodică a necesității de stocare a datelor cu caracter personal. Respectarea acestor termene este asigurată prin măsuri procedurale.

Articolul 6

Distincția între diferitele categorii de persoane vizate

Statele membre garantează că, după caz și în măsura posibilului, operatorul face distincție clară între datele cu caracter personal ale diferitelor categorii de persoane vizate, precum:

- (a) persoane în privința cărora există motive serioase să se creadă că au săvârșit sau că urmează să săvârșescă o infracțiune;
- (b) persoane condamnate pentru săvârșirea unei infracțiuni;
- (c) victime ale unei infracțiuni sau persoane în privința cărora, în baza anumitor fapte, există motive să se creadă că persoanele respective ar putea fi victimele unei infracțiuni; și
- (d) alte părți care au legătură cu infracțiunea, ca de exemplu persoane care ar putea fi chemate să depună mărturie în cadrul anchetelor legate de infracțiuni sau în cadrul procedurilor penale ulterioare sau persoane care pot oferi informații cu privire la infracțiuni sau persoane care sunt în legătură sau asociate cu persoanele menționate la literale (a) și (b).

Articolul 7

Distincția între datele cu caracter personal și verificarea calității datelor cu caracter personal

- (1) Statele membre garantează că se face distincție, pe cât posibil, între datele cu caracter personal bazate pe fapte și datele cu caracter personal bazate pe evaluări personale.
- (2) Statele membre garantează că autoritățile competente iau toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte, incomplete sau nu mai sunt actuale nu sunt transmise sau puse la dispoziție. În acest scop, fiecare autoritate competentă verifică, în măsura în care este posibil, calitatea datelor cu caracter personal înainte ca acestea să fie transmise sau puse la dispoziție. În măsura în care acest lucru este posibil, în cadrul tuturor transmișorilor de date cu caracter personal, se adaugă informații necesare care permit autorității competente destinate să evalueze gradul de exactitate, caracterul integral, gradul de fiabilitate și de actualitate al datelor cu caracter personal.
- (3) În cazul în care se constată transmiterea unor date cu caracter personal incorecte sau transmiterea unor date cu caracter personal în mod ilegal, acest lucru se comunică de îndată destinatarului. Într-un astfel de caz, datele cu caracter personal sunt rectificate sau șterse sau prelucrarea este restricționată în conformitate cu articolul 16.

*Articolul 8***Legalitatea prelucrării**

- (1) Statele membre garantează legalitatea prelucrării numai dacă și în măsura în care aceasta este necesară pentru îndeplinirea unei sarcini de către o autoritate competentă în scopurile stabilite la articolul 1 alineatul (1) și că aceasta se întemeiază pe dreptul Uniunii sau pe dreptul intern.
- (2) Dreptul intern care reglementează prelucrarea care intră sub incidența prezentei directive precizează cel puțin obiectivele prelucrării, datele cu caracter personal care urmează să fie prelucrate și scopurile prelucrării.

*Articolul 9***Condiții specifice de prelucrare**

- (1) Datele cu caracter personal colectate de autoritățile competente în scopurile stabilite la articolul 1 alineatul (1) nu se prelucrează în alte scopuri decât cele stabilite la articolul 1 alineatul (1), cu excepția cazurilor în care o astfel de prelucrare este autorizată în temeiul dreptului Uniunii sau al dreptului intern. În cazurile în care datele cu caracter personal sunt prelucrate în alte scopuri, prelucrării respective i se aplică Regulamentul (UE) 2016/679, cu excepția cazului în care prelucrarea este efectuată în cadrul unei activități care nu intră sub incidența dreptului Uniunii.
- (2) În cazul în care autoritățile competente sunt împuternicite prin dreptul intern să îndeplinească alte atribuții decât cele aferente scopurilor stabilite la articolul 1 alineatul (1), pentru prelucrarea în astfel de scopuri se aplică Regulamentul (UE) 2016/679, inclusiv în ce privește prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, cu excepția cazului în care prelucrarea este efectuată în cadrul unei activități care nu intră sub incidența dreptului Uniunii.
- (3) Statele membre garantează că, în cazul în care dreptul Uniunii sau dreptul intern aplicabil autorității competente care a transmis datele prevede condiții specifice de prelucrare, autoritatea competentă care a transmis datele informează destinatarul respectivelor date cu caracter personal cu privire la aceste condiții și la obligația de a le respecta.
- (4) Statele membre garantează că autoritatea competentă care a transmis datele nu aplică condițiile prevăzute la alineatul (3) destinatarilor din alte state membre sau agențiilor, oficiilor și organismelor instituite în conformitate cu titlul V capitolele 4 și 5 din TFUE, altele decât cele aplicabile transiterii similare de date în statul membru al autorității competente care a transmis datele.

*Articolul 10***Prelucrarea de categorii speciale de date cu caracter personal**

Prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, afilierea sindicală, prelucrarea datelor genetice, prelucrarea datelor biometrice pentru identificarea unică a unei persoane fizice sau prelucrarea datelor privind sănătatea sau a datelor privind viața sexuală și orientarea sexuală a unei persoane fizice este autorizată numai atunci când este strict necesară și sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei vizate și numai atunci când:

- (a) este autorizată de dreptul Uniunii sau de dreptul intern;
- (b) este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane fizice; sau
- (c) prelucrarea respectivă se referă la date care sunt făcute publice în mod manifest de persoana vizată.

*Articolul 11***Procesul decizional individual automatizat**

- (1) Statele membre garantează că o decizie întemeiată exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce un efect juridic negativ pentru persoana vizată sau care o afectează în mod semnificativ, este interzisă, cu excepția cazului în care este autorizată de dreptul Uniunii sau de dreptul intern care se aplică operatorului și care prevede garanții adecvate pentru drepturile și libertățile persoanei vizate, cel puțin dreptul de a obține intervenția umană din partea operatorului.

(2) Deciziile menționate la alineatul (1) din prezentul articol nu se întemeiază pe categoriile speciale de date cu caracter personal menționate la articolul 10, cu excepția cazului în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, a libertăților și a intereselor legitime ale persoanei vizate.

(3) În conformitate cu dreptul Uniunii, este interzisă crearea de profiluri care are drept rezultat discriminarea persoanelor fizice pe baza categoriilor speciale de date cu caracter personal menționate la articolul 10.

CAPITOLUL III

Drepturile persoanei vizate

Articolul 12

Comunicare și modalități de exercitare a drepturilor persoanei vizate

(1) Statele membre garantează faptul că operatorul ia măsuri rezonabile pentru a transmite persoanei vizate orice informații menționate la articolul 13 și transmite acesteia orice comunicare în legătură cu articolele 11, 14-18 și 31 referitoare la prelucrare, într-o formă concisă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Informațiile se transmit prin orice mijloace adecvate, inclusiv prin mijloace electronice. Ca regulă generală, operatorul transmite informațiile în același format în care a fost primită cererea.

(2) Statele membre garantează faptul că operatorul facilitează exercitarea drepturilor persoanei vizate în temeiul articolelor 11 și 14-18.

(3) Statele membre garantează faptul că operatorul informează în scris persoana vizată cu privire la modul în care a dat curs cererii acesteia, fără întârzieri nejustificate.

(4) Statele membre garantează faptul că transmiterea informațiilor în conformitate cu articolul 13 și orice comunicare transmisă și măsură luată în temeiul articolelor 11, 14-18 și 31 este gratuită. 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) să perceapă o taxă rezonabilă care să țină cont de costurile administrative pentru transmiterea informațiilor sau a comunicărilor sau pentru luarea măsurilor solicitate; sau
- (b) poate refuza să dea curs cererii.

Operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

(5) În cazul în care operatorul are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea menționată la articolul 14 sau 16, acesta poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

Articolul 13

Informații care se pun la dispoziția persoanei vizate sau se comunică acesteia

(1) Statele membre garantează că operatorul pune la dispoziția persoanelor vizate cel puțin următoarele informații:

- (a) identitatea și datele de contact ale operatorului;
- (b) datele de contact ale responsabilului cu protecția datelor, după caz;
- (c) scopurile în care sunt prelucrate datele cu caracter personal;
- (d) dreptul de a depune o plângere în fața autorității de supraveghere și datele de contact ale autorității de supraveghere;
- (e) existența dreptului de a solicita operatorului acces la datele cu caracter personal referitoare la persoana vizată ori rectificarea sau ștergerea acestor date sau restricționarea prelucrării lor.

(2) În plus față de informațiile menționate la alineatul (1), statele membre garantează prin lege că operatorul comunică persoanei vizate, în anumite cazuri, următoarele informații suplimentare, pentru a permite acesteia exercitarea drepturilor sale:

- (a) temeiul juridic al prelucrării;
- (b) perioada pentru care vor fi stocate datele cu caracter personal sau, în cazul în care nu este posibil, criteriile utilizate pentru a stabili respectiva perioadă;

- (c) dacă este cazul, categoriile de destinatari ai datelor cu caracter personal, inclusiv în țări terțe sau organizații internaționale;
- (d) în cazul în care este necesar, informații suplimentare, în special atunci când datele cu caracter personal sunt colectate fără știrea persoanei vizate.
- (3) Statele membre pot adopta măsuri legislative de amânare, restricționare sau omitere a furnizării de informații persoanei vizate în conformitate cu alineatul (2) în măsura în care și atât timp cât o astfel de măsură constituie o măsură necesară și proporțională într-o societate democratică, ținând seama de drepturile fundamentale și de interesele legitime ale persoanei fizice, pentru:
- (a) evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau juridice;
- (b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;
- (c) protejarea securității publice;
- (d) protejarea securității naționale;
- (e) protejarea drepturilor și libertăților celorlalți.
- (4) Statele membre pot adopta măsuri legislative pentru a stabili categoriile de prelucrare care pot intra, integral sau parțial, sub incidența oricăreia dintre literele de la alineatul (3).

Articolul 14

Dreptul de acces al persoanei vizate

Sub rezerva articolului 15, statele membre garantează dreptul persoanei vizate de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații:

- (a) scopurile și temeiul juridic al prelucrării;
- (b) categoriile de date cu caracter personal vizate;
- (c) destinatarii sau categoriile de destinatari cărora le-au fost divulgate datele cu caracter personal, în special destinatarii din țări terțe sau organizații internaționale;
- (d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, în cazul în care acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- (e) existența dreptului de a solicita de la operator rectificarea sau ștergerea datelor cu caracter personal, sau restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată;
- (f) dreptul de a depune o plângere în fața autorității de supraveghere și datele de contact ale autorității de supraveghere;
- (g) comunicarea datelor cu caracter personal care sunt în curs de prelucrare și a oricărei informații disponibile cu privire la originea datelor.

Articolul 15

Limitarea dreptului de acces

(1) Statele membre pot adopta măsuri legislative care limitează, integral sau parțial, dreptul de acces al persoanei vizate în măsura și atât timp o astfel de limitare, parțială sau totală, constituie o măsură necesară și proporțională într-o societate democratică, ținându-se seama de drepturile fundamentale și de interesele legitime ale respectivei persoane fizice, pentru:

- (a) evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau juridice;
- (b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;
- (c) protejarea securității publice;

- (d) protejarea securității naționale;
 - (e) protejarea drepturilor și libertăților celorlalți.
- (2) Statele membre pot adopta măsuri legislative pentru a stabili categoriile de prelucrare care se pot intra, integral sau parțial, sub incidența literelor (a)-(e) de la alineatul (1).
- (3) În cazurile prevăzute la alineatele (1) și (2), statele membre garantează că operatorul informează în scris persoana vizată, fără întârzieri nejustificate, cu privire la refuzarea sau limitarea accesului și la motivele refuzului sau ale limitării. Astfel de informații pot fi omise atunci când furnizarea lor ar contraveni unuia dintre scopurile de la alineatul (1). Statele membre garantează că operatorul informează persoana vizată cu privire la posibilitatea de a depune o plângere la autoritatea de supraveghere sau de a introduce o cale de atac judiciară.
- (4) Statele membre garantează că operatorul justifică motivele de fapt și de drept pe care se întemeiază decizia. Aceste informații se pun la dispoziția autorităților de supraveghere.

Articolul 16

Dreptul la rectificarea sau la ștergerea datelor cu caracter personal și la restricționarea prelucrării

- (1) Statele membre garantează persoanei vizate dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile prelucrării, statele membre garantează persoanei vizate dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.
- (2) Statele membre impun operatorului obligația de a șterge datele cu caracter personal fără întârzieri nejustificate și garantează persoanei vizate dreptul de a obține de la operator ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, în cazul în care prelucrarea încalcă dispozițiile adoptate în temeiul articolului 4, 8 sau 10, sau în cazul în care datele cu caracter personal trebuie șterse pentru îndeplinirea unei obligații legale care îi revine operatorului.
- (3) În loc de ștergere, operatorul restricționează prelucrarea datelor cu caracter personal în cazul în care:
- (a) exactitatea datelor cu caracter personal este contestată de persoana vizată, iar exactitatea sau inexactitatea datelor respective nu poate fi stabilită cu certitudine; sau
 - (b) datele cu caracter personal trebuie să fie păstrate ca mijloace de probă.

În cazul în care prelucrarea este restricționată în conformitate cu litera (a) de la primul paragraf, operatorul informează în acest sens persoana vizată înainte de ridicarea restricțiilor de prelucrare.

- (4) Statele garantează că operatorul informează în scris persoana vizată cu privire la orice refuz de rectificare sau de ștergere a datelor cu caracter personal sau de restricționare a prelucrării și cu privire la motivele refuzului. Statele membre pot adopta măsuri legislative care restricționează, integral sau parțial, obligația de a furniza astfel de informații în măsura în care o astfel de restricționare a prelucrării constituie o măsură necesară și proporțională într-o societate democratică, ținându-se seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice vizate pentru:
- (a) a evita obstrucționarea cercetărilor, anchetelor sau procedurilor oficiale sau juridice;
 - (b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;
 - (c) a proteja securitatea publică;
 - (d) a proteja securitatea națională;
 - (e) a proteja drepturile și libertățile celorlalți.

Statele membre garantează că operatorul informează persoana vizată cu privire la posibilitatea de a depune o plângere la autoritatea de supraveghere sau de a introduce o cale de atac judiciară.

(5) Statele membre garantează comunicarea de către operator a rectificării datelor cu caracter personal inexacte autorității competente de la care provin datele cu caracter personal inexacte.

(6) Statele membre garantează faptul că operatorul informează destinatarul cu privire la rectificarea sau ștergerea datelor cu caracter personal sau cu privire la restricționarea prelucrării, în temeiul alineatelor (1), (2) și (3), precum și faptul că destinatarul rectifică sau șterge datele cu caracter personal sau restricționează prelucrarea datelor cu caracter personal atunci când le revine responsabilitatea pentru acestea.

Articolul 17

Exercitarea drepturilor de către persoana vizată și verificarea de către autoritatea de supraveghere

(1) În cazurile menționate la articolul 13 alineatul (3), la articolul 15 alineatul (3) și la articolul 16 alineatul (4), statele membre adoptă măsuri prin care se prevede că drepturile persoanei vizate pot fi, de asemenea, exercitate prin intermediul autorității de supraveghere competente.

(2) Statele membre garantează că operatorul informează persoana vizată cu privire la posibilitatea de a-și exercita drepturile prin intermediul autorității de supraveghere în temeiul alineatului (1).

(3) Atunci când este exercitat dreptul menționat la alineatul (1), autoritatea de supraveghere informează persoana vizată cel puțin că au fost realizate toate verificările necesare sau o revizuire de către autoritatea de supraveghere. Autoritatea de supraveghere informează, de asemenea, persoana vizată în legătură cu dreptul acesteia de a introduce o cale de atac.

Articolul 18

Drepturile persoanei vizate în cadrul investigațiilor și procedurilor penale

Statele membre garantează că drepturile menționate la articolele 13, 14 și 16 se exercită în conformitate cu dreptul intern în cazul în care datele cu caracter personal sunt conținute într-o hotărâre judecătorească sau într-un cazier sau dosar prelucrat pe parcursul investigațiilor și procedurilor penale.

CAPITOLUL IV

Operatorul și persoana împuternicită de către operator

Secțiunea 1

Obligații generale

Articolul 19

Obligațiile operatorului

(1) Statele membre garantează că, ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate la adresa drepturilor și libertăților persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezenta directivă. Respectivile măsuri se revizuiesc și se actualizează dacă este necesar.

(2) Atunci când sunt proporționale în raport cu operațiunile de prelucrare, măsurile menționate la alineatul (1) includ punerea în aplicare de către operator a unor politici corespunzătoare de protecție a datelor.

Articolul 20

Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

(1) Statele membre garantează că, având în vedere stadiul actual al tehnologiei, costurile de punere în aplicare, precum și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și de gravitate la adresa drepturilor și libertăților persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât la momentul stabilirii mijloacelor de prelucrare, cât și la cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minim a datelor și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentei directive și a proteja drepturile persoanelor vizate.

(2) Statele membre garantează că operatorul pune în aplicare măsuri tehnice și organizatorice adecvate prin care să se asigure că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Obligația respectivă se aplică volumului de date cu caracter personal colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, măsurile respective trebuie să asigure că, în mod implicit, datele cu caracter personal nu sunt accesibile, fără intervenția persoanei fizice, unui număr nedefinit de persoane fizice.

Articolul 21

Operatori asociați

(1) Statele membre garantează faptul că, atunci când doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați. Aceștia stabilesc într-un mod transparent responsabilitățile care revin fiecăruia în vederea respectării prezentei directive, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute la articolul 13, prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite de dreptul Uniunii sau de dreptul intern care li se aplică. Acordul desemnează punctul de contact pentru persoanele vizate. Statele membre pot desemna care dintre operatorii asociați poate acționa ca punct unic de contact pentru exercitarea de către persoanele vizate a drepturilor lor.

(2) Indiferent de termenii acordului menționat la alineatul (1), statele membre pot să prevadă dispoziții potrivit cărora persoana vizată își exercită drepturile cu privire la și în raport cu fiecare dintre operatori în conformitate cu dispozițiile adoptate în temeiul prezentei directive.

Articolul 22

Persoana împuternicită de către operator

(1) Statele membre garantează că, atunci când o prelucrare urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane împuternicite care să ofere garanții suficiente pentru punerea în aplicare a măsurilor tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentei directive și să asigure protecția drepturilor persoanei vizate.

(2) Statele membre garantează că persoana împuternicită de către operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații scrise generale, persoana împuternicită de către operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de către operator, oferind astfel operatorului posibilitatea de a formula obiecții față de aceste modificări.

(3) Statele membre garantează că prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau un alt act juridic în temeiul dreptului Uniunii sau al dreptului intern, care are caracter obligatoriu pentru persoana împuternicită de către operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate, precum și obligațiile și drepturile operatorului. Respectivul contract sau act juridic prevede, în special, că persoana împuternicită de operator:

- (a) acționează numai la instrucțiunile operatorului;
- (b) garantează faptul că persoanele autorizate să prelucreze date cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație legală de confidențialitate corespunzătoare;
- (c) asistă operatorul prin orice mijloace adecvate pentru a asigura respectarea dispozițiilor privind drepturile persoanei vizate;
- (d) la alegerea operatorului, șterge sau returnează toate datele cu caracter personal operatorului după încetarea furnizării serviciilor de prelucrare a datelor și elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede stocarea datelor cu caracter personal;

- (e) pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea prezentului articol;
 - (f) respectă condițiile menționate la alineatele (2) și (3) pentru recrutarea unei alte persoane împuternicite de către operator.
- (4) Contractul sau un alt act juridic menționat la alineatul (3) se întocmește în scris și poate fi pus la dispoziție în format electronic.
- (5) În cazul în care o persoană împuternicită de către operator stabilește, cu încălcarea prezentei directive, scopurile și mijloacele de prelucrare, persoana împuternicită este considerată ca fiind operator în ceea ce privește prelucrarea respectivă.

Articolul 23

Desfășurarea activității de prelucrare sub autoritatea operatorului sau a persoanei împuternicite de către operator

Statele membre garantează că persoana împuternicită de către operator și orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de către operator care are acces la datele cu caracter personal prelucrează datele respective numai la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern impun aceasta.

Articolul 24

Evidențe ale activităților de prelucrare

- (1) Statele membre garantează că operatorul menține o evidență a tuturor categoriilor de activități de prelucrare aflate în responsabilitatea sa. Respectiva evidență cuprinde toate informațiile următoare:
- (a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat și ale responsabilului cu protecția datelor;
 - (b) scopurile prelucrării;
 - (c) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
 - (d) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
 - (e) acolo unde este cazul, utilizarea creării de profiluri;
 - (f) acolo unde este cazul, categoriile de transferuri de date cu caracter personal către o țară terță sau o organizație internațională;
 - (g) indicarea temeiului juridic al operațiunii de prelucrare, inclusiv transferurile, pentru care sunt destinate datele cu caracter personal;
 - (h) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date cu caracter personal;
 - (i) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 29 alineatul (1).
- (2) Statele membre garantează că fiecare persoană împuternicită de către operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, evidență care cuprinde:
- (a) numele și datele de contact ale persoanei sau persoanelor împuternicite de către operator, ale fiecărui operator în numele căruia acționează această persoană și, după caz, cele ale responsabilului cu protecția datelor;
 - (b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;
 - (c) acolo unde este cazul, transferurile de date cu caracter personal către o țară terță sau către o organizație internațională, inclusiv, identificarea țării terțe sau a organizației internaționale respective, atunci când au primit instrucțiuni explicite în acest sens de la operator;
 - (d) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 29 alineatul (1).

(3) Evidențele menționate la alineatele (1) și (2) se păstrează în scris, inclusiv în format electronic.

Operatorul și persoana împuternicită de acesta pun evidențele la dispoziția autorității de supraveghere, la cererea acesteia.

Articolul 25

Înregistrarea

(1) Statele membre se asigură că se înregistrează cel puțin următoarele operațiuni de prelucrare din cadrul sistemelor de prelucrare automată: colectarea, modificarea, consultarea, divulgarea inclusiv transferurile, combinarea și ștergerea. Înregistrările consultărilor și ale divulgărilor fac posibilă determinarea motivelor, a datei și a momentului acestor operațiuni și, în măsura în care este posibil, identificarea persoanei care a consultat sau a divulgat date cu caracter personal și identitatea destinatarilor acestor date cu caracter personal.

(2) Înregistrările sunt utilizate numai pentru verificarea legalității prelucrării, monitorizare proprie, asigurarea integrității și a securității datelor cu caracter personal și în cadrul unor proceduri penale.

(3) Operatorul și persoana împuternicită de către operator pun înregistrările la dispoziția autorității de supraveghere, la cererea acesteia.

Articolul 26

Cooperarea cu autoritatea de supraveghere

Statele membre garantează că operatorul și persoana împuternicită de către operator cooperează cu autoritatea de supraveghere, la cererea acesteia, în îndeplinirea sarcinilor acesteia.

Articolul 27

Evaluarea impactului asupra protecției datelor

(1) În cazul în care un tip de prelucrare, în special care implică utilizarea de noi tehnologii, și, ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, este susceptibil să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, statele membre garantează că operatorul, înainte de prelucrare, efectuează o evaluare a impactului operațiunilor de prelucrare preconizate asupra protecției datelor cu caracter personal.

(2) Evaluarea menționată la alineatul (1) cuprinde cel puțin o descriere generală a operațiunilor de prelucrare preconizate, o evaluare a riscurilor la adresa drepturilor și libertăților persoanelor vizate, măsurile preconizate în vederea abordării riscurilor, garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze respectarea prezentei directive, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale celorlalte persoane interesate.

Articolul 28

Consultarea prealabilă a autorității de supraveghere

(1) Statele membre garantează că operatorul sau persoana împuternicită de către operator consultă autoritatea de supraveghere înainte de prelucrarea datelor cu caracter personal care fac parte dintr-un sistem nou de evidență a datelor care urmează a fi creat, în cazul în care:

- (a) o evaluare a impactului asupra protecției datelor, prevăzută la articolul 27, indică faptul că prelucrarea ar genera un risc ridicat în absența măsurilor luate de operator pentru atenuarea riscului sau
- (b) un tip de prelucrare, în special în cazul în care se utilizează noi tehnologii, mecanisme sau proceduri, implică un risc ridicat la adresa drepturilor și libertăților persoanelor vizate.

(2) Statele membre garantează că autoritatea de supraveghere este consultată în cadrul procesului de pregătire a unei propuneri de măsură legislativă care să fie adoptată de un parlament național sau a unei măsuri de reglementare întemeiate pe o astfel de măsură legislativă, care se referă la prelucrare.

(3) Statele membre garantează că autoritatea de supraveghere poate stabili o listă a operațiunilor de prelucrare care fac obiectul consultării prealabile, în conformitate cu alineatul (1).

(4) Statele membre garantează că operatorul transmite autorității de supraveghere evaluarea impactului asupra protecției datelor în temeiul articolului 27 și, la cererea acesteia, orice altă informație care permite autorității de supraveghere să evalueze conformitatea prelucrării și în special riscurile la adresa protecției datelor cu caracter personal ale persoanei vizate și garanțiile aferente.

(5) Statele membre garantează că atunci când autoritatea de supraveghere consideră că prelucrarea preconizată, menționată la alineatul (1) din prezentul articol, ar încălca dispozițiile adoptate în temeiul prezentei directive, în special în cazul în care riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris operatorului, în termen de cel mult șase săptămâni de la primirea cererii de consultare, și, dacă este cazul, persoanei împuternicite de către operator, și își poate recurge la oricare dintre competențele menționate la articolul 47. Termenul menționat poate fi prelungit cu o lună, ținându-se seama de complexitatea prelucrării preconizate. Autoritatea de supraveghere informează operatorul și, dacă este cazul, persoana împuternicită de către operator, cu privire la prelungirea termenului respectiv, inclusiv cu privire la motivele prelungirii, în termen de o lună de la primirea cererii de consultare.

Secțiunea 2

Securitatea datelor cu caracter personal

Articolul 29

Securitatea prelucrării

(1) Statele membre garantează că, având în vedere stadiul actual al tehnologiei și costurile implementării și ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și de gravitate la adresa drepturilor și libertăților persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, în special în ceea ce privește prelucrarea categoriilor speciale de date cu caracter personal menționate la articolul 10.

(2) În ceea ce privește prelucrarea automată, fiecare stat membru garantează că operatorul sau persoana împuternicită de către operator pune în aplicare, în urma unei evaluări a riscurilor, măsuri menite:

- (a) să împiedice accesul persoanelor neautorizate la echipamentele de prelucrare utilizate pentru prelucrare („controlul accesului la echipamente”);
- (b) să împiedice orice citire, copiere, modificare sau eliminare neautorizată a suporturilor de date („controlul suporturilor de date”);
- (c) să împiedice introducerea neautorizată de date cu caracter personal și inspectarea, modificarea sau ștergerea neautorizată a datelor cu caracter personal stocate („controlul stocării”);
- (d) să împiedice utilizarea sistemelor de prelucrare automată de către persoane neautorizate cu ajutorul echipamentelor de comunicare a datelor („controlul utilizatorului”);
- (e) să asigure faptul că persoanele autorizate să utilizeze un sistem de prelucrare automată au acces numai la datele cu caracter personal pentru care au autorizare („controlul accesului la date”);
- (f) să asigure că este posibilă verificarea și identificarea organismelor cărora le-au fost transmise sau puse la dispoziție sau s-ar putea să le fie transmise sau puse la dispoziție date cu caracter personal utilizându-se echipamente de comunicare a datelor („controlul comunicării”);
- (g) să asigure că este posibil ulterior să se verifice și să se identifice datele cu caracter personal introduse în sistemele de prelucrare automată, momentul introducerii datelor cu caracter personal și entitatea care le-a introdus („controlul introducerii datelor”);
- (h) să împiedice citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transferurilor de date cu caracter personal sau în timpul transportării suporturilor de date („controlul transportării”);
- (i) să asigure posibilitatea recuperării sistemelor instalate în cazul unei întreruperi („recuperarea”);
- (j) să asigure funcționarea sistemului, raportarea defecțiunilor de funcționare (fiabilitate) și imposibilitatea coruperii datelor cu caracter personal stocate din cauza funcționării defectuoase a sistemului („integritate”).

Articolul 30

Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal

- (1) Statele membre garantează că, în cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere fără întârzieri nejustificate și, în cazul în care este posibil, în cel mult 72 de ore după ce a luat cunoștință de aceasta, cu excepția cazului în care încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc la adresa drepturilor și libertăților persoanelor fizice. În cazul notificării se efectuează în termen de 72 de ore, aceasta va fi însoțită de o justificare a întârzierii.
- (2) Persoana împuternicită de către operator înștiințează operatorul fără întârzieri nejustificate după ce ia cunoștință de o încălcare a securității datelor cu caracter personal.
- (3) Notificarea menționată la alineatul (1) trebuie, cel puțin:
- (a) să descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ de persoane vizate în cauză, precum și categoriile și numărul aproximativ de înregistrări de date cu caracter personal în cauză;
 - (b) să comunice numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
 - (c) să descrie consecințele probabile ale încălcării securității datelor cu caracter personal;
 - (d) să descrie măsurile luate sau propuse de operator pentru a remedia încălcarea securității datelor cu caracter personal, inclusiv, dacă este cazul, măsuri pentru a atenua eventualele efecte adverse ale acesteia.
- (4) În cazul în care și în măsura în care furnizarea informațiilor în același timp nu este posibilă, informațiile pot fi furnizate treptat, fără întârzieri nejustificate.
- (5) Statele membre garantează că operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, menționate la alineatul (1), care cuprind o descriere a situației în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație trebuie să permită autorității de supraveghere să verifice respectarea prezentului articol.
- (6) Statele membre garantează că, în cazul în care încălcarea securității datelor implică date cu caracter personal care au fost transmise de un operator dintr-un alt stat membru sau către un astfel de operator, informațiile prevăzute la alineatul (3) se comunică operatorului din respectivul stat membru fără întârzieri nejustificate.

Articolul 31

Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal

- (1) Statele membre garantează că, în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, operatorul informează persoana vizată, fără întârzieri nejustificate, cu privire la încălcarea securității datelor cu caracter personal.
- (2) În informarea transmisă persoanei vizate, prevăzută la alineatul (1) din prezentul articol, se include o descriere într-un limbaj simplu și clar a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile și măsurile menționate la articolul 30 alineatul (3) literele (b), (c) și (d).
- (3) Informarea persoanei vizate, menționată la alineatul (1), nu este necesară în cazul în care este îndeplinită oricare dintre următoarele condiții:
- (a) operatorul a pus în aplicare măsuri tehnologice și organizatorice adecvate de protecție, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;
 - (b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat la adresa drepturilor și libertăților persoanelor vizate menționat la alineatul (1) nu mai este susceptibil să se materializeze;
 - (c) aceasta ar necesita un efort disproporționat. În acest caz, informarea se înlocuiește printr-o informare publică sau o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

(4) În cazul în care operatorul nu a informat deja persoana vizată cu privire la încălcarea securității datelor cu caracter personal, autoritatea de supraveghere, luând în considerare probabilitatea ca încălcarea securității datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite să facă acest lucru sau poate decide că oricare dintre condițiile menționate la alineatul (3) sunt îndeplinite.

(5) Informarea persoanei vizate menționată la alineatul (1) din prezentul articol poate fi amânată, restricționată sau omisă, sub rezerva condițiilor și a motivelor menționate la articolul 13 alineatul (3).

Secțiunea 3

Responsabilul cu protecția datelor

Articolul 32

De desemnarea responsabilului cu protecția datelor

(1) Statele membre garantează că operatorul desemnează un responsabil cu protecția datelor. Statele membre pot scuti de această obligație instanțele și alte autorități judiciare independente atunci când acționează în exercițiul funcțiilor lor judiciare.

(2) Responsabilul cu protecția datelor este desemnat pe baza calităților sale profesionale și, în special, a cunoștințelor de specialitate în domeniul legislației și practicilor privind protecția datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la articolul 34.

(3) Un unic responsabil cu protecția datelor poate fi desemnat pentru mai multe autorități competente, luând în considerare structura organizatorică și dimensiunea acestora.

(4) Statele membre garantează că operatorul publică datele de contact ale responsabilului cu protecția datelor și le transmite autorității de supraveghere.

Articolul 33

Funcția responsabilului cu protecția datelor

(1) Statele membre impun operatorului să se asigure că responsabilul cu protecția datelor este consultat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal.

(2) Operatorul sprijină responsabilul cu protecția datelor în îndeplinirea sarcinilor menționate la articolul 34, asigurându-i resursele necesare pentru executarea acestor sarcini, precum și accesul la datele cu caracter personal și la operațiunile de prelucrare, și să își mențină cunoștințele de specialitate.

Articolul 34

Sarcinile responsabilului cu protecția datelor

Statele membre garantează că operatorul încredințează responsabilului cu protecția datelor cel puțin următoarele sarcini:

- (a) informarea și consilierea operatorului și a angajaților care efectuează prelucrarea cu privire la obligațiile care le revin în temeiul prezentei directive și al altor dispoziții de drept al Uniunii sau de drept intern privind protecția datelor;
- (b) monitorizarea respectării prezentei directive, a altor dispoziții de drept al Uniunii sau de drept intern privind protecția datelor și a politicilor operatorului în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
- (c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu articolul 27;
- (d) cooperarea cu autoritatea de supraveghere;
- (e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 28, precum și, dacă este cazul, acordarea consultanței cu privire la orice altă chestiune.

CAPITOLUL V

Transferurile de date cu caracter personal către țări terțe sau organizații internaționale

Articolul 35

Principii generale pentru transferurile de date cu caracter personal

- (1) Statele membre garantează că orice transfer de date cu caracter personal de către autoritățile competente, care sunt în curs de prelucrare sau care sunt destinate prelucrării după transferul către o țară terță sau către o organizație internațională, inclusiv transferurilor ulterioare către o altă țară terță sau organizație internațională, poate avea loc numai sub rezerva respectării altor dispoziții ale prezentei directive, în cazul în care sunt îndeplinite condițiile prevăzute în prezentul capitol, și anume:
- (a) transferul este necesar în scopurile stabilite la articolul 1 alineatul (1);
 - (b) datele cu caracter personal sunt transferate unui operator într-o țară terță sau unei organizații internaționale care este o autoritate competentă în sensul articolului 1 alineatul (1);
 - (c) în cazul în care datele cu caracter personal sunt transmise sau puse la dispoziție din alt stat membru, acel stat membru a autorizat în prealabil efectuarea transferului, în conformitate cu dreptul său intern;
 - (d) Comisia a adoptat o decizie privind caracterul adecvat al nivelului de protecție, în temeiul articolului 36, sau, în absența unei astfel de decizii, există sau se oferă garanții adecvate în temeiul articolului 37 sau, în absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 36 sau a unor garanții adecvate în conformitate cu articolul 37, se aplică derogări pentru situații speciale în conformitate cu articolul 38; și
 - (e) în cazul unui transfer ulterior către o altă țară terță sau organizație internațională, autoritatea competentă care a realizat transferul inițial sau o altă autoritate competentă din același stat membru autorizează transferul ulterior, ținând seama în mod corespunzător de toți factorii relevanți, inclusiv de gravitatea infracțiunii, de scopul în care datele cu caracter personal au fost transferate inițial și de nivelul de protecție a datelor cu caracter personal din țara terță sau din organizația internațională către care sunt transferate ulterior datele cu caracter personal.
- (2) Statele membre garantează că transferurile fără autorizarea prealabilă de către un alt stat membru, în conformitate cu litera (c) de la alineatul (1), sunt permise numai dacă transferul de date cu caracter personal este necesar pentru prevenirea unei amenințări imediate și grave la adresa securității publice a unui stat membru sau a unei țări terțe sau a intereselor fundamentale ale unui stat membru, iar autorizarea prealabilă nu poate fi obținută în timp util. Autoritatea responsabilă pentru acordarea unei autorizări prealabile este informată fără întârziere.
- (3) Toate dispozițiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice garantat prin prezenta directivă nu este subminat.

Articolul 36

Transferuri în baza unei decizii privind caracterul adecvat al nivelului de protecție

- (1) Statele membre garantează că transferul de date cu caracter personal către o țară terță sau o organizație internațională se poate realiza atunci când Comisia a decis că țara terță, un teritoriu ori unul sau mai multe sectoare determinate din acea țară terță sau organizația internațională în cauză asigură un nivel de protecție adecvat. Transferurile realizate în aceste condiții nu necesită autorizări speciale.
- (2) Atunci când evaluează caracterul adecvat al nivelului de protecție, Comisia ține seama, în special, de următoarele elemente:
- (a) statul de drept, respectarea drepturilor omului și a libertăților fundamentale, legislația relevantă, atât generală, cât și sectorială, inclusiv privind securitatea publică, apărarea, securitatea națională și dreptul penal și accesul autorităților publice la datele cu caracter personal, precum și punerea în aplicare a acestei legislații, a normelor de protecție a datelor, a normelor profesionale și a măsurilor de securitate, inclusiv a normelor privind transferul ulterior de date cu caracter personal către o altă țară terță sau organizație internațională, care sunt respectate în țara respectivă sau de organizația internațională respectivă, jurisprudența, precum și drepturile efective și opozabile ale persoanelor vizate și reparații efective pe cale administrativă și judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate;
 - (b) existența și funcționarea efectivă a uneia sau a mai multor autorități de supraveghere independente în țara terță sau sub incidența cărora intră o organizație internațională, cu responsabilitate pentru asigurarea și impunerea respectării normelor de protecție a datelor, incluzând competențe adecvate de sancționare, pentru acordarea de asistență și consiliere persoanelor vizate cu privire la exercitarea drepturilor acestora și pentru cooperarea cu autoritățile de supraveghere din statele membre; și

(c) angajamentele internaționale la care a aderat țara terță sau organizația internațională în cauză sau alte obligații care decurg din convenții sau instrumente cu caracter juridic obligatoriu, precum și participarea acestora la sisteme multilaterale sau regionale, mai ales în domeniul protecției datelor cu caracter personal.

(3) Comisia, după ce evaluează caracterul adecvat al nivelului de protecție, poate decide, prin intermediul unui act de punere în aplicare, că o țară terță, un teritoriu sau unul sau mai multe sectoare determinate dintr-o țară terță sau o organizație internațională asigură un nivel de protecție adecvat în sensul alineatului (2) din prezentul articol. Actul de punere în aplicare prevede un mecanism de revizuire periodică, cel puțin o dată la patru ani, care ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională. Actul de punere în aplicare menționează aplicarea sa teritorială și sectorială și, după caz, identifică autoritatea sau autoritățile de supraveghere menționate la alineatul (2) litera (b) din prezentul articol. Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 58 alineatul (2).

(4) Comisia monitorizează în permanență evoluțiile din țările terțe și organizațiile internaționale care ar putea afecta funcționarea deciziilor adoptate în conformitate cu alineatul (3).

(5) În cazul în care din informațiile disponibile, în special în urma revizuirii menționate la alineatul (3) din prezentul articol, reiese că o țară terță, un teritoriu sau un sector determinat dintr-o țară terță sau o organizație internațională nu mai asigură un nivel de protecție adecvat în sensul alineatului (2) din prezentul articol, Comisia, în măsura în care este necesar, abrogă, modifică sau suspendă, prin intermediul unor acte de punere în aplicare, decizia menționată la alineatul (3) din prezentul articol fără efect retroactiv. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 58 alineatul (2).

Din motive imperioase de urgență justificate corespunzător, Comisia adoptă acte de punere în aplicare imediat aplicabile în conformitate cu procedura menționată la articolul 58 alineatul (3).

(6) Comisia inițiază consultări cu țara terță sau organizația internațională în vederea remedierii situației care a stat la baza deciziei luate în conformitate cu alineatul (5).

(7) Statele membre garantează că o decizie luată în temeiul alineatului (5) nu aduce atingere transferurilor de date cu caracter personal către țara terță, către teritoriul sau către unul sau mai multe sectoare determinate din cea țară terță sau către organizația internațională în cauză în conformitate cu articolele 37 și 38.

(8) Comisia publică în *Jurnalul Oficial al Uniunii Europene* și pe site-ul său web o listă a țărilor terțe, a teritoriilor și sectoarelor determinate din țările terțe și a organizațiilor internaționale în cazul cărora a decis că nivelul de protecție adecvat este asigurat sau nu mai este asigurat.

Articolul 37

Transferuri sub rezerva unor garanții adecvate

(1) În absența unei decizii luate în conformitate cu articolul 36 alineatul (3), statele membre garantează că transferul de date cu caracter personal către o țară terță sau către o organizație internațională poate avea loc atunci când:

- (a) s-au prezentat garanții adecvate în ceea ce privește protecția datelor cu caracter personal printr-un act cu caracter juridic obligatoriu; sau
- (b) operatorul a evaluat toate circumstanțele aferente transferului de date cu caracter personal și a concluzionat că există garanții adecvate în ceea ce privește protecția datelor cu caracter personal.

(2) Operatorul informează autoritatea de supraveghere cu privire la categoriile de transferuri în temeiul alineatului (1) litera (b).

(3) Atunci când un transfer se întemeiază pe alineatul (1) litera (b), un astfel de transfer se documentează, iar documentația se pune la dispoziția autorității de supraveghere la cerere, incluzând data și ora transferului, informații cu privire la autoritatea competentă destinatară, justificarea transferului și datele cu caracter personal transferate.

Articolul 38

Derogări pentru situații specifice

(1) În absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 37 sau a unor garanții adecvate în conformitate cu articolul 36, statele membre garantează că un transfer sau o categorie de transferuri de date cu caracter personal către o țară terță sau către o organizație internațională poate avea loc numai în condițiile în care transferul este necesar:

- (a) pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane;
- (b) pentru protejarea intereselor legitime ale persoanei vizate, în cazul în care dreptul statului membru care transferă datele cu caracter personal prevede acest lucru;
- (c) pentru prevenirea unei amenințări imediate și grave la adresa securității publice a unui stat membru sau a unei țări terțe;
- (d) în cazuri individuale în scopurile stabilite la articolul 1 alineatul (1); sau
- (e) într-un caz individual pentru constatarea, exercitarea sau apărarea unui drept în instanță privind scopurile stabilite la articolul 1 alineatul (1).

(2) Datele cu caracter personal nu sunt transferate dacă autoritatea competentă care transferă datele stabilește că drepturile și libertățile fundamentale ale persoanei vizate în cauză prevalează asupra interesului public în cazul transferului prevăzut la alineatul (1) literele (d) și (e).

(3) Atunci când un transfer se întemeiază pe alineatul (1), un astfel de transfer trebuie să fie documentat, iar documentația trebuie pusă la dispoziția autorității de supraveghere la cerere, incluzând data și ora transferului, informații cu privire la autoritatea competentă destinatară, justificarea transferului și datele cu caracter personal transferate.

Articolul 39

Transferurile de date cu caracter personal către destinatari stabiliți în țări terțe

(1) Prin derogare de la articolul 35 alineatul (1) litera (b) și fără a aduce atingere niciunui acord internațional menționat la alineatul (2) din prezentul articol, dreptul Uniunii sau dreptul intern poate să prevadă că autoritățile competente menționate la articolul 3 punctul 7 litera (a) pot, în cazuri individuale și specifice, transfera date cu caracter personal direct destinatarilor stabiliți în țări terțe, dar numai în cazul în care celelalte dispoziții ale prezentei directive sunt respectate și dacă sunt îndeplinite următoarele condiții:

- (a) transferul este strict necesar pentru executarea unei sarcini de către autoritatea competentă care transferă datele, astfel cum este prevăzut de dreptul Uniunii sau de dreptul intern în scopurile prevăzute la articolul 1 alineatul (1);
- (b) autoritatea competentă care transferă datele stabilește că niciunul dintre drepturile și libertățile fundamentale ale persoanei vizate în cauză nu prevalează în fața interesului public care necesită transferul în cazul respectiv;
- (c) autoritatea competentă care transferă datele consideră că transferul către o autoritate din țara terță, care este competentă în scopurile menționate la articolul 1 alineatul (1), este ineficient sau necorespunzător, în special din cauză că transferul nu poate fi realizat în timp util;
- (d) autoritatea din țara terță, care este competentă în scopurile menționate la articolul 1 alineatul (1), este informată fără întârzieri nejustificate, cu excepția cazului în care această măsură este ineficientă sau necorespunzătoare; și
- (e) autoritatea competentă care transferă datele informează destinatarul cu privire la scopul sau scopurile determinate exclusive în care aceasta din urmă poate să prelucreze datele cu caracter personal, cu condiția ca o astfel de prelucrare să fie necesară.

(2) Un acord internațional menționat la alineatul (1) este orice acord internațional bilateral sau multilateral în vigoare între statele membre și țări terțe în domeniul cooperării judiciare în materie penală și al cooperării polițienești.

(3) Autoritatea competentă care transferă datele informează autoritatea de supraveghere cu privire la transferurile efectuate în temeiul prezentului articol.

(4) Atunci când un transfer se întemeiază pe alineatul (1), un astfel de transfer trebuie să fie documentat.

*Articolul 40***Cooperarea internațională în domeniul protecției datelor cu caracter personal**

În ceea ce privește țările terțe și organizațiile internaționale, Comisia și statele membre iau măsurile corespunzătoare pentru:

- (a) elaborarea de mecanisme de cooperare internațională pentru a facilita asigurarea efectivă a respectării legislației privind protecția datelor cu caracter personal;
- (b) acordarea de asistență internațională reciprocă în asigurarea respectării legislației din domeniul protecției datelor cu caracter personal, inclusiv prin notificări, transferul reclamațiilor, asistență în anchete și schimb de informații, sub rezerva unor garanții adecvate pentru protecția datelor cu caracter personal și a altor drepturi și libertăți fundamentale;
- (c) implicarea părților interesate relevante în discuțiile și activitățile care au ca scop consolidarea cooperării internaționale în vederea asigurării respectării legislației din domeniul protecției datelor cu caracter personal;
- (d) promovarea schimburilor de legislație și practici în materie de protecție a datelor cu caracter personal și a documentării cu privire la acestea, inclusiv cu privire la conflictele de jurisdicție cu țările terțe.

*CAPITOLUL VI****Autorități de supraveghere independente***

Secțiunea 1

Statut independent*Articolul 41***Autoritatea de supraveghere**

- (1) Fiecare stat membru garantează că una sau mai multe autorități publice independente sunt responsabile de monitorizarea aplicării prezentei directive, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea și în vederea facilitării liberei circulații a datelor cu caracter personal în cadrul Uniunii („autoritatea de supraveghere”).
- (2) Fiecare autoritate de supraveghere contribuie la aplicarea consecventă a prezentei directive în întreaga Uniune. În acest scop, autoritățile de supraveghere cooperează atât între ele, cât și cu Comisia, în conformitate cu capitolul VII.
- (3) Statele membre pot să prevadă că o autoritate de supraveghere instituită în conformitate cu Regulamentul (UE) 2016/679 constituie autoritatea de supraveghere menționată în prezenta directivă și își asumă responsabilitatea pentru sarcinile autorității de supraveghere care urmează să fie instituită în conformitate cu alineatul (1) din prezentul articol.
- (4) În cazul în care un stat membru instituie mai multe autorități de supraveghere, statul membru respectiv desemnează autoritatea de supraveghere care reprezintă autoritățile respective în cadrul comitetului menționat la articolul 51.

*Articolul 42***Independență**

- (1) Fiecare stat membru garantează că autoritatea sa de supraveghere beneficiază de independență deplină în îndeplinirea sarcinilor și exercitarea competențelor care le revin în conformitate cu prezenta directivă.
- (2) Statele membre garantează că membrii autorităților lor de supraveghere, în îndeplinirea sarcinilor și în exercitarea competențelor care le revin în conformitate cu prezenta directivă, rămân independenți de orice influență externă directă sau indirectă și nici nu solicită, nici nu acceptă instrucțiuni de la nimeni.
- (3) Membrii autorităților de supraveghere din statele membre nu întreprind acțiuni incompatibile cu îndatoririle lor, iar, pe durata mandatului, nu desfășoară activități incompatibile, remunerate sau nu.
- (4) Fiecare stat membru garantează că autoritatea sa de supraveghere beneficiază de resurse umane, tehnice și financiare, de un sediu și de infrastructura necesară pentru îndeplinirea sarcinilor și exercitarea competențelor în mod eficace, inclusiv a celor care urmează să fie realizate în contextul asistenței reciproce, al cooperării și al participării în cadrul comitetului.

(5) Fiecare stat membru garantează că autoritatea sa de supraveghere selectează și dispune de personal propriu, care se află sub conducerea exclusivă a membrului sau membrilor autorității de supraveghere vizate.

(6) Fiecare stat membru garantează că autoritatea sa de supraveghere face obiectul unui control financiar care nu aduce atingere independenței sale și că dispune de bugete publice anuale distincte, care pot face parte din bugetul general de stat sau național.

Articolul 43

Condiții generale aplicabile membrilor autorității de supraveghere

(1) Statele membre garantează că fiecare membru al autorităților lor de supraveghere este numit prin intermediul unei proceduri transparente:

- de către parlament;
- de către guvern;
- de către șeful statului membru în cauză; sau
- de către un organism independent împuternicit prin dreptul intern să facă numirea.

(2) Fiecare membru dispune de calificările, experiența și competențele, în special în domeniul protecției datelor cu caracter personal, necesare pentru îndeplinirea atribuțiilor și exercitarea competențelor sale.

(3) Atribuțiile unui membru încetează în cazul expirării mandatului, în cazul demisiei sau destituirii în conformitate cu dreptul statului membru în cauză.

(4) Un membru poate fi demis doar în cazuri de abateri grave sau în cazul în care membrul respectiv nu mai întrunește condițiile necesare pentru îndeplinirea atribuțiilor sale.

Articolul 44

Norme privind instituirea autorității de supraveghere

(1) Fiecare stat membru prevede în dreptul său următoarele:

- (a) instituirea autorității sale de supraveghere;
- (b) calificările și condițiile de eligibilitate necesare pentru a fi numit membru al autorității sale de supraveghere;
- (c) normele și procedurile pentru numirea membrului sau a membrilor autorității sale de supraveghere;
- (d) durata mandatului membrului sau al membrilor autorității sale de supraveghere, care nu poate fi mai mică de patru ani, cu excepția primului mandat după 6 mai 2016, care poate fi mai scurt în cazul în care acest lucru este necesar pentru a proteja independența autorității de supraveghere printr-o procedură de numiri eşalonate;
- (e) dacă și de câte ori este eligibil pentru reînnoire mandatul membrului sau membrilor autorității sale de supraveghere; și
- (f) condițiile care reglementează obligațiile membrului sau membrilor și ale personalului autorității sale de supraveghere, interdicțiile privind acțiunile, ocupațiile și beneficiile incompatibile cu acestea în cursul mandatului și după încetarea acestuia, precum și normele care reglementează încetarea activității profesionale.

(2) Membrul sau membrii și personalul fiecărei autorități de supraveghere au obligația, în conformitate cu dreptul Uniunii sau cu dreptul intern, de a păstra atât pe parcursul mandatului, cât și după încetarea acestuia, secretul profesional în ceea ce privește toate informațiile confidențiale de care au luat cunoștință în cursul îndeplinirii atribuțiilor sau al exercitării competențelor lor. Pe durata mandatului lor, această obligație de păstrare a secretului profesional se aplică, în special, în ceea ce privește denunțarea de către persoane fizice a cazurilor de încălcare a prezentei directive.

Secțiunea 2

Abilitări, sarcini și competențe*Articolul 45***Abilitări**

- (1) Fiecare stat membru garantează că autoritatea sa de supraveghere este abilitată să îndeplinească sarcinile și să exercite competențele care îi revin în conformitate cu prezenta directivă pe teritoriul respectivului stat membru.
- (2) Fiecare stat membru garantează că autorității sale de supraveghere îi revine competența să supravegheze operațiunile de prelucrare ale instanțelor atunci când acestea acționează în exercițiul funcției lor judiciare. Statele membre pot să stabilească dispoziții potrivit cărora autorităților sale de supraveghere nu le revine competența să supravegheze operațiunile de prelucrare ale altor autorități judiciare independente atunci când acestea acționează în exercițiul funcției lor judiciare.

*Articolul 46***Sarcini**

- (1) Fiecare stat membru garantează, pe teritoriul său, că autoritatea sa de supraveghere:
- (a) monitorizează și asigură respectarea prezentei directive și a măsurilor de punere în aplicare aferente acesteia;
 - (b) promovează acțiuni de sensibilizare și de înțelegere în rândul publicului a riscurilor, normelor, garanțiilor și drepturilor în materie de prelucrare;
 - (c) oferă consiliere, în conformitate cu dreptul intern, parlamentului național, guvernului și altor instituții și organisme cu privire la măsurile legislative și administrative referitoare la protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea;
 - (d) promovează acțiuni de sensibilizare a operatorilor și a persoanelor împuternicite de aceștia cu privire la obligațiile care le revin în temeiul prezentei directive;
 - (e) furnizează informații, la cerere, oricărei persoane vizate în legătură cu exercitarea drepturilor sale în temeiul prezentei directive și, dacă este cazul, cooperează cu autoritățile de supraveghere din alte state membre în acest scop;
 - (f) tratează plângerile depuse de o persoană vizată sau de un organism, o organizație sau o asociație, în conformitate cu articolul 55, investighează într-o măsură adecvată obiectul plângerii și informează persoana care a depus plângerea cu privire la evoluția și rezultatul investigației, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigații mai amănunțite sau coordonarea cu o altă autoritate de supraveghere;
 - (g) verifică legalitatea prelucrării în conformitate cu articolul 17 și informează persoana vizată, într-un termen rezonabil, cu privire la rezultatul verificării în temeiul alineatului (3) al articolului respectiv sau la motivele pentru care nu a avut loc verificarea;
 - (h) cooperează, inclusiv prin schimb de informații, cu alte autorități de supraveghere și își oferă reciproc asistență pentru a asigura consecvența aplicării și respectării prezentei directive;
 - (i) desfășoară investigații privind aplicarea prezentei directive, inclusiv pe baza unor informații primite de la o altă autoritate de supraveghere sau autoritate publică;
 - (j) monitorizează evoluțiile relevante, în măsura în care acestea au impact asupra protecției datelor cu caracter personal, în special evoluția tehnologiilor informațiilor și comunicațiilor;
 - (k) oferă consiliere cu privire la operațiunile de prelucrare menționate la articolul 28; și
 - (l) contribuie la activitățile comitetului.
- (2) Fiecare autoritate de supraveghere facilitează depunerea plângerilor menționate la alineatul (1) litera (f) prin măsuri precum punerea la dispoziție a unui formular de depunere a plângerii, care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.

(3) Îndeplinirea sarcinilor fiecărei autorități de supraveghere este gratuită pentru persoana vizată și pentru responsabilul cu protecția datelor.

(4) În cazul în care o cerere este în mod vădit nefondată sau excesivă, în special când este repetitivă, autoritatea de supraveghere poate percepe o taxă rezonabilă pe baza costurilor sale administrative sau poate refuza să îi dea curs. Obligația de a demonstra caracterul evident nefondat sau excesiv al cererii respective revine autorității de supraveghere.

Articolul 47

Competențe

(1) Fiecare stat membru garantează prin lege că autorității sale de supraveghere îi revin competențe de investigare efective. Respectivul competențe includ, cel puțin, competența de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal care sunt prelucrate și la toate informațiile necesare pentru îndeplinirea sarcinilor sale.

(2) Fiecare stat membru garantează prin lege că autorității sale de supraveghere îi revin competențe corective efective, cum ar fi, de exemplu:

- (a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la probabilitatea ca operațiunile de prelucrare preconizate să încalce dispozițiile adoptate în temeiul prezentei directive;
- (b) de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile adoptate în temeiul prezentei directive, specificând, după caz, modalitatea și termenul-limită pentru aceasta; în special dispunând rectificarea sau ștergerea datelor cu caracter personal, sau restricționarea prelucrării, în conformitate cu articolul 16;
- (c) de a impune o limitare temporară sau definitivă, inclusiv o interdicție, în ce privește prelucrarea.

(3) Fiecare stat membru garantează prin lege că autorității sale de supraveghere îi revin competențe de consiliere efective pentru a oferi consiliere operatorului în conformitate cu procedura de consultare prealabilă menționată la articolul 28 și de a emite avize, din proprie inițiativă sau la cerere, parlamentului național, guvernului sau, în conformitate cu dreptul său intern, altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal.

(4) Exercițarea competențelor conferite autorității de supraveghere în temeiul prezentului articol face obiectul unor garanții adecvate, inclusiv căi de atac judiciare eficiente și procese echitabile, prevăzute de dreptul Uniunii și de dreptul intern în conformitate cu Carta.

(5) Fiecare stat membru garantează prin lege că autorității sale de supraveghere îi revine competența de a aduce în atenția autorităților judiciare cazurile de încălcare a dispozițiilor adoptate în temeiul prezentei directive și, după caz, de a iniția sau de a se implica într-un alt mod în proceduri judiciare, în scopul de a asigura respectarea dispozițiilor adoptate în temeiul prezentei directive.

Articolul 48

Denunțarea cazurilor de încălcare

Statele membre garantează că autoritățile competente instituie mecanisme eficiente de încurajare a denunțării confidențiale a cazurilor de încălcare a prezentei directive.

Articolul 49

Rapoarte de activitate

Fiecare autoritate de supraveghere întocmește un raport anual cu privire la activitățile sale, care poate include o listă a cazurilor de încălcare notificate și natura sancțiunilor aplicate. Rapoartele se transmit parlamentului național, guvernului și altor autorități desemnate de dreptul intern. Rapoartele se pune la dispoziția publicului, a Comisiei și a comitetului.

CAPITOLUL VII

Cooperarea

Articolul 50

Asistență reciprocă

- (1) Fiecare stat membru garantează că autoritățile sale de supraveghere își furnizează reciproc informațiile relevante și asistență pentru a pune în aplicare și a aplica prezenta directivă în mod consecvent și instituie măsuri de cooperare eficiente între ele. Asistența reciprocă se referă, în special, la cereri de informații și măsuri de supraveghere, cum ar fi cereri în vederea efectuării de consultări, inspecții și investigații.
- (2) Fiecare stat membru garantează luarea de către fiecare autoritate de supraveghere a tuturor măsurilor corespunzătoare necesare pentru a răspunde cererii unei alte autorități de supraveghere, fără întârziere și în cel mult o lună de la data primirii cererii. Astfel de măsuri pot include, în special, transmiterea informațiilor relevante privind desfășurarea unei investigații.
- (3) Cererile de asistență cuprind toate informațiile necesare, inclusiv scopul și motivele care stau la baza acestora. Informațiile care fac obiectul schimbului se utilizează numai în scopul în care au fost solicitate.
- (4) O autoritate de supraveghere căreia i se adresează o cerere de asistență nu poate refuza să îi dea curs, cu excepția cazului în care:
- nu are competență cu privire la obiectul cererii sau la măsurile pe care este solicitată să le execute; sau
 - a da curs cererii ar încălca prezenta directivă sau dreptul Uniunii sau dreptul intern sub incidența căruia intră autoritatea de supraveghere care a primit cererea.
- (5) Autoritatea de supraveghere căreia i s-a adresat cererea informează autoritatea de supraveghere care a transmis cererea cu privire la rezultate sau, după caz, la progresele înregistrate ori măsurile întreprinse pentru a răspunde cererii. În cazul unui refuz în temeiul alineatului (4), autoritatea de supraveghere căreia i s-a adresat cererea explică motivele de refuz.
- (6) Autoritățile de supraveghere cărora li s-a adresat o cerere furnizează, de regulă, informațiile solicitate de alte autorități de supraveghere prin mijloace electronice, utilizând un formular-standard.
- (7) Pentru acțiunile întreprinse în urma unei cereri de asistență reciprocă autoritățile de supraveghere cărora li s-a adresat o cerere nu percep taxă. Autoritățile de supraveghere pot conveni asupra unor compensații reciproce în cazul unor cheltuieli specifice rezultate în urma acordării de asistență reciprocă în situații excepționale.
- (8) Comisia poate preciza, prin intermediul unor acte de punere în aplicare, forma și procedurile pentru asistența reciprocă menționată în prezentul articol, precum și modalitățile de schimb de informații prin mijloace electronice între autoritățile de supraveghere și între autoritățile de supraveghere și comitet. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 58 alineatul (2).

Articolul 51

Sarcinile comitetului

- (1) Comitetul instituit prin Regulamentul (UE) 2016/679 îndeplinește, în ceea ce privește prelucrarea care intră sub incidența prezentei directive, toate sarcinile următoare:
- oferă Comisiei consiliere cu privire la orice aspect legat de protecția datelor cu caracter personal în cadrul Uniunii, inclusiv cu privire la orice propunere de modificare a prezentei directive;
 - examinează, din proprie inițiativă, la cererea unuia dintre membrii săi sau la cererea Comisiei, orice chestiune referitoare la aplicarea prezentei directive și emite orientări, recomandări și bune practici pentru a încuraja aplicarea consecventă a prezentei directive;
 - elaborează orientări destinate autorităților de supraveghere, referitoare la aplicarea măsurilor menționate la articolul 47 alineatele (1) și (3);
 - emite orientări, recomandări și bune practici, în conformitate cu litera (b) de la prezentul alineat, pentru stabilirea cazurilor de încălcare a securității datelor cu caracter personal și pentru determinarea întârzierilor nejustificate menționate la articolul 30 alineatele (1) și (2), precum și pentru circumstanțele speciale în care un operator sau o persoană imputernicită de către operator are obligația de a notifica încălcarea securității datelor cu caracter personal;

- (e) emite orientări, recomandări și bune practici, în conformitate cu litera (b) de la prezentul alineat, în ceea ce privește circumstanțele în care o încălcare a securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor menționate la articolul 31 alineatul (1);
- (f) revizuieste aplicarea practică a orientărilor, a recomandărilor și a bunelor practici menționate la literele (b) și (c);
- (g) prezintă Comisiei un aviz pentru evaluarea caracterului adecvat al nivelului de protecție dintr-o țară terță, un teritoriu sau unul sau mai multe sectoare determinate dintr-o țară terță, sau o organizație internațională, inclusiv pentru a evalua dacă o țară terță, un teritoriu, un sector determinat sau o organizație internațională nu mai asigură un nivel de protecție adecvat.
- (h) promovează cooperarea și schimbul eficient bilateral și multilateral de informații și cele mai bune practici între autoritățile de supraveghere;
- (i) promovează programe comune de formare și facilitează schimburile de personal între autoritățile de supraveghere și, după caz, cu autoritățile de supraveghere ale țărilor terțe sau cu organizațiile internaționale;
- (j) promovează schimbul de cunoștințe și de documente privind dreptul și practicile în materie de protecție a datelor cu autoritățile de supraveghere a protecției datelor la nivel mondial.

În ceea ce privește litera (g) de la primul paragraf, Comisia pune la dispoziția comitetului toată documentația necesară, inclusiv corespondența purtată cu guvernul țării terțe, al teritoriului respectiv sau cu sectorul specific din respectiva țară terță, sau cu organizația internațională.

- (2) În cazul în care Comisia solicită consiliere din partea comitetului, aceasta poate indica un termen limită, ținând seama de caracterul urgent al chestiunii.
- (3) Comitetul își transmite avizele, orientările, recomandările și bunele practici Comisiei și comitetului menționat la articolul 58 alineatul (1) și le publică.
- (4) Comisia informează comitetul cu privire la măsurile pe care le-a luat în urma avizelor, orientărilor, recomandărilor și bunelor practici emise de comitet.

CAPITOLUL VIII

Căi de atac, răspundere și sancțiuni

Articolul 52

Dreptul de a depune o plângere la o autoritate de supraveghere

- (1) Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, statele membre garantează oricărei persoane vizate dreptul de a depune o plângere la o singură autoritate de supraveghere, în cazul în care persoana vizată consideră că prelucrarea datelor cu caracter personal care o vizează încalcă dispozițiile adoptate în temeiul prezentei directive.
- (2) Statele membre garantează că, în cazul în care plângerea nu este depusă la autoritatea de supraveghere competentă în temeiul articolului 45 alineatul (1), autoritatea de supraveghere la care a fost depusă plângerea o transmite autorității de supraveghere competente, fără întârzieri nejustificate. Persoana vizată este informată cu privire la transmitere.
- (3) Statele membre garantează că autoritatea de supraveghere la care s-a depus plângerea oferă, la cerere, asistență suplimentară persoanei vizate.
- (4) Persoana vizată este informată de către autoritatea de supraveghere competentă cu privire la evoluția și rezultatul plângerii, inclusiv cu privire la posibilitatea de a exercita o cale de atac judiciară în conformitate cu articolul 53.

Articolul 53

Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere

- (1) Fără a aduce atingere oricăror alte căi de atac administrative sau extrajudiciare, statele membre dispun că o persoană fizică sau juridică are dreptul de a exercita o cale de atac judiciară eficientă împotriva unei decizii obligatorii din punct de vedere juridic a unei autorități de supraveghere care o vizează.

(2) Fără a aduce atingere oricăror alte căi de atac administrative sau extrajudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care autoritatea de supraveghere competentă în conformitate cu articolul 45 alineatul (1) nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse în conformitate cu articolul 52.

(3) Statele membre garantează că acțiunile împotriva unei autorități de supraveghere sunt introduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere.

Articolul 54

Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau a unei persoane împuternicite de către operator

Fără a aduce atingere vreunei căi de atac administrative sau extrajudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere în conformitate cu articolul 52, statele membre garantează persoanei vizate dreptul la exercitarea unei căi de atac judiciare eficiente în cazul în care aceasta consideră că, prin prelucrarea datelor sale cu caracter personal cu nerespectarea dispozițiilor adoptate în temeiul prezentei directive, au fost încălcate drepturile care îi revin în conformitate cu dispozițiile respective.

Articolul 55

Reprezentarea persoanelor vizate

În conformitate cu dreptul intern procedural, statele membre garantează oricărei persoane vizate dreptul de a mandata un organism, o organizație sau o asociație, care nu are scop lucrativ și care a fost constituită în mod corespunzător în conformitate cu dreptul intern, ale cărei obiective statutare sunt de interes public și care este activă în domeniul protecției drepturilor și libertăților persoanelor vizate în ceea ce privește protecția datelor lor cu caracter personal, să depună plângerea în numele său și să exercite în numele său drepturile menționate la articolele 52, 53 și 54.

Articolul 56

Dreptul la despăgubiri

Statele membre garantează oricărei persoane care a suferit prejudicii materiale sau morale ca urmare a unei operațiuni de prelucrare ilegale sau a oricărei acțiuni care încalcă dispozițiile adoptate în temeiul prezentei directive dreptul de a obține despăgubiri, în temeiul dreptului intern, pentru prejudiciul cauzat de operator sau de o altă autoritate competentă.

Articolul 57

Sanțiuni

Statele membre definesc normele privind sancțiunile aplicabile în cazurile de încălcare a dispozițiilor adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a se asigura că acestea sunt puse în aplicare. Sancțiunile prevăzute trebuie să fie eficiente, proporționale și disuasive.

CAPITOLUL IX

Acte de punere în aplicare

Articolul 58

Procedura comitetului

(1) Comisia este asistată de comitetul înființat prin articolul 93 din Regulamentul (UE) 2016/679. Acesta reprezintă un comitet în sensul Regulamentului (UE) nr. 182/2011.

(2) Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

(3) Atunci când se face trimitere la prezentul alineat, se aplică articolul 8 din Regulamentul (UE) nr. 182/2011 coroborat cu articolul 5 din același regulament.

CAPITOLUL X

Dispoziții finale

Articolul 59

Abrogarea Deciziei-cadru 2008/977/JAI

- (1) Decizia-cadru 2008/977/JAI se abrogă începând cu 6 mai 2018.
- (2) Trimiterile la decizia abrogată menționată la alineatul (1) se interpretează ca trimiteri la prezenta directivă.

Articolul 60

Actele Uniunii aflate deja în vigoare

Dispozițiile specifice referitoare la protecția datelor cu caracter personal din actele juridice ale Uniunii care au intrat în vigoare până la 6 mai 2016 în domeniul cooperării judiciare în materie penală și al cooperării polițienești, care reglementează prelucrarea între statele membre și accesul autorităților desemnate ale statelor membre la sistemele de informații instituite în temeiul tratatelor și care intră sub incidența prezentei directive nu sunt afectate.

Articolul 61

Relația cu acordurile internaționale încheiate anterior în domeniul cooperării judiciare în materie penală și al cooperării polițienești

Acordurile internaționale care implică transferul de date cu caracter personal către țări terțe sau organizații internaționale, care au fost încheiate de statele membre înainte de 6 mai 2016 și sunt aplicabile înainte de 6 mai 2016 și care sunt în conformitate cu dreptul Uniunii, rămân în vigoare până la modificarea, înlocuirea sau revocarea lor.

Articolul 62

Rapoartele Comisiei

- (1) Până la 6 mai 2022 și, ulterior, la fiecare patru ani, Comisia transmite Parlamentului European și Consiliului, un raport privind evaluarea și revizuirea prezentei directive. Rapoartele sunt făcute publice.
- (2) În contextul evaluărilor și revizuirilor menționate la alineatul (1), Comisia examinează, în special, aplicarea și funcționarea capitolului V privind transferul datelor cu caracter personal către țări terțe sau organizații internaționale, acordând o atenție deosebită deciziilor adoptate în temeiul articolului 36 alineatul (3) și al articolului 39.
- (3) În scopul alineatelor (1) și (2), Comisia poate solicita informații de la statele membre și de la autoritățile de supraveghere.
- (4) La efectuarea evaluărilor și revizuirilor menționate la alineatele (1) și (2), Comisia ia în considerare pozițiile și concluziile Parlamentului European, ale Consiliului și ale altor organisme și surse relevante.
- (5) Comisia transmite, dacă este necesar, propuneri corespunzătoare în vederea modificării prezentei directive, în special ținând seama de evoluțiile din domeniul tehnologiei informației și având în vedere progresele societății informaționale.
- (6) Până la 6 mai 2019, Comisia revizuieste celelalte acte adoptate de Uniune care reglementează prelucrarea de către autoritățile competente în scopurile prevăzute la articolul 1 alineatul (1), inclusiv actele menționate la articolul 60, pentru a evalua necesitatea de a le alinia la prezenta directivă și prezintă, după caz, propunerile necesare de modificare a actelor respective pentru a asigura o abordare uniformă privind protecția datelor cu caracter personal care intră în domeniul de aplicare al prezentei directive.

*Articolul 63***Transpunerea**

(1) Statele membre adoptă și publică, până la 6 mai 2018, actele cu putere de lege și actele administrative necesare pentru a se conforma prezentei directive. Statele membre notifică de îndată Comisiei textele acestor dispoziții. Statele membre aplică aceste dispoziții începând cu 6 mai 2018.

Atunci când statele membre adoptă dispozițiile respective, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o astfel de trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.

(2) Prin derogare de la alineatul (1), un stat membru poate prevedea că, în mod excepțional, în cazul în care acest lucru implică eforturi disproporționate, sistemele de prelucrare automată instituite înainte de 6 mai 2016 sunt aduse în conformitate cu articolul 25 alineatul (1) până la 6 mai 2023.

(3) Prin derogare de la alineatele (1) și (2) din prezentul articol, un stat membru poate aduce, în circumstanțe excepționale, în conformitate cu articolul 25 alineatul (1), un sistem de prelucrare automată, în conformitate cu alineatul (2) din prezentul articol, într-un termen determinat, după încheierea perioadei menționate la alineatul (2) din prezentul articol, dacă, în caz contrar, s-ar provoca dificultăți majore pentru funcționarea respectivului sistem de prelucrare automată. Statul membru respectiv notifică Comisiei motivele respectivelor dificultăți majore și motivele pe care se întemeiază termenul determinat în care statul membru aduce în conformitate cu articolul 25 alineatul (1) respectivul sistem de prelucrare automată. Termenul determinat nu depășește în niciun caz 6 mai 2026.

(4) Statele membre comunică Comisiei textul principalelor dispoziții de drept intern pe care le adoptă în domeniul reglementat de prezenta directivă.

*Articolul 64***Intrarea în vigoare**

Prezenta directivă intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.

*Articolul 65***Destinatari**

Prezenta directivă se adresează statelor membre.

Adoptată la Bruxelles, 27 aprilie 2016.

Pentru Parlamentul European
Președintele
M. SCHULZ

Pentru Consiliu
Președintele
J.A. HENNIS-PLASSCHAERT

DIRECTIVA (UE) 2016/681 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI**din 27 aprilie 2016****privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave**

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 82 alineatul (1) litera (d) și articolul 87 alineatul (2) litera (a),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European ⁽¹⁾,

după consultarea Comitetului Regiunilor,

hotărând în conformitate cu procedura legislativă ordinară ⁽²⁾,

întrucât:

- (1) La 6 noiembrie 2007, Comisia a adoptat o propunere de decizie-cadru a Consiliului privind utilizarea registrului cu numele pasagerilor (PNR) în scopul aplicării legii. Cu toate acestea, în urma intrării în vigoare a Tratatului de la Lisabona la 1 decembrie 2009, propunerea Comisiei, care nu a fost adoptată de Consiliu până la data respectivă, a devenit caducă.
- (2) „Programul de la Stockholm – O Europă deschisă și sigură în serviciul cetățenilor și pentru protecția acestora” ⁽³⁾ invită Comisia să prezinte o propunere privind utilizarea datelor din PNR în vederea prevenirii, depistării, investigării și urmării penale a infracțiunilor de terorism și a infracțiunilor grave.
- (3) În comunicarea sa din 21 septembrie 2010 privind o abordare globală referitoare la transferul de date din registrul cu numele pasagerilor (PNR) către țări terțe, Comisia a prezentat o serie de elemente principale ale unei politici a Uniunii în acest domeniu.
- (4) Directiva 2004/82/CE a Consiliului ⁽⁴⁾ reglementează transferul datelor privind informațiile prelabile referitoare la pasagerii (API) de către operatorii de transport aerian către autoritățile naționale competente, în scopul îmbunătățirii controalelor la frontieră și al combaterii imigrației ilegale.
- (5) Obiectivele prezentei directive sunt, printre altele, asigurarea securității, protejarea vieții și siguranței persoanelor și crearea unui cadru juridic pentru protecția datelor din PNR în ceea ce privește prelucrarea acestora de către autoritățile competente.
- (6) Utilizarea eficace a datelor din PNR, cum ar fi compararea datelor din PNR cu diferite baze de date privind persoane și obiecte căutate, este necesară pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, consolidând astfel securitatea internă, pentru strângerea probelor și, acolo unde este cazul, pentru identificarea complicilor infractorilor și destructurarea rețelelor infracționale.
- (7) Evaluarea datelor din PNR permite identificarea persoanelor care nu erau suspectate de implicare în infracțiuni de terorism sau în infracțiuni grave înainte de o astfel de evaluare, și care ar trebui să facă obiectul unor cercetări

⁽¹⁾ JO C 218, 23.7.2011, p. 107.⁽²⁾ Poziția Parlamentului European din 14 aprilie 2016 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 21 aprilie 2016.⁽³⁾ JO C 115, 4.5.2010, p. 1.⁽⁴⁾ Directiva 2004/82/CE a Consiliului din 29 aprilie 2004 privind obligația operatorilor de transport de a comunica datele privind pasagerii (JO L 261, 6.8.2004, p. 24).

suplimentare desfășurate de către autoritățile competente. Prin utilizarea datelor din PNR se poate contracara amenințarea reprezentată de infracțiunile de terorism și de infracțiunile grave dintr-o altă perspectivă decât prin prelucrarea altor categorii de date cu caracter personal. Cu toate acestea, pentru a asigura faptul că prelucrarea datelor din PNR rămâne limitată la ceea ce este necesar, definirea și aplicarea de criterii de evaluare ar trebui să fie limitate la infracțiuni de terorism și infracțiuni grave pentru care este relevantă utilizarea unor astfel de criterii. Mai mult decât atât, criteriile de evaluare ar trebui definite într-un mod care să reducă la minimum numărul persoanelor nevinovate identificate greșit prin intermediul acestui sistem.

- (8) Transportatorii aerieni colectează și prelucrează deja datele din PNR ale pasagerilor lor în scopuri comerciale proprii. Prezenta directivă nu ar trebui să impună transportatorilor aerieni nicio obligație de a colecta sau păstra date suplimentare de la pasageri sau să impună vreo obligație pasagerilor de a furniza date în plus față de cele furnizate deja transportatorilor aerieni.
- (9) Unii transportatori aerieni păstrează, ca parte a datelor din PNR, datele API pe care le colectează, iar alții nu. Utilizarea datelor din PNR împreună cu datele API conferă valoare adăugată asistenței oferite statelor membre pentru verificarea identității unei persoane, consolidând, prin aceasta, valoarea rezultatului respectiv în ceea ce privește aplicarea legii și reducând la minimum riscul de a efectua verificări și cercetări cu privire la persoane nevinovate. Este așadar importantă asigurarea faptului că, atunci când transportatorii aerieni colectează date API, aceștia le transferă indiferent dacă păstrează datele API prin alte mijloace tehnice decât pentru alte date din PNR.
- (10) Pentru a preveni, depista, investiga și urmări penal infracțiunile de terorism și infracțiunile grave, este esențial ca toate statele membre să introducă dispoziții care să stabilească obligații pentru transportatorii aerieni care operează zboruri extra-UE de a transfera datele din PNR colectate, inclusiv datele API. De asemenea, statele membre ar trebui să aibă posibilitatea să extindă această obligație la transportatorii aerieni care operează zboruri intra-UE. Aceste dispoziții nu ar trebui să aducă atingere Directivei 2004/82/CE.
- (11) Prelucrarea datelor cu caracter personal ar trebui să fie proporțională cu obiectivele specifice de securitate urmărite prin prezenta directivă.
- (12) Definiția infracțiunilor de terorism aplicată în prezenta directivă ar trebui să fie aceeași ca cea din Decizia-cadru 2002/475/JAI a Consiliului ⁽¹⁾. Definiția infracțiunilor grave ar trebui să cuprindă categoriile de infracțiuni enumerate în anexa II la prezenta directivă.
- (13) Datele din PNR ar trebui să fie transferate unei singure unități de informații despre pasageri (UIP) desemnate din statul membru în cauză, astfel încât să se asigure claritatea și să se reducă costurile pentru transportatorii aerieni. UIP poate avea diferite filiale într-un stat membru și totodată statele membre pot institui o UIP în comun. Statele membre ar trebui să facă schimb de informații prin intermediul rețelilor relevante de schimb de informații în scopul de a facilita partajarea de informații și a asigura interoperabilitatea.
- (14) Statele membre ar trebui să suporte costurile aferente utilizării, păstrării și schimbului de date din PNR.
- (15) O listă a datelor din PNR solicitate care urmează să fie obținute de o UIP ar trebui să fie elaborată cu scopul de a reflecta cerințele legitime ale autorităților publice de prevenire, depistare, investigare și urmărire penală a infracțiunilor de terorism și a infracțiunilor grave, îmbunătățind prin aceasta securitatea internă în cadrul Uniunii și protejând totodată drepturile fundamentale, în special dreptul la viață privată și dreptul la protecția datelor cu caracter personal. În acest scop, ar trebui să se aplice standarde ridicate în conformitate cu Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta”), cu Convenția pentru protejerea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (denumită în continuare „Convenția nr. 108”) și cu Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale (denumită în continuare „CEDO”). O astfel de listă nu ar trebui să se bazeze pe rasa sau originea etnică, religia sau convingerile, opiniile politice sau de orice altă natură, apartenența la un sindicat, starea de sănătate, viața sexuală sau orientarea sexuală a unei persoane. Datele din PNR ar trebui să conțină exclusiv detalii privind rezervările pasagerilor și itinerariile călătoriilor, care permit autorităților competente să-i identifice pe acei pasageri ai curselor aeriene care reprezintă o amenințare pentru securitatea internă.
- (16) În prezent sunt disponibile două metode de transfer de date: metoda de tip „pull”, prin care autoritățile competente din statul membru care solicită datele din PNR pot accesa sistemul de rezervări al transportatorului aerian și extrage („pull”) o copie a datelor din PNR solicitate, și metoda de tip „push”, prin care transportatorii aerieni transferă („push”) datele PNR solicitate către autoritatea care le solicită, permițându-le astfel transportatorilor aerieni să păstreze controlul asupra datelor pe care le furnizează. Se consideră că metoda de tip „push” oferă un grad mai mare de protecție a datelor și ar trebui să fie obligatorie pentru toți transportatorii aerieni.

⁽¹⁾ Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO L 164, 22.6.2002, p. 3).

- (17) Comisia susține orientările Organizației Aviației Civile Internaționale (OACI) privind PNR. Respectivele orientări ar trebui să reprezinte, prin urmare, baza adoptării formatelor de date compatibile pentru transferurile de date din PNR de către transportatorii aerieni către statele membre. În vederea asigurării unor condiții uniforme pentru punerea în aplicare a formatelor de date compatibile și a protocoalelor relevante aplicabile transferurilor de date de la transportatorii aerieni ar trebui conferite competențe de executare Comisiei. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ⁽¹⁾.
- (18) Statele membre ar trebui să ia toate măsurile necesare pentru a le permite transportatorilor aerieni să își îndeplinească obligațiile ce le revin în temeiul prezentei directive. Statele membre ar trebui să prevadă sancțiuni eficace, proporționale și disuasive, inclusiv sancțiuni financiare, împotriva transportatorilor aerieni care nu își respectă obligațiile privind transferul de date din PNR.
- (19) Fiecare stat membru ar trebui să fie responsabil de evaluarea amenințărilor potențiale legate de infracțiuni de terorism și de infracțiuni grave.
- (20) Ținându-se cont pe deplin de dreptul la protecția datelor cu caracter personal și de dreptul la nediscriminare, nu ar trebui să fie luată nicio decizie care produce efecte juridice adverse asupra unei persoane sau care o afectează în mod semnificativ exclusiv ca urmare a prelucrării automatizate a datelor din PNR. Mai mult, conform articolelor 8 și 21 din Cartă, nicio astfel de decizie nu ar trebui să discrimineze o persoană pe motive precum sexul, rasa, culoarea, originea etnică sau socială, caracteristicile genetice, limba, religia sau convingerile, opiniile politice sau de orice altă natură, apartenența la o minoritate națională, averea, nașterea, un handicap, vârsta sau orientarea sexuală. Cu ocazia revizuirii aplicării prezentei directive, Comisia ar trebui, de asemenea, să ia în considerare respectivele principii.
- (21) Rezultatul prelucrării datelor din PNR nu ar trebui să fie utilizat în niciun caz de statele membre ca motiv pentru eludarea obligațiilor lor internaționale în temeiul Convenției de la Geneva din 28 iulie 1951 privind statutul refugiaților astfel cum a fost modificată de Protocolul din 31 ianuarie 1967, și nici nu ar trebui să fie utilizat pentru a refuza solicitanților de azil utilizarea unor căi legale sigure și eficiente către teritoriul Uniunii pentru a-și exercita dreptul lor la protecție internațională.
- (22) Ținând pe deplin seama de principiile evidențiate în jurisprudența relevantă recentă a Curții de Justiție a Uniunii Europene, aplicarea prezentei directive ar trebui să asigure respectarea deplină a drepturilor fundamentale, a dreptului la viață privată și a principiului proporționalității. De asemenea, ar trebui să respecte cu adevărat obiectivele vizând necesitatea și proporționalitatea pentru a îndeplini interesele generale recunoscute de Uniune și nevoia de a proteja drepturile și libertățile celorlalți în combaterea infracțiunilor de terorism și a infracțiunilor grave. Aplicarea prezentei directive ar trebui justificată în mod corespunzător și ar trebui să existe garanțiile necesare pentru a se asigura legalitatea oricărei acțiuni de stocare, analiză, transfer sau utilizare a datelor din PNR.
- (23) Statele membre ar trebui să facă schimb de date din PNR pe care le primesc, între ele și cu Europol, atunci când acest lucru este considerat necesar pentru prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor de terorism sau a infracțiunilor grave. UIP ar trebui să transmită, după caz, rezultatul prelucrării datelor din PNR fără întârziere către UIP ale altor state membre pentru investigații suplimentare. Dispozițiile prezentei directive nu ar trebui să aducă atingere altor instrumente ale Uniunii privind schimbul de informații între poliție și alte autorități de aplicare a legii și autoritățile judiciare, inclusiv Deciziei 2009/371/JAI a Consiliului ⁽²⁾ și Deciziei-cadru 2006/960/JAI a Consiliului ⁽³⁾. Acest schimb de date din PNR ar trebui să fie reglementat de normele privind cooperarea polițienească și judiciară și nu ar trebui să aducă atingere nivelului ridicat de protecție a vieții private și a datelor cu caracter personal impus de Cartă, de Convenția nr. 108 și de CEDO.
- (24) Ar trebui să fie asigurat un schimb securizat de informații privind datele PNR între statele membre prin intermediul oricărui canal de cooperare existent între autoritățile competente ale statelor membre, precum și, în special, cu Europol, prin intermediul aplicației de rețea pentru schimbul securizat de informații (SIENA) a Europol.

⁽¹⁾ Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

⁽²⁾ Decizia 2009/371/JAI a Consiliului din 6 aprilie 2009 privind înființarea Oficiului European de Poliție (Europol) (JO L 121, 15.5.2009, p. 37).

⁽³⁾ Decizia-cadru 2006/960/JAI a Consiliului din 18 decembrie 2006 privind simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii ale statelor membre ale Uniunii Europene (JO L 386, 29.12.2006, p. 89).

- (25) Datele din PNR ar trebui să fie păstrate atât timp cât este necesar în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave și proporțional cu acest scop. Din cauza naturii datelor și scopurilor pentru care acestea sunt utilizate, este necesar ca datele din PNR să fie păstrate o perioadă suficient de îndelungată pentru efectuarea de analize și pentru utilizarea în investigații. În vederea evitării utilizării disproporționate, după perioada inițială de păstrare datele ar trebui să fie depersonalizate prin mascarea elementelor de date. Pentru a asigura cel mai înalt nivel de protecție a datelor, accesul la datele complete din PNR care permit identificarea directă a persoanei vizate, ar trebui acordat numai în condiții foarte stricte și limitate după perioada inițială respectivă.
- (26) În cazul în care date specifice din PNR au fost transferate unei autorități competente și sunt utilizate în contextul unor anchete penale sau urmăririi penale specifice, păstrarea acestor date de către autoritatea competentă ar trebui să fie reglementată prin dreptul intern, indiferent de perioadele de păstrare a datelor prevăzute în prezenta directivă.
- (27) Prelucrarea datelor PNR în fiecare stat membru, de către UIP și autoritățile competente, ar trebui să facă obiectul unui standard de protecție a datelor cu caracter personal în temeiul dreptului intern în concordanță cu Decizia-cadru 2008/977/JAI a Consiliului ⁽¹⁾ și cu cerințele specifice în materie de protecție a datelor prevăzute în prezenta directivă. Trimiterile la Decizia-cadru 2008/977/JAI ar trebui înțelese ca trimiteri la legislația aflată în vigoare, precum și la legislația care o va înlocui.
- (28) Ținând seama de dreptul la protecția datelor cu caracter personal, drepturile persoanelor vizate cu privire la prelucrarea datelor acestora din PNR, cum ar fi drepturile de acces, rectificare, ștergere și restricționare și drepturile de a fi despăgubit și de a exercita o cale de atac, ar trebui să fie în concordanță atât cu Decizia-cadru 2008/977/JAI cât și cu nivelul ridicat de protecție prevăzut de Cartă și de CEDO.
- (29) Ținând cont de dreptul pasagerilor de a fi informați cu privire la prelucrarea datelor lor cu caracter personal, statele membre ar trebui să asigure faptul că pasagerilor li se furnizează informații corecte, ușor accesibile și ușor de înțeles privind colectarea datelor în PNR, transferul acestora către UIP și drepturile lor ca persoane vizate.
- (30) Prezenta directivă nu aduce atingere dreptului Uniunii și dreptului intern privind principiul accesului public la documente oficiale.
- (31) Transferurile de date din PNR de către statele membre către țări terțe ar trebui să fie permise doar de la caz la caz și cu respectarea deplină a dispozițiilor prevăzute de statele membre în temeiul Deciziei-cadru 2008/977/JAI. În vederea asigurării protecției datelor cu caracter personal, astfel de transferuri ar trebui să facă obiectul unor cerințe suplimentare referitoare la scopul transferului. Acestea ar trebui, de asemenea, să facă obiectul principiilor necesității și proporționalității și să îndeplinească nivelul ridicat de protecție prevăzut de Cartă și de CEDO.
- (32) Autoritatea națională de supraveghere înființată în contextul punerii în aplicare a Deciziei-cadru 2008/977/JAI ar trebui să fie, de asemenea, responsabilă de consilierea privind dispozițiile adoptate de statele membre în temeiul prezentei directive și de monitorizarea aplicării acestora.
- (33) Prezenta directivă nu aduce atingere posibilității statelor membre de a prevedea, în dreptul intern, un sistem pentru colectarea și prelucrarea datelor din PNR de la operatorii economici care nu sunt transportatori aerieni, cum ar fi agențiile de voiaj și operatorii de turism care oferă servicii legate de călătorii – inclusiv rezervarea de zboruri – pentru care colectează și prelucrează date din PNR, sau de la alți transportatori decât cei menționați în prezenta directivă, cu condiția ca aceste dispoziții ale dreptului intern să respecte dreptul Uniunii.
- (34) Prezenta directivă nu aduce atingere normelor actuale ale Uniunii privind modalitățile în care se realizează controalele la frontieră și nici normelor Uniunii care reglementează intrarea și ieșirea de pe teritoriul Uniunii.
- (35) Ca o consecință a diferențelor juridice și tehnice dintre dispozițiile naționale privind prelucrarea datelor cu caracter personal, inclusiv datele din PNR, transportatorii aerieni se confruntă și se vor confrunta cu cerințe diferite referitoare la tipurile de informații care urmează să fie transmise și la condițiile în care acestea sunt

⁽¹⁾ Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală (JO L 350, 30.12.2008, p. 60).

furnizate autorităților naționale competente. Respectivă diferențe pot aduce atingere cooperării eficiente între autoritățile naționale competente în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave. Prin urmare, este necesar să se stabilească la nivelul Uniunii un cadrul legal comun pentru transferul și prelucrarea datelor din PNR.

- (36) Prezenta directivă respectă drepturile fundamentale și principiile Cartei, în special dreptul la protecția datelor cu caracter personal, dreptul la viață privată și dreptul la nediscriminare, astfel cum sunt protejate prin articolele 8, 7 și 21 din Cartă, și, prin urmare, ar trebui să fie pusă în aplicare în consecință. Prezenta directivă este compatibilă cu principiile protecției datelor, iar dispozițiile sale sunt conforme cu Decizia-cadru 2008/977/JAI. În plus, în vederea respectării principiului proporționalității, în domenii specifice prezenta directivă prevede norme mai stricte privind protecția datelor decât Decizia-cadru 2008/977/JAI.
- (37) Domeniul de aplicare al prezentei directive este cât se poate de limitat, întrucât: prevede păstrarea datelor din PNR în UIP pentru o perioadă care nu depășește cinci ani, după care datele ar trebui șterse; permite ca datele să fie depersonalizate prin mascarea elementelor de date după o perioadă inițială de șase luni; și interzice colectarea și utilizarea datelor sensibile. Pentru a asigura eficiența și un nivel ridicat de protecție a datelor, statele membre sunt obligate să asigure că o autoritate de supraveghere națională independentă și, în special, un responsabil cu protecția datelor, sunt responsabili de consilierea și de monitorizarea privind modul de prelucrare a datelor din PNR. Fiecare prelucrare de date din PNR ar trebui să fie luată într-o evidență sau documentată în scopul verificării legalității sale, al automonitorizării și în scopul garantării integrității și securității adecvate a prelucrării datelor. De asemenea, statele membre ar trebui să se asigure că pasagerilor le sunt oferite informații clare și precise cu privire la colectarea datelor în PNR și cu privire la drepturile lor.
- (38) Deoarece obiectivele prezentei directive, și anume transferul datelor din PNR de către transportatorii aerieni și prelucrarea acestor date în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave, nu pot fi realizate în mod satisfăcător de către statele membre, dar pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității astfel cum este definit la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este definit la articolul menționat, prezenta directivă nu depășește ceea ce este necesar pentru realizarea obiectivelor menționate.
- (39) În conformitate cu articolul 3 din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, aceste state membre au notificat intenția lor de a participa la adoptarea și la aplicarea prezentei directive.
- (40) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu participă la adoptarea prezentei directive, nu are obligații în temeiul acesteia și aceasta nu i se aplică.
- (41) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ⁽¹⁾ și a emis un aviz la 25 martie 2011,

ADOPTĂ PREZENTA DIRECTIVĂ:

CAPITOLUL I

Dispoziții generale

Articolul 1

Obiectul și domeniul de aplicare

- (1) Prezenta directivă reglementează:
- (a) transferul de către transportatorii aerieni al datelor din registrul cu numele pasagerilor (PNR) ale pasagerilor zborurilor extra-UE;
- (b) prelucrarea datelor menționate la litera (a), inclusiv colectarea, utilizarea și păstrarea acestora de către statele membre și schimbul de astfel de date între statele membre.

⁽¹⁾ Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

(2) Datele din PNR colectate în conformitate cu prezenta directivă pot fi prelucrate doar în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave, astfel cum este prevăzut la articolul 6 alineatul (2) literele (a), (b) și (c).

Articolul 2

Aplicarea prezentei directivei în cazul zborurilor intra-UE

(1) Dacă un stat membru decide să aplice prezenta directivă în cazul zborurilor intra-UE, acesta notifică în scris Comisia. Un stat membru poate transmite sau revoca o astfel de notificare în orice moment. Comisia publică respectiva notificare și orice revocare a acesteia în *Jurnalul Oficial al Uniunii Europene*.

(2) Atunci când se transmite o notificare menționată la alineatul (1), toate dispozițiile prezentei directive se aplică zborurilor intra-UE ca și cum ar fi zboruri extra-UE și datelor din PNR de la zborurile intra-UE ca și cum ar fi date PNR de la zboruri extra-UE.

(3) Un stat membru poate decide să aplice prezenta directivă numai anumitor zboruri intra-UE. În luarea unei astfel de decizii, statul membru alege zborurile pe care le consideră necesare pentru urmărirea obiectivelor prezentei directive. Statul membru poate decide în orice moment modificarea selecției zborurilor intra-UE.

Articolul 3

Definiții

În sensul prezentei directive, se aplică următoarele definiții:

1. „transportator aerian” înseamnă o întreprindere de transport aerian care deține o licență de operare valabilă sau un document echivalent care îi permite să efectueze activități de transport aerian de pasageri;
2. „zbor extra-UE” înseamnă orice zbor regulat sau neregulat al unui transportator aerian cu proveniența dintr-o țară terță și planificat să aterizeze pe teritoriul unui stat membru sau să decoleze de pe teritoriul unui stat membru și planificat să aterizeze într-o țară terță, inclusiv, în ambele cazuri, zboruri cu orice escală pe teritoriul statelor membre sau al țărilor terțe;
3. „zbor intra-UE” înseamnă orice zbor regulat sau neregulat al unui transportator aerian cu proveniența de pe teritoriul unui stat membru și planificat să aterizeze pe teritoriul unuia sau mai multor state membre, fără escală pe teritoriul unei țări terțe;
4. „pasager” înseamnă orice persoană, inclusiv persoanele aflate în transfer sau în tranzit și excluzând membrii echipajului, transportată sau care urmează să fie transportată într-o aeronavă cu consimțământul transportatorului aerian, acest consimțământ fiind exprimat prin înregistrarea persoanei respective pe lista pasagerilor;
5. „registru cu numele pasagerilor” sau „PNR” înseamnă un registru al cerințelor de călătorie ale fiecărui pasager, care conține informațiile necesare pentru a permite prelucrarea și controlul rezervărilor de către transportatorii aerieni care efectuează rezervările și de către cei participanți, pentru fiecare călătorie rezervată de către sau în numele oricărei persoane, indiferent că este conținut în sistemele de rezervare, în sistemele de control al plecărilor utilizat pentru verificarea pasagerilor la îmbarcarea în avion, sau în sisteme echivalente care oferă aceleași funcționalități;
6. „sistem de rezervare” înseamnă sistemul intern al transportatorului aerian, în care datele din PNR sunt colectate pentru gestionarea rezervărilor;
7. „metoda de tip push” înseamnă metoda prin care transportatorii aerieni transferă datele din PNR, enumerate în anexa I, în baza de date a autorității solicitante;

8. „infracțiuni de terorism” înseamnă infracțiunile prevăzute de dreptul intern menționate la articolele 1-4 din Decizia-cadru 2002/475/JAI;
9. „infracțiuni grave” înseamnă infracțiunile enumerate în anexa II, care sunt pasibile de pedepse cu închisoarea sau cu o măsură privativă de libertate pe o perioadă maximă de cel puțin trei ani în temeiul dreptului intern al unui stat membru;
10. „a depersonaliza prin mascarea elementelor de date” înseamnă a face ca acele elemente ale datelor care ar putea servi la identificarea directă a persoanei vizate să nu fie vizibile pentru un utilizator.

CAPITOLUL II

Responsabilitățile statelor membre

Articolul 4

Unitatea de informații despre pasageri

- (1) Fiecare stat membru instituie sau desemnează o autoritate competentă pentru prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave sau o filială a unei astfel de autorități, care să acționeze ca unitate de informații despre pasageri (UIP).
- (2) UIP este responsabilă de:
 - (a) colectarea datelor din PNR de la transportatorii aerieni, stocarea și prelucrarea acestor date și transferul datelor respective sau al rezultatului prelucrării acestora autorităților competente menționate la articolul 7;
 - (b) schimbul de date din PNR, precum și de schimbul de rezultate ale prelucrării acestora cu UIP din alte state membre și cu Europol, în conformitate cu articolele 9 și 10.
- (3) Membrii personalului UIP pot fi detașați de la autoritățile competente. Statele membre furnizează UIP resurse adecvate pentru ca acestea să-și îndeplinească sarcinile.
- (4) Două sau mai multe state membre (denumite în continuare „statele membre participante”) pot stabili sau desemna o singură autoritate în calitate de UIP. O astfel de UIP se înființează într-unul dintre statele membre participante și este considerată UIP națională a tuturor statelor membre participante. Statele membre participante convin împreună asupra normelor detaliate privind funcționarea UIP și respectă cerințele stabilite în prezenta directivă.
- (5) În termen de o lună de la înființarea UIP, fiecare stat membru transmite o notificare Comisiei cu privire la acest lucru și poate să își modifice notificarea în orice moment. Comisia publică notificarea și eventualele modificări ale acesteia, în *Jurnalul Oficial al Uniunii Europene*.

Articolul 5

Responsabilul cu protecția datelor în cadrul UIP

- (1) UIP numește un responsabil cu protecția datelor pentru monitorizarea prelucrării datelor din PNR și punerea în aplicare a garanțiilor relevante.
- (2) Statele membre pun la dispoziția responsabililor cu protecția datelor mijloacele necesare pentru ca aceștia să își exercite în mod eficient și independent îndatoririle și atribuțiile în conformitate cu prezentul articol.
- (3) Statele membre se asigură că persoana vizată are dreptul de a contacta responsabilul cu protecția datelor, ca punct unic de contact, cu privire la toate aspectele legate de prelucrarea datelor din PNR ale persoanei vizate.

Articolul 6

Prelucrearea datelor din PNR

- (1) Datele din PNR transferate de către transportatorii aerieni sunt colectate de către UIP a statului membru relevant, astfel cum este prevăzut la articolul 8. În cazul în care datele din PNR transferate de transportatorii aerieni includ date diferite față de cele enumerate în anexa I, UIP șterge aceste date imediat și definitiv la primirea lor.
- (2) UIP prelucrează datele din PNR doar în următoarele scopuri:
- (a) efectuarea unei evaluări a pasagerilor înainte de sosirea sau de plecarea programată a acestora din statul membru, în vederea identificării persoanelor care necesită o examinare suplimentară de către autoritățile competente menționate la articolul 7 și, după caz, de către Europol, în conformitate cu articolul 10, având în vedere faptul că respectivele persoane pot fi implicate într-o infracțiune de terorism sau într-o infracțiune gravă;
 - (b) oferirea de răspunsuri, de la caz la caz, unei cereri temeinic justificate bazate pe motive suficiente din partea autorităților competente vizând furnizarea și prelucrearea datelor din PNR în cazuri specifice în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism sau a infracțiunilor grave și comunicarea rezultatelor acestei prelucrări autorităților competente sau, după caz, Europol; și
 - (c) analizarea datelor din PNR în vederea actualizării sau a definirii de noi criterii ce urmează a fi utilizate pentru evaluările efectuate în temeiul alineatului (3) litera (b) în scopul identificării oricăror persoane care pot fi implicate într-o infracțiune de terorism sau într-o infracțiune gravă.
- (3) În momentul efectuării evaluării menționate la alineatul (2) litera (a), UIP poate:
- (a) să compare datele din PNR cu bazele de date relevante în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave, inclusiv cu bazele de date privind persoane sau obiecte căutate sau care fac obiectul unei alerte, în conformitate cu normele Uniunii și cu normele internaționale și naționale aplicabile unor astfel de bazele de date; sau
 - (b) să prelucreze date din PNR în conformitate cu anumite criterii prestabilite.
- (4) Orice evaluare a pasagerilor înainte de sosirea programată în statul membru sau de plecarea programată a acestora din statul membru, efectuată în temeiul alineatului (3) litera (b) pe baza unor criterii prestabilite, se realizează în mod nediscriminatoriu. Respectivul criterii prestabilite trebuie să fie personalizate, proporționale și specifice. Statele membre se asigură că UIP stabilesc aceste criterii și le revizuiesc periodic în cooperare cu autoritățile competente menționate la articolul 7. Aceste criterii nu se întemeiază în niciun caz pe rasa sau originea etnică a unei persoane, opiniile sale politice, religia sau convingerile sale filozofice, apartenența la un sindicat, starea sa de sănătate, viața sexuală sau orientarea sexuală.
- (5) Statele membre se asigură că toate rezultatele pozitive obținute printr-o prelucrare automatizată a datelor din PNR realizată în temeiul alineatului (2) litera (a) sunt reexaminat individual prin mijloace neautomatizate pentru a verifica dacă autoritatea competentă menționată la articolul 7 trebuie să aplice măsuri în temeiul dreptului intern.
- (6) UIP a unui stat membru transmite datele din PNR ale persoanelor identificate conform alineatului (2) litera (a) sau rezultatul prelucrării datelor respective autorităților competente menționate la articolul 7 ale aceluiași stat membru, pentru examinare suplimentară. Aceste transferuri se fac doar de la caz la caz și, în cazul prelucrării automatizate a datelor din PNR, după reexaminarea individuală prin mijloace neautomatizate.
- (7) Statele membre se asigură că responsabilul cu protecția datelor are acces la toate datele prelucrate de către UIP. În cazul în care responsabilul cu protecția datelor consideră că prelucrearea oricăror date nu a fost legală, acesta poate sesiza în acest sens autoritatea națională de supraveghere.
- (8) Stocarea, prelucrearea și analiza datelor din PNR de către UIP se realizează exclusiv într-un loc sigur sau în locuri sigure de pe teritoriul statelor membre.

(9) Consecințele evaluărilor pasagerilor menționate la alineatul (2) litera (a) din prezentul articol nu periclitează dreptul persoanelor care se bucură de dreptul la liberă circulație pe teritoriul Uniunii de a intra pe teritoriul statului membru respectiv, conform Directivei 2004/38/CE a Parlamentului European și a Consiliului ⁽¹⁾. În plus, atunci când evaluările se efectuează în cazul unor zboruri intra-UE între state membre cărora li se aplică Regulamentul (CE) nr. 562/2006 al Parlamentului European și al Consiliului ⁽²⁾, consecințele acestor evaluări respectă regulamentul menționat.

Articolul 7

Autorități competente

(1) Fiecare stat membru adoptă o listă a autorităților competente îndreptățite să solicite sau să primească date din PNR sau rezultatul prelucrării acestor date de la UIP în vederea examinării suplimentare a acestor informații sau a adoptării măsurilor necesare în vederea prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism sau a infracțiunilor grave.

(2) Autoritățile menționate la alineatul (1) sunt autoritățile competente în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor de terorism sau a infracțiunilor grave.

(3) În sensul articolului 9 alineatul (3), fiecare stat membru notifică Comisiei lista autorităților sale competente până la 25 mai 2017, și poate modifica notificarea sa în orice moment. Comisia publică această notificare și orice modificări ale acesteia în *Jurnalul Oficial al Uniunii Europene*.

(4) Datele din PNR și rezultatul prelucrării acestor date primite de la UIP pot face obiectul unei prelucrări ulterioare de către autoritățile competente ale statelor membre doar în scopul specific al prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave.

(5) Alineatul (4) nu aduce atingere competențelor naționale de aplicare a legii sau judiciare în cazul în care alte infracțiuni sau indicii privind astfel de infracțiuni sunt depistate în cursul acțiunilor de aplicare a legii, ca urmare a unei astfel de prelucrări.

(6) Autoritățile competente nu iau doar pe baza prelucrării automatizate a datelor PNR nicio decizie care produce efecte juridice adverse asupra unei persoane sau care afectează în mod semnificativ o persoană. Astfel de decizii nu se iau pe baza rasei sau originii etnice a unei persoane, a opiniilor sale politice, a religiei sau a convingerilor sale filozofice, a apartenenței la un sindicat, a stării sale de sănătate, a vieții sexuale sau orientării sexuale.

Articolul 8

Obligațiile transportatorilor aerieni privind transferurile de date

(1) Statele membre adoptă măsurile necesare pentru a se asigura că transportatorii aerieni transferă, prin „metoda push”, datele din PNR enumerate în anexa I, în măsura în care aceștia colectează deja astfel de date în cadrul activităților lor obișnuite, către baza de date a UIP a statului membru pe teritoriul căruia va sosi sau de pe teritoriul căruia va pleca zborul. Dacă este vorba de un zbor al cărui cod este partajat de unul sau mai mulți transportatori aerieni, obligația de a transfera datele din PNR ale tuturor pasagerilor aparține transportatorului aerian care operează zborul. În cazul în care un zbor extra-UE are una sau mai multe escale pe aeroporturi din state membre diferite, transportatorii aerieni transferă datele din PNR referitoare la toți pasagerii către UIP din toate statele membre în cauză. Acest lucru este valabil și în cazul în care un zbor intra-UE are una sau mai multe escale pe aeroporturi din state membre diferite, dar numai în ceea ce privește statele membre care colectează date din PNR de la zborurile intra-UE.

⁽¹⁾ Directiva 2004/38/CE a Parlamentului European și a Consiliului din 29 aprilie 2004 privind dreptul la liberă circulație și ședere pe teritoriul statelor membre pentru cetățenii Uniunii și membrii familiilor acestora, de modificare a Regulamentului (CEE) nr. 1612/68 și de abrogare a Directivelor 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE și 93/96/CEE (JO L 158, 30.4.2004, p. 77).

⁽²⁾ Regulamentul (CE) nr. 562/2006 al Parlamentului European și al Consiliului din 15 martie 2006 de instituire a unui Cod comunitar privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen) (JO L 105, 13.4.2006, p. 1).

(2) În cazul în care transportatorii aerieni au colectat date privind informații prealabile referitoare la pasageri (API) enumerate la punctul 18 din anexa I, dar nu păstrează datele respective prin aceleași mijloace tehnice ca alte date din PNR, statele membre adoptă măsurile necesare pentru a se asigura că transportatorii aerieni transferă, prin „metoda push”, datele respective către UIP a statelor membre menționate la alineatul (1). În cazul unui astfel de transfer, toate dispozițiile prezentei directive se aplică în privința respectivelor date API.

(3) Transportatorii aerieni transferă datele din PNR prin mijloace electronice utilizând protocoale comune și formate de date compatibile, care urmează a fi adoptate în conformitate cu procedura de examinare menționată la articolul 17 alineatul (2) sau, în caz de defecțiune tehnică, prin orice alte mijloace adecvate care asigură un nivel adecvat de securitate a datelor:

(a) cu 24 până la 48 de ore înainte de ora programată pentru plecarea zborului; și

(b) imediat după închiderea zborului, adică imediat după îmbarcarea pasagerilor în aeronava care se pregătește de decolare și când niciun pasager nu se mai poate îmbarca sau nu mai poate debarca.

(4) Statele membre permit transportatorilor aerieni să limiteze transferul menționat la alineatul (3) litera (b) la actualizări ale transferurilor menționate la litera (a) din alineatul respectiv.

(5) Dacă accesul la datele din PNR este necesar pentru a răspunde unei amenințări specifice și reale având legătură cu infracțiuni de terorism sau cu infracțiuni grave, la solicitarea unei UIP efectuată în conformitate cu dreptul intern, transportatorii aerieni transferă de la caz la caz date din PNR în alte momente decât cele menționate la alineatul (3).

Articolul 9

Schimbul de informații dintre statele membre

(1) Statele membre se asigură că, în ceea ce privește persoanele identificate de o UIP în conformitate cu articolul 6 alineatul (2), toate datele din PNR relevante și necesare sau rezultatul prelucrării respectivelor date este transmis de respectiva UIP către UIP omoloage ale celorlalte state membre. UIP ale statelor membre destinate să transmit informațiile primite către autoritățile lor competente, în conformitate cu articolul 6 alineatul (6).

(2) UIP a unui stat membru are dreptul de a solicita, dacă este necesar, ca UIP a oricărui alt stat membru să îi comunice datele din PNR care sunt păstrate în baza de date a acestuia din urmă și care nu au fost încă depersonalizate prin mascarea elementelor de date în temeiul articolului 12 alineatul (2) și, de asemenea, dacă este necesar, rezultatul oricărei prelucrări a acestora, dacă a fost deja efectuată în temeiul articolului 6 alineatul (2) litera (a). O astfel de solicitare trebuie să fie motivată corespunzător. Aceasta se poate baza pe oricare dintre elementele de date sau o combinație a acestora, după cum consideră necesar UIP solicitantă într-un caz specific de prevenire, depistare, investigare și urmărire penală a infracțiunilor de terorism sau a infracțiunilor grave. UIP comunică informațiile solicitate cât de repede posibil. În cazul în care datele solicitate au fost depersonalizate prin mascarea elementelor de date în conformitate cu articolul 12 alineatul (2), UIP comunică datele din PNR complete numai dacă se consideră în mod rezonabil că este necesar în scopul menționat la articolul 6 alineatul (2) litera (b) și numai dacă este autorizată în acest sens de o autoritate menționată la articolul 12 alineatul (3) litera (b).

(3) Autoritățile competente ale unui stat membru pot solicita direct UIP a oricărui alt stat membru să comunice datele din PNR care sunt păstrate în baza de date a acestuia numai atunci când este necesar în cazuri de urgență și în condițiile prevăzute la alineatul (2). Solicitățile din partea autorităților competente trebuie să fie motivate. O copie a solicitării se trimite întotdeauna UIP a statului membru solicitant. În toate celelalte cazuri, autoritățile competente își transmit solicitările prin UIP din propriul stat membru.

(4) Cu titlu excepțional, în cazul în care accesul la datele din PNR este necesar pentru a răspunde unei amenințări specifice și reale având legătură cu infracțiuni de terorism sau cu infracțiuni grave, UIP a unui stat membru are dreptul de a solicita UIP a unui alt stat membru să obțină date din PNR în conformitate cu articolul 8 alineatul (5) și să le comunice UIP solicitante.

(5) Schimbul de informații în temeiul prezentului articol se poate derula prin intermediul oricărui canal de cooperare existent între autoritățile competente ale statelor membre. Limba folosită în solicitare și în schimbul de informații este

cea aplicabilă canalului utilizat. Atunci când se transmit notificări conform articolului 4 alineatul (5), statele membre informează și Comisia cu privire la coordonatele punctelor de contact cărora le pot fi adresate solicitări în caz de urgență. Comisia comunică aceste detalii statelor membre.

Articolul 10

Condițiile de acces al Europol la datele din PNR

- (1) Europol are competența de a solicita date din PNR sau rezultatul prelucrării respectivelor date de la UIP din statele membre, în limitele competențelor sale și în vederea îndeplinirii atribuțiilor sale.
- (2) De la caz la caz, Europol poate adresa UIP a oricărui stat membru, prin intermediul unității naționale Europol, o cerere în format electronic și justificată corespunzător de transmitere a unor date specifice din PNR sau a rezultatului prelucrării respectivelor date. Europol poate adresa o astfel de cerere atunci când acest lucru este strict necesar pentru sprijinirea și consolidarea acțiunii statelor membre în vederea prevenirii, depistării sau investigării unei anumite infracțiuni de terorism sau a unei anumite infracțiuni grave, în măsura în care infracțiunea respectivă intră în sfera de competență a Europol, în temeiul Deciziei 2009/371/JAI. Cererea respectivă conține motive rezonabile pe baza cărora Europol consideră că transmiterea datelor din PNR sau a rezultatului prelucrării datelor din PNR va contribui în mod substanțial la prevenirea, depistarea sau investigarea infracțiunii în cauză.
- (3) Europol informează responsabilul cu protecția datelor, numit în conformitate cu articolul 28 din Decizia 2009/371/JAI, în legătură cu toate schimburile de informații în temeiul prezentului articol.
- (4) Schimbul de informații în temeiul prezentului articol are loc prin intermediul SIENA și în conformitate cu Decizia 2009/371/JAI. Limba folosită în cerere și în schimbul de informații este cea aplicabilă SIENA.

Articolul 11

Transferul datelor către țări terțe

- (1) Un stat membru poate transfera unei țări terțe date din PNR și rezultatul prelucrării acestor date, care sunt stocate de UIP în conformitate cu articolul 12, doar de la caz la caz și dacă:
 - (a) sunt îndeplinite condițiile prevăzute la articolul 13 din Decizia-cadru 2008/977/JAI;
 - (b) transferul este necesar în scopul prezentei directive menționat la articolul 1 alineatul (2);
 - (c) țara terță este de acord să transfere datele unei alte țări terțe doar în cazul în care acest lucru este strict necesar în scopul prezentei directive menționat la articolul 1 alineatul (2) și doar cu autorizarea expresă a statului membru respectiv; și
 - (d) sunt îndeplinite aceleași condiții ca cele prevăzute la articolul 9 alineatul (2).
- (2) În pofida articolului 13 alineatul (2) din Decizia-cadru 2008/977/JAI, transferurile de date din PNR fără consimțământul prealabil al statului membru de la care sunt obținute datele este permis în circumstanțe excepționale și numai dacă:
 - (a) astfel de transferuri sunt esențiale pentru a răspunde unei amenințări specifice și reale, având legătură cu infracțiuni de terorism sau cu infracțiuni grave, la adresa unui stat membru sau a unei țări terțe; și
 - (b) consimțământul prealabil nu poate fi obținut în timp util.Autoritatea responsabilă de acordarea consimțământului este informată fără întârziere, iar transferul este înregistrat în mod corespunzător și face obiectul unei verificări ulterioare.
- (3) Statele membre transferă date din PNR autorităților competente din țările terțe numai în condiții conforme cu prezenta directivă și numai după ce se asigură că destinatarii intenționează să utilizeze datele din PNR în conformitate cu condițiile și garanțiile respective.
- (4) Responsabilul cu protecția datelor din UIP a statului membru care a transferat datele din PNR este informat de fiecare dată când statul membru transferă datele din PNR în temeiul prezentului articol.

Articolul 12

Perioada de păstrare a datelor și depersonalizarea

(1) Statele membre se asigură că datele din PNR furnizate de transportatorii aerieni UIP sunt păstrate într-o bază de date la UIP pentru o perioadă de cinci ani după transferul lor către UIP a statului membru pe teritoriul căruia sosește sau de pe teritoriul căruia pleacă zborul.

(2) La expirarea unei perioade de șase luni de la transferul datelor din PNR, menționat la alineatul (1), toate datele din PNR se depersonalizează prin mascarea următoarelor elemente de date care ar putea servi la identificarea directă a pasagerului la care se referă datele din PNR:

- (a) numele, inclusiv numele altor pasageri din PNR precum și numărul călătorilor din PNR care călătoresc împreună;
- (b) adresa și informațiile de contact;
- (c) toate informațiile privind plata, inclusiv adresa de facturare, în măsura în care acestea conțin informații care ar putea servi la identificarea directă a pasagerului la care se referă PNR sau a oricăror altor persoane;
- (d) informațiile din profilul „client fidel” („frequent flyer”);
- (e) mențiuni cu caracter general, în măsura în care acestea conțin informații care ar putea servi la identificarea directă a pasagerului la care se referă PNR; și
- (f) orice date API care au fost colectate.

(3) După expirarea perioadei de șase luni menționată la alineatul (2), dezvăluirea datelor complete din PNR este permisă numai dacă:

- (a) se consideră în mod rezonabil că este necesară în scopul menționat la articolul 6 alineatul (2) litera (b); și
- (b) este aprobată de către:
 - (i) o autoritate judiciară; sau
 - (ii) o altă autoritate națională competentă, în temeiul dreptului intern, să verifice dacă sunt îndeplinite condițiile pentru dezvăluire, sub rezerva informării responsabilului cu protecția datelor din cadrul UIP și a revizuirii ulterioare de către acesta.

(4) Statele membre asigură ștergerea definitivă a datelor din PNR după expirarea perioadei menționate la alineatul (1). Această obligație nu aduce atingere cazurilor în care date specifice din PNR au fost transferate unei autorități competente și sunt utilizate în contextul unor cazuri specifice în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor de terorism sau a infracțiunilor grave, când păstrarea acestor date de către autoritatea competentă este reglementată de dreptul intern.

(5) Rezultatul prelucrării menționate la articolul 6 alineatul (2) litera (a) este păstrat de UIP numai pentru perioada necesară pentru informarea autorităților competente și, în conformitate cu articolul 9 alineatul (1), informarea UIP ale altor state membre cu privire la un rezultat pozitiv. În cazul în care rezultatul unei prelucrări automatizate s-a dovedit negativ, după o reexaminare individuală prin mijloace neautomatizate astfel cum se menționează la articolul 6 alineatul (5), acesta poate fi, totuși, stocat pentru a se evita viitoare răspunsuri pozitive „false” pe durata în care datele de bază nu sunt șterse în temeiul alineatului (4) din prezentul articol.

Articolul 13

Protecția datelor cu caracter personal

(1) Fiecare stat membru se asigură că, în ceea ce privește toate prelucrările de date cu caracter personal în temeiul prezentei directive, fiecare pasager are același drept la protecția datelor sale cu caracter personal, drepturi la acces, rectificare, ștergere sau restricționare și drepturile de a fi despăgubit și de a exercita o cale de atac, în conformitate cu dreptul Uniunii și cu dreptul intern și în aplicarea articolelor 17, 18, 19 și 20 din Decizia-cadru 2008/977/JAI. Articolele respective sunt, prin urmare, aplicabile.

(2) Fiecare stat membru se asigură că dispozițiile adoptate în temeiul dreptului intern în aplicarea articolelor 21 și 22 din Decizia-cadru 2008/977/JAI privind confidențialitatea prelucrării și securitatea datelor se aplică, de asemenea, tuturor prelucrărilor de date cu caracter personal în temeiul prezentei directive.

(3) Prezenta directivă nu aduce atingere aplicabilității Directivei 95/46/CE a Parlamentului European și a Consiliului ⁽¹⁾ în ceea ce privește prelucrarea datelor cu caracter personal de către transportatorii aerieni, în special obligația acestora de a lua măsuri tehnice și organizatorice adecvate pentru a proteja securitatea și confidențialitatea datelor cu caracter personal.

(4) Statele membre interzic prelucrarea datelor din PNR care dezvăluie rasa sau originea etnică, opiniile politice, religia sau convingerile filozofice, apartenența la un sindicat, sănătatea, viața sexuală sau orientarea sexuală a unei persoane. În situația în care UIP primește date din PNR care dezvăluie astfel de informații, acestea sunt șterse imediat.

(5) Statele membre se asigură că UIP păstrează documentația referitoare la toate sistemele și procedurile de prelucrare aflate în responsabilitatea sa. Această documentație conține cel puțin:

- (a) numele și datele de contact ale organizației și ale personalului UIP care are sarcina de a prelucra datele din PNR și diferitele niveluri de autorizare a accesului;
- (b) cererile depuse de autoritățile competente și UIP ale altor state membre;
- (c) toate cererile de date din PNR și transferurile de aceste date către o țară terță.

La cerere, UIP pune toată documentația la dispoziția autorității naționale de supraveghere.

(6) Statele membre se asigură că UIP păstrează înregistrări cel puțin pentru următoarele operațiuni de prelucrare: colectarea, consultarea, dezvăluirea și ștergerea. Înregistrările operațiunilor de consultare și de dezvăluire indică, în special, scopul, data și ora acestor operațiuni și, în măsura în care este posibil, identitatea persoanei care a consultat sau a dezvăluit datele din PNR și identitatea destinatarilor acestor date. Înregistrările sunt utilizate exclusiv în scopul verificării și al automonitorizării, pentru asigurarea integrității și securității datelor sau pentru audit. La cerere, UIP pune înregistrările la dispoziția autorității naționale de supraveghere.

Înregistrările respective sunt păstrate pentru o perioadă de cinci ani.

(7) Statele membre se asigură că UIP pune în aplicare măsurile și procedurile tehnice și organizatorice adecvate pentru a garanta un nivel ridicat de securitate, adaptat la riscurile reprezentate de prelucrare și de natura datelor din PNR.

(8) Statele membre se asigură că, atunci când o încălcare a securității datelor cu caracter personal ar putea prezenta un risc ridicat pentru protecția datelor cu caracter personal sau ar afecta viața privată a persoanei vizate, UIP comunică fără întârzieri nejustificate această încălcare persoanei vizate și autorității naționale de supraveghere.

Articolul 14

Sancțiuni

Statele membre stabilesc norme privind sancțiunile care se aplică în cazul nerespectării dispozițiilor naționale adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a asigura aplicarea acestora.

În special, statele membre stabilesc norme privind sancțiuni, inclusiv sancțiuni financiare, împotriva transportatorilor aerieni care nu transmit datele astfel cum este prevăzut la articolul 8 sau nu fac acest lucru în formatul cerut.

Sancțiunile prevăzute trebuie să fie eficace, proporționale și cu efect de descurajare.

⁽¹⁾ Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO L 281, 23.11.1995, p. 31).

Articolul 15

Autoritatea națională de supraveghere

- (1) Fiecare stat membru prevede că autoritatea națională de supraveghere menționată la articolului 25 din Decizia-cadru 2008/977/JAI este responsabilă de consilierea privind aplicarea pe teritoriul său a dispozițiilor adoptate de statele membre în temeiul prezentei directive, precum și de monitorizarea respectivei aplicări. Se aplică articolul 25 din Decizia-cadru 2008/977/JAI.
- (2) Respectivul autorități naționale de supraveghere își desfășoară activitățile de la alineatul (1) urmărind protejarea drepturilor fundamentale legate de prelucrarea datelor cu caracter personal.
- (3) Fiecare autoritate națională de supraveghere are următoarele îndatoriri:
- (a) tratează plângerile depuse de orice persoană vizată, investighează chestiunea și informează persoanele vizate cu privire la evoluția și la soluționarea plângerilor lor într-o perioadă de timp rezonabilă;
- (b) verifică legalitatea prelucrării datelor, desfășoară investigații, inspecții și audituri în conformitate cu dreptul intern, fie din proprie inițiativă, fie pe baza unei plângeri menționate la litera (a).
- (4) La cerere, fiecare autoritate națională de supraveghere oferă consiliere oricărei persoane vizate cu privire la exercitarea drepturilor prevăzute în dispozițiile adoptate în temeiul prezentei directive.

CAPITOLUL III

Măsuri de punere în aplicare

Articolul 16

Protocoale comune și formate de date compatibile

- (1) Toate transferurile de date din PNR efectuate de către transportatorii aerieni către UIP în sensul prezentei directive sunt efectuate prin mijloace electronice care oferă garanții suficiente în ceea ce privește măsurile tehnice de securitate și măsurile organizatorice care reglementează prelucrarea ce urmează a fi efectuată. În cazul unei defecțiuni tehnice, datele din PNR pot fi transferate prin orice alte mijloace adecvate, cu condiția ca același nivel de securitate să fie menținut și ca dreptul Uniunii privind protecția datelor să fie respectat pe deplin.
- (2) La un an de la data la care Comisia adoptă pentru prima dată, în conformitate cu alineatul (3), protocoalele comune și formatele de date compatibile, toate transferurile de date din PNR efectuate de către transportatorii aerieni către UIP în sensul prezentei directive sunt efectuate electronic, prin utilizarea de metode securizate conform protocoalelor comune respective. Aceste protocoale sunt comune tuturor transferurilor, pentru a asigura securitatea datelor din PNR în timpul transferului. Datele din PNR sunt transferate într-un format de date compatibil, pentru a asigura posibilitatea citirii datelor de către toate părțile implicate. Toți transportatorii aerieni sunt obligați să selecționeze și să îi precizeze UIP protocolul comun și formatul de date pe care intenționează să le utilizeze pentru transferurile lor.
- (3) Lista protocoalelor comune și a formatelor de date compatibile este stabilită și, dacă este necesar, este adaptată de către Comisie prin intermediul actelor de punere în aplicare. Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 17 alineatul (2).
- (4) Alineatul (1) se aplică atât timp cât protocoalele comune și formatele de date compatibile menționate la alineatele (2) și (3) nu sunt disponibile.
- (5) În termen de un an de la data adoptării protocoalelor comune și a formatelor de date compatibile menționate la alineatul (2), fiecare stat membru asigură adoptarea măsurilor tehnice necesare pentru a putea utiliza protocoalele comune și formatele de date.

*Articolul 17***Procedura comitetului**

(1) Comisia este asistată de un comitet. Respectivul comitet este un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

(2) Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

În cazul în care comitetul nu emite un aviz, Comisia nu adoptă proiectul de act de punere în aplicare și se aplică articolul 5 alineatul (4) al treilea paragraf din Regulamentul (UE) nr. 182/2011.

*CAPITOLUL IV***Dispoziții finale***Articolul 18***Transpunere**

(1) Statele membre asigură intrarea în vigoare a actelor cu putere de lege și a actelor administrative necesare pentru a se conforma prezentei directive până la 25 mai 2018. Statele membre informează de îndată Comisia cu privire la aceasta.

Atunci când statele membre adoptă aceste acte, ele conțin o trimitere la prezenta directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.

(2) Statele membre transmit Comisiei textul principalelor dispoziții de drept intern pe care le adoptă în domeniul reglementat de prezenta directivă.

*Articolul 19***Revizuirea**

(1) Pe baza informațiilor furnizate de statele membre, inclusiv informațiile statistice menționate la articolul 20 alineatul (2), Comisia revizuieste toate elementele prezentei directive și transmite și prezintă un raport Parlamentului European și Consiliului până la 25 mai 2020.

(2) În realizarea acestei revizuii, Comisia acordă o atenție deosebită următoarelor:

- (a) respectării standardelor aplicabile de protecție a datelor cu caracter personal;
- (b) necesității și proporționalității colectării și prelucrării datelor din PNR pentru fiecare dintre scopurile prevăzute în prezenta directivă;
- (c) duratei perioadei de păstrare a datelor;
- (d) eficacității schimbului de date între statele membre; și
- (e) calității evaluărilor, inclusiv în ceea ce privește informațiile statistice colectate în conformitate cu articolul 20.

(3) Raportul menționat la alineatul (1) include, de asemenea, o evaluare cu privire la necesitatea, proporționalitatea și eficiența includerii în domeniul de aplicare a prezentei directive a colectării și a transferului datelor din PNR cu caracter obligatoriu, referitoare la toate sau la anumite zboruri intra-UE. Comisia ține seama de experiența acumulată de statele membre, îndeosebi acele state membre care aplică prezenta directivă în ceea ce privește zborurile intra-UE în conformitate cu articolul 2. Raportul analizează, de asemenea, necesitatea includerii operatorilor economici care nu sunt transportatori, cum ar fi agențiile de voiaj și operatorii de turism care oferă servicii legate de călătorii, inclusiv rezervarea de zboruri, în cadrul domeniului de aplicare al prezentei directive.

(4) Dacă este cazul, ținând seama de revizuirea efectuată în temeiul prezentului articol, Comisia face o propunere legislativă Parlamentului European și Consiliului în vederea modificării prezentei directive.

Articolul 20

Date statistice

(1) Statele membre pun anual la dispoziția Comisiei un set de informații statistice privind datele din PNR furnizate UIP. Aceste statistici nu trebuie să conțină nicio informație cu caracter personal.

(2) Statisticile includ cel puțin:

- (a) numărul total de pasageri ale căror date din PNR au fost colectate și partajate;
- (b) numărul de pasageri identificați pentru examinări suplimentare.

Articolul 21

Relația cu alte instrumente

(1) Statele membre pot continua să aplice acordurile sau înțelegerile bilaterale sau multilaterale dintre acestea privind schimbul de informații dintre autoritățile competente, aflate în vigoare la 24 mai 2016, în măsura în care aceste acorduri sau înțelegeri sunt compatibile cu prezenta directivă.

(2) Prezenta directivă nu aduce atingere aplicabilității Directivei 95/46/CE în ceea ce privește prelucrarea datelor cu caracter personal de către transportatorii aerieni.

(3) Prezenta directivă nu aduce atingere altor obligații și angajamente ale statelor membre sau ale Uniunii în temeiul unor acorduri bilaterale sau multilaterale cu țări terțe.

Articolul 22

Intrarea în vigoare

Prezenta directivă intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezenta directivă se adresează statelor membre în conformitate cu tratatele.

Adoptată la Bruxelles, 27 aprilie 2016.

Pentru Parlamentul European

Președintele

M. SCHULZ

Pentru Consiliu

Președintele

J.A. HENNIS-PLASSCHAERT

ANEXA I

Datele din registrul cu numele pasagerilor în măsura în care au fost colectate de transportatorii aerieni

1. Cod de reper al dosarului pasagerului
 2. Data rezervării/emiterii biletului
 3. Data (datele) prevăzută (prevăzute) a(le) călătoriei
 4. Nume
 5. Adresă și informații de contact (număr de telefon, adresă de e-mail)
 6. Toate informațiile privind forma de plată, inclusiv adresa de facturare
 7. Itinerarul complet de călătorie pentru anumite PNR
 8. Informațiile din profilul „client fidel” („frequent flyer”)
 9. Agenția/agentul de turism
 10. Situația de călătorie a pasagerului, inclusiv confirmările, situația înregistrării pentru zbor, informații privind neprezentarea pasagerului la îmbarcare sau privind prezentarea acestuia în ultimul moment la îmbarcare fără rezervare prealabilă
 11. Informații scindate/divizate din registrul cu numele pasagerilor
 12. Mențiuni cu caracter general (inclusiv toate informațiile disponibile despre minorii însoțiți cu vârsta sub 18 ani, precum numele și sexul minorului, vârsta, limba (limbile) vorbită (vorbite), numele și datele de contact ale persoanei care îl însoțește la plecare și relația sa cu minorul, numele și datele de contact ale persoanei care îl așteaptă la sosire și relația sa cu minorul, agentul prezent la plecare și la sosire)
 13. Informații despre bilet, inclusiv numărul biletului, data emiterii biletului și bilete dus simplu, câmpurile aferente furnizării automate a prețului unui bilet de călătorie
 14. Numărul locului și alte informații privind locul
 15. Informații cu privire la codurile partajate
 16. Toate informațiile cu privire la bagaje
 17. Numărul pasagerilor înregistrați în PNR și alte nume ale acestora
 18. Orice date API colectate (inclusiv tipul, numărul, țara de emisie și data expirării oricărui document de identitate, cetățenia, numele de familie, prenumele, sexul, data nașterii, compania aeriană, numărul zborului, data plecării, data sosirii, aeroportul de plecare, aeroportul de sosire, ora plecării și ora sosirii)
 19. Un istoric al tuturor modificărilor datelor din PNR enumerate la punctele 1-18.
-

ANEXA II

Lista de infracțiuni menționată la articolul 3 punctul 9

1. participarea la un grup infracțional organizat,
 2. traficul de ființe umane,
 3. exploatarea sexuală a copiilor și pornografia infantilă,
 4. traficul ilicit de stupefiante și substanțe psihotrope,
 5. traficul ilegal de arme, muniții și materiale explozibile,
 6. corupția,
 7. fraudă, inclusiv fraudă care aduce atingere intereselor financiare ale Uniunii,
 8. spălarea produselor infracțiunii și falsificarea de monedă, inclusiv falsificarea monedei euro,
 9. infracțiuni informatice și criminalitatea cibernetică,
 10. infracțiuni împotriva mediului, inclusiv traficul ilicit de specii de animale pe cale de dispariție și traficul ilicit de specii și soiuri de plante pe cale de dispariție,
 11. facilitarea intrării și șederii neautorizate,
 12. omorul și vătămarea corporală gravă,
 13. traficul ilicit de organe și țesuturi umane,
 14. răpirea, lipsirea de libertate în mod ilegal și luarea de ostateci,
 15. furtul organizat și tâlhăria prin folosirea unei arme,
 16. traficul ilicit de bunuri culturale, inclusiv antichități și opere de artă,
 17. contrafacerea și pirateria produselor,
 18. falsificarea de documente administrative și uzul de fals,
 19. traficul ilicit de substanțe hormonale și alți factori de creștere,
 20. traficul ilicit de materiale nucleare sau radioactive,
 21. violul,
 22. infracțiunile de competența Curții Penale Internaționale,
 23. sechestrarea ilicită a aeronavelor/navelor,
 24. sabotajul,
 25. traficul de autovehicule furate,
 26. spionajul industrial.
-

ISSN 1977-0782 (ediție electronică)
ISSN 1830-3625 (ediție tipărită)



Oficiul pentru Publicații al Uniunii Europene
2985 Luxemburg
LUXEMBURG

RO