

Bruxelles, 2 octombrie 2015
(OR. en)

12555/15

**Dosar interinstituțional:
2012/0010 (COD)**

**DATAPROTECT 154
JAI 707
DAPIX 163
FREMP 202
COMIX 456
CODEC 1279**

NOTĂ

Sursă:	Președinția
Destinatar:	Consiliul
Nr. doc. ant.:	12266/15
Nr. doc. Csie:	5833/12
Subiect:	Propunere de directivă a Parlamentului European și a Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și libera circulație a acestor date - Abordare generală

I. INTRODUCERE

1. La 27 ianuarie 2012, Comisia a prezentat o propunere de directivă privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și libera circulație a acestor date (denumită în continuare „proiectul de directivă”) ¹. Prezenta propunere vizează înlocuirea Deciziei-cadru 2008/977/JAI ².

¹ Documentul 5833/12.

² JO L 350, 30.12.2008, p. 60-71.

2. În paralel cu propunerea de directivă menționată anterior, Comisia a prezentat o propunere de regulament general privind protecția datelor (denumit în continuare „proiectul de regulament”) ³, care ar trebui să înlocuiască Directiva 95/46/CE ⁴. Proiectul de directivă și cel de regulament constituie pachetul de reformă a cadrului juridic privind protecția datelor.
3. Parlamentul European și-a adoptat poziția în primă lectură cu privire la proiectul de directivă, în contextul procedurii legislative ordinare, la 12 martie 2014 ⁵.
4. Autoritatea Europeană pentru Protecția Datelor și-a dat avizul privind propunerea Comisiei la 8 martie 2012 ⁶.
5. Grupul de lucru pentru schimbul de informații și protecția datelor (DAPIX) a început examinarea textului la reuniunea acestuia din 16 aprilie 2012, în cursul președinției daneze. Proiectul de directivă a fost discutat în cadrul DAPIX în timpul fiecărei președinții care a urmat.
6. În timpul președinției luxemburgheze, începând cu luna iulie 2015, proiectul de directivă a fost discutat în cadrul reuniunilor DAPIX, precum și în cadrul reuniunilor Grupului „Prietenii Președinției” din 2-3 iulie, 15-16 iulie, 22 iulie, 3-4 septembrie, 9 septembrie, 16 septembrie 2015, 21-22 septembrie, în cadrul reuniunii consilierilor JAI din 28 septembrie 2015 și în cadrul Coreper la 24 septembrie și la 1 octombrie 2015.
7. În concluziile sale din 25-26 iunie 2015 Consiliul European a solicitat adoptarea pachetului privind protecția datelor până la sfârșitul anului 2015 ⁷.
8. În cadrul reuniunii sale din 15 iunie 2015, Consiliul și-a adoptat abordarea generală privind proiectul de regulament. Negocierile cu Parlamentul European cu privire la regulament avansează într-un ritm rapid și se desfășoară într-un spirit de compromis.

³ Propunere de regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor) (documentul 5853/12).

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. 31-50.

⁵ Documentul 7428/14.

⁶ Documentul 7375/12.

⁷ A se vedea punctul 12 litera (a) din documentul EUCO 22/15.

9. Având în vedere cele de mai sus, Președinția a depus eforturi în vederea finalizării negocierilor privind cele două propuneri din pachet până la sfârșitul anului 2015.
10. S-au înregistrat progrese considerabile cu privire la textul proiectului de directivă începând cu 1 iulie 2015. Președinția consideră că textul este gata pentru a fi înaintat miniștrilor în vederea confirmării abordării generale, astfel încât negocierile cu Parlamentul European să poată începe pe această bază.

II. TEXTUL DE COMPROMIS

11. Textul proiectului de directivă înaintat de Președinție în vederea abordării generale figurează în anexă. Toate modificările față de propunerea inițială a Comisiei sunt indicate prin caractere subliniate; porțiunile de text eliminate sunt marcate prin simbolul (...). În cazurile în care porțiuni de text existente au fost mutate, acestea sunt indicate prin *caractere cursive*. Observațiile delegațiilor cu privire la textul proiectului de directivă - care nu conținea încă modificările aduse considerentelor 18, 27, 36, 57, 71 și articolelor 61 și 62 - sunt prezentate în rezultatul lucrărilor reuniunii Comitetului Reprezentanților Permanenți din 1 octombrie 2015, astfel cum figurează în documentul 12643/15.
12. Ținând cont de reuniunea Comitetului Reprezentanților Permanenți din 1 octombrie 2015 și în efortul de a răspunde preocupărilor rămase ale delegațiilor, Președinția a făcut următoarele modificări în textul proiectului de directivă:
 - i. în considerentul 18, cuvintele „în sensul prezentei directive” au fost eliminate.
 - ii. în considerentul 27, cuvântul „și” este înlocuit cu „sau”.
 - iii. în considerentul 36, cuvântul „temporară” a fost eliminat, iar cuvintele „într-un astfel de caz” au fost adăugate.
 - iv. în considerentul 57, a fost adăugată o teză pentru a indica faptul că competențele autorităților de supraveghere nu ar trebui să afecteze normele specifice privind procedurile penale sau independența sistemului judiciar.

- v. articolul 61 fost modificat astfel încât să se prevadă că, atunci când evaluează aplicarea directivei, Comisia ar trebui, de asemenea, să evalueze în special funcționarea articolul 36aa.
- vi. perioada de punere în aplicare prevăzută la articolul 62 (și în considerentul 71) a fost prelungită la trei ani.

III. CONCLUZIE

- 13. Având în vedere cele de mai sus și într-un spirit de compromis, în vederea acordării unui mandat Președinției pentru a se angaja în negocieri cu reprezentanții Parlamentului European, Consiliul este invitat să confirme abordarea generală cu privire la textul proiectului de directivă, astfel cum figurează în anexa la prezenta notă.
-

Propunere de

**DIRECTIVĂ A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI
privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de
către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi
penale a infracțiunilor sau al executării pedepselor, al protejării împotriva amenințărilor la
adresa siguranței publice și al prevenirii acestora, precum și la libera circulație a acestor date**

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,

după consultarea Autorității Europene pentru Protecția Datelor,⁸

⁸ JO C... , p.

hotărând în conformitate cu procedura legislativă ordinară,
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 și articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene prevăd că orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.
- (2) Principiile (...) și normele privind protecția persoanelor fizice referitor la 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. Aceasta ar trebui 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 și de date a crescut spectaculos. Tehnologia permite (...) utilizarea de date cu caracter personal la un nivel fără precedent în cadrul activităților (...) precum prevenirea, identificarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor.
- (4) Această evoluție necesită facilitarea liberei circulații a datelor între autoritățile competente (...) în scopul prevenirii, identificării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor, al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora în cadrul Uniunii și a transferului către țări terțe și organizații internaționale, asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal. Aceste evoluții impun construirea unui cadru solid și mai coerent în materie de protecție a datelor în Uniune, însoțit de o aplicare riguroasă a normelor.
- (5) 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 ⁹ se aplică tuturor activităților de prelucrare a datelor 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 „puse în practică pentru exercitarea activităților din afara domeniului de aplicare a dreptului comunitar”, cum ar fi activitățile în domeniul cooperării judiciare în materie penală și al cooperării polițienești.

⁹ JO L 281, 23.11.1995, p. 31.

- (6) 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 ¹⁰ se aplică în domeniul cooperării judiciare în materie penală și al cooperării polițienești. Domeniul de aplicare a prezentei decizii-cadru 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, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, al protejării împotriva amenințărilor la adresa siguranței 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 Tratatul privind funcționarea Uniunii Europene 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/XXX al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor) 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 JO L 350, 30.12.2008, p. 60.

(10) În Declarația 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 normele specifice privind protecția datelor cu caracter personal și libera circulație a acestor date în domeniul cooperării judiciare în materie penală și al cooperării polițienești în temeiul articolului 16 din Tratatul privind funcționarea Uniunii Europene s-ar putea dovedi necesare, având în vedere natura specifică a acestor domenii.

(11) Prin urmare, o directivă distinctă ar trebui să fie adaptată naturii specifice a acestor domenii și să stabilească normele privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile (...) competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor. Aceste autorități competente pot include nu numai autorități publice, precum autoritățile judiciare, poliția sau alte autorități de aplicare a legii, ci și orice organism/entitate însărcinat (însărcinată) prin dreptul intern să îndeplinească sarcini publice sau să exercite atribuții publice în scopul prevenirii, identificării, investigării, sau urmăririi penale a infracțiunilor sau al executării pedepselor. Cu toate acestea, în cazul în care un astfel de organism/entitate prelucrează date cu caracter personal în alte scopuri decât îndeplinirea unor funcții publice și/sau exercitarea unor competențe publice în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, se aplică Regulamentul UE/XXX. Prin urmare, Regulamentul UE/XXX se aplică în cazurile în care un organism/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*, instituțiile financiare păstrează în scopul identificării, investigării și urmăririi penale anumite date care sunt prelucrate de către acestea și furnizează datele respective numai autorităților naționale competente în cazuri specifice și în conformitate cu dreptul intern. Un organism/o entitate care prelucrează date cu caracter personal în numele acestor autorități (...), în cadrul domeniului de aplicare al prezentei directive, ar trebui să aibă obligații în temeiul unui contract sau al altui act juridic și al dispozițiilor aplicabile persoanelor împuternicite de operatori în conformitate cu prezenta directivă, în timp ce aplicarea Regulamentului UE/XXX nu este afectată în ceea ce privește activitățile de prelucrare ale persoanei împuternicite, desfășurate în afara domeniului de aplicare al prezentei directive.

(11a) Activitățile desfășurate de poliție sau de alte autorități de aplicare a legii se concentrează în principal asupra prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor, inclusiv activitățile polițienești desfășurate fără a cunoaște dinainte dacă un incident constituie o infracțiune sau nu. Acestea pot include, de asemenea, exercitarea autorității prin aplicarea unor măsuri coercitive, precum activitățile polițienești desfășurate cu ocazia unor manifestații, evenimente sportive majore și revolte.

Respectivele activități efectuate de autoritățile menționate mai sus includ, de asemenea, menținerea legii și ordinii ca sarcină conferită poliției sau altor autorități de aplicare a legii atunci când acest lucru este necesar pentru a asigura protecție împotriva amenințărilor la adresa securității publice și pentru prevenirea acestor amenințări, în scopul prevenirii comportamentelor umane care pot conduce la amenințări la adresa intereselor fundamentale ale societății protejate prin lege și care pot conduce la o infracțiune.

Statele membre pot încredința autorităților competente alte sarcini care nu sunt neapărat îndeplinite în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, astfel încât prelucrarea datelor cu caracter personal pentru aceste alte scopuri, în măsura în care se încadrează în domeniul de aplicare al dreptului Uniunii, intră în domeniul de aplicare al (...) Regulamentului UE/XXX.

(11aa) Conceptul de infracțiune, în sensul prezentei directive, ar trebui să fie un concept autonom al dreptului Uniunii astfel cum este interpretat de Curtea de Justiție a Uniunii Europene.

(11b) 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 siguranță națională și prelucrarea datelor cu caracter personal de către statele membre atunci când acestea desfășoară activități care se încadrează în domeniul de aplicare al titlului V capitolul 2 din Tratatul privind Uniunea Europeană (...) nu ar trebui să fie considerate (...) activități care se încadrează în domeniul de aplicare al prezentei directive.

(12) 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, directiva ar trebui să prevadă norme armonizate pentru protecția și libera circulație a datelor cu caracter personal (...) prelucrate în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora. Armonizarea drepturilor statelor membre nu ar trebui să aibă ca rezultat scăderea nivelului de protecție a datelor pe care îl oferă statele respective, ci ar trebui, dimpotrivă, să urmărească asigurarea unui 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.

(13) Prezenta directivă nu aduce atingere (...) principiului accesului publicului la documente oficiale (...). În temeiul (...) Regulamentului UE/XXX, 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 al statului membru 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 (...).

(14) 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.

(15) Protecția persoanelor fizice ar trebui să fie neutră din punct de vedere tehnologic și să nu depindă de tehnologiile (...) utilizate, în caz contrar, creându-se un risc serios de eludare. Protecția persoanelor fizice ar trebui să se aplice prelucrării datelor cu caracter personal prin mijloace automate, precum și prelucrării manuale, în cazul în care datele 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 în domeniul de aplicare al prezentei directive.

(...)

(15a) Regulamentul (CE) nr. 45/2001 ¹¹ se aplică prelucrării datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii. Regulamentul (CE) nr. 45/2001 și alte instrumente juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal ar trebui adaptate la principiile și normele din Regulamentul UE/XXX.

¹¹ JO L 8, 12.1.2001, p. 1.

(15b) (...) 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.

(16) 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 care este probabil, în mod rezonabil să fie utilizate fie de operator, fie de orice altă persoană în scopul identificării persoanei fizice respective, în mod direct sau indirect. Pentru a se determina ce mijloace este probabil, în mod rezonabil, să fie utilizate 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 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 care sunt anonimizate astfel încât persoana vizată nu mai este identificabilă.

(16a) Datele genetice ar trebui definite drept date cu caracter personal referitoare la caracteristicile genetice ale unei persoane, care au fost moștenite sau dobândite (...) și care oferă informații unice despre fiziologia sau starea de sănătate a persoanei respective, rezultate în mod special în urma unei analize cromozomiale, a acidului dezoxiribonucleic (ADN) sau a acidului ribonucleic (ARN) sau a unei analize a oricărui alt element ce permite obținerea unor informații echivalente. (...)

(17) Datele cu caracter personal privind sănătatea ar trebui să includă (...) date 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 (...); incluzând (...) informații privind: înscrierea persoanei fizice pentru acordarea de servicii de sănătate; un număr, simbol sau semn distinctiv atribuit unei persoane fizice pentru identificarea unică a acesteia în scopuri medicale; informații rezultate din testarea sau examinarea unei părți a corpului sau a unei substanțe corporale, inclusiv date genetice și eșantioane de material biologic; orice informații privind, de exemplu, o boală, un handicap, un risc de îmbolnăvire, istoricul medical, tratamentul clinic sau starea psihologică sau biomedicală efectivă a persoanei vizate, indiferent de sursa acestora, cum ar fi, de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro.

(18) Orice prelucrare a datelor cu caracter personal trebuie să fie (...) legală și echitabilă față de persoanele fizice în cauză, iar prelucrarea trebuie să fie făcută numai pentru scopuri specifice prevăzute de lege. Principiul prelucrării echitabile în sine nu împiedică autoritățile de aplicare a legii să desfășoare activități precum investigațiile sub acoperire sau supravegherea video. Aceste activități pot fi întreprinse în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării sancțiunilor penale sau 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 de interesele legitime ale persoanei în cauză. 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 6 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale și la articolul 47 din Carta drepturilor fundamentale. Persoanele ar trebui 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 sunt prelucrate ar trebui să fie explicite și legitime și să fie determinate la momentul colectării datelor. Datele ar trebui să fie adecvate și relevante (...) pentru scopurile în care sunt prelucrate; aceasta necesită, în special, asigurarea faptului că datele 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.

(19) Pentru prevenirea, investigarea și urmărirea penală a infracțiunilor, autoritățile (...) competente trebuie să prelucreze (...) datele cu caracter personal colectate în contextul prevenirii, identificării, investigării sau urmăririi penale a anumitor infracțiuni penale dincolo de acest context pentru a înțelege mai bine fenomenele și tendințele infracționale, pentru a culege informații despre rețelele de crimă organizată și pentru a face legături între diferitele infracțiuni constatate.

(19a) În vederea menținerii securității prelucrării și a prevenirii prelucrărilor care încalcă dispozițiile prezentei directive, datele cu caracter personal ar trebui prelucrate într-un mod care să asigure un nivel corespunzător de securitate și confidențialitate, inclusiv să prevină accesul neautorizat la acestea sau (...) utilizarea neautorizată a datelor și a echipamentului utilizat pentru prelucrare, luând în considerare stadiul actual al tehnologiei disponibile și costurile punerii acestora în aplicare în raport cu riscurile și natura datelor cu caracter personal a căror protecție trebuie asigurată.

(20) (...)

(20a) Colectarea datelor cu caracter personal ar trebui să fie efectuată în scopuri specificate, 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, identificării, investigării sau urmăririi penale a infracțiunilor sau ale executării pedepselor sau ale protejării împotriva amenințărilor la adresa siguranței publice și ale 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 este compatibilă în condițiile în care această prelucrare este autorizată în conformitate cu dispozițiile legale aplicabile și este necesară și proporțională în raport cu acest alt scop.

(21) Principiul exactității datelor ar trebui aplicat luând în considerare natura și scopul prelucrării în cauză. Întrucât datele cu caracter personal referitoare la diferite categorii de persoane vizate sunt prelucrate, autoritățile (...) competente (...) ar trebui, în măsura posibilului, să facă distincție între datele cu caracter personal ale diferitelor categorii de persoane vizate, cum ar fi persoanele condamnate pentru comiterea unei infracțiuni, persoanele suspectate, (...) victimele și părțile terțe. 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.

(22) În interpretarea și aplicarea dispozițiilor prezentei directive de către autoritățile (...) competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, ar trebui să se țină seama de specificul sectorului, inclusiv de obiectivele specifice urmărite.

(23) (...)

(24) (...) 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 atât protecția persoanelor fizice, cât 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 transmiterile de date cu caracter personal.

(24a) Ori de câte ori prezenta directivă 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, însă un astfel de temei juridic sau o astfel de măsură legislativă ar trebui să fie clară și precisă, iar aplicarea acesteia să fie previzibilă pentru cei vizați, în conformitate cu jurisprudența Curții de Justiție a Uniunii Europene și a Curții Europene a Drepturilor Omului.

(24b) Prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării sancțiunilor penale sau protecția împotriva fraudei și prevenirea amenințărilor la adresa siguranței publice 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, indiferent dacă este efectuată sau nu prin mijloace automate, precum colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea. În special, normele din prezenta directivă ar trebui să se aplice la transmiterea datelor cu caracter personal în sensul prezentei directive către un destinatar care nu face obiectul prezentei directive. (...) Un astfel de destinatar ar însemna persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organ căruia îi sunt transmise în mod legal datele de către autoritățile competente (...). În cazul în care datele au fost inițial colectate de către o autoritate competentă în unul din scopurile prezentei directive, Regulamentul UE/XXX 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 statului membru (...). În special, normele din Regulamentul UE/XXX ar trebui să se aplice la transmiterea de date cu caracter personal în scopuri care nu intră în domeniul de aplicare al prezentei directive. Pentru prelucrarea datelor cu caracter personal de către un beneficiar care nu este sau nu acționează în calitate de autoritate competentă în sensul prezentei directive și căruia îi sunt divulgate în mod legal date cu caracter personal de către o autoritate competentă, ar trebui să se aplice (...) Regulamentul UE/XXX. La punerea în aplicare a prezentei directive, statele membre pot, de asemenea, aduce precizări suplimentare cu privire la aplicarea normelor din Regulamentul UE/XXX, sub rezerva condițiilor prevăzute în Regulamentul UE/XXX.

(25) Pentru a fi legală, prelucrarea datelor cu caracter personal în temeiul prezentei directive ar trebui să fie necesară pentru (...) îndeplinirea unei sarcini de interes public de către o autoritate competentă în temeiul dreptului Uniunii sau dreptului statelor membre, în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor sau al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, inclusiv prelucrarea necesară (...) pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane (...). Îndeplinirea sarcinii de prevenire, identificare, investigare sau urmărire penală a infracțiunilor, conferită în mod instituțional prin lege autorităților competente, le permite acestora să solicite/ordone persoanelor fizice să respecte solicitările făcute. În acest caz, consimțământul persoanei vizate (astfel cum este definit în Regulamentul UE/XXX) nu ar trebui să ofere 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 acesteia din urmă 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 cu etichete electronice pentru executarea pedepselor. (...)

(25a) 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 de prelucrare a datelor cu caracter personal, cum ar fi, de exemplu, folosirea unor coduri de utilizare, autoritatea (...) care a transmis datele ar trebui să informeze destinatarul căruia îi sunt transmise datele cu privire la aceste condiții și obligația de a le respecta. Astfel de condiții pot cuprinde, de exemplu, faptul că destinatarul căruia îi sunt transmise datele nu transmite mai departe aceste date sau nu le folosește în alte scopuri sau nu informează persoana vizată în cazul unei limitări a dreptului la informare fără aprobarea prealabilă a autorității competente care a transmis datele. Aceste obligații se aplică, de asemenea, transferurilor către destinatari din țări terțe sau către organizații internaționale. Statele membre ar trebui să prevadă că autoritatea (...) competentă care a transmis datele nu aplică astfel de condiții (...) în cazul destinatarilor din alte state membre sau în cazul agențiilor, oficiilor și organismelor instituite în conformitate cu titlul V capitolele IV și V din Tratatul privind funcționarea Uniunii Europene, altele decât cele aplicabile transmiterii similare de date (...) în statul membru al autorității competente care a transmis datele.

(26) 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 poate genera riscuri importante la adresa drepturilor și libertăților fundamentale. Ar trebui incluse în această categorie și datele cu caracter personal care dezvăluie originea rasială sau etnică, utilizarea termenului „origine rasială” în prezenta directivă neimplicând o acceptare de către Uniunea Europeană a teoriilor care urmăresc să stabilească existența unor rase umane separate. Asemenea date nu ar trebui prelucrate, cu excepția cazului în care prelucrarea este condiționată de garanții adecvate pentru drepturile și libertățile (...) persoanei vizate prevăzute de lege și este permisă în (...) cazuri prevăzute de [...] lege (...); sau, dacă nu este deja permisă 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 pot include, de exemplu, posibilitatea de a colecta aceste date numai împreună cu alte date referitoare la persoana vizată, de a garanta în mod adecvat datele colectate, reguli mai stricte privind accesul la date al personalului autorității (...) competente sau 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 datelor este în mod special intruzivă pentru persoane. Cu toate acestea, acordul persoanei vizate nu ar trebui să constituie, în sine, un temei juridic pentru prelucrarea datelor sensibile cu caracter personal de către autoritățile (...) competente.

(27) Persoana vizată ar trebui să aibă dreptul de a nu face obiectul unei decizii care evaluează aspecte personale 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 dreptul de a contesta decizia.

(28) Pentru ca persoanele vizate să își poată exercita drepturile, toate informațiile care le sunt adresate 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.

(29) Ar trebui prevăzute modalități pentru a facilita exercitarea de către persoana vizată a drepturilor care îi sunt conferite prin dispozițiile adoptate în conformitate cu prezenta directivă, printre care se numără în special mecanismele prin care aceasta poate solicita, în mod gratuit, (...) accesul la date, precum și rectificarea, ștergerea și restricționarea acestora. Operatorul ar trebui să aibă obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate. Cu toate acestea, 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 putea refuza să dea curs cererii. (...)

(30) (...) Cel puțin următoarele informații ar trebui să fie puse la dispoziția persoanei vizate: (...) identitatea operatorului, existența unei operațiuni de prelucrare (...) scopurile prelucrării, (...) și (...) dreptul de a înainta o plângere. (...) Aceasta ar putea avea loc pe site-ul autorității competente.

(31) (...)

(32) 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 special, în ce scopuri sunt prelucrate datele, (...) pentru ce perioadă și care este identitatea destinatarilor datelor, inclusiv în țările terțe. (...) Pentru ca acest drept să fie respectat, este suficient ca solicitantul să dețină o sinteză completă a acestor date într-o formă inteligibilă, adică o formă care permite solicitantului să ia cunoștință de aceste date și să verifice că acestea sunt exacte și prelucrate în conformitate cu prezenta directivă, astfel încât acesta să poată, dacă este cazul, să își exercite drepturile care îi sunt conferite prin prezenta directivă.

(33) Statele membre ar trebui să aibă posibilitatea de a adopta măsuri legislative în vederea amânării, a restricționării sau a omiterii informării persoanelor vizate sau a accesului la datele lor cu caracter personal în măsura în care o astfel de (...) măsură constituie o măsură necesară și proporțională într-o societate democratică, ținând seama de interesele legitime ale persoanei fizice vizate, pentru a se evita obstrucționarea cercetărilor, a anchetelor sau a procedurilor oficiale sau judiciare, pentru a nu se afecta măsurile de prevenire, identificare, investigare (...) sau urmărire penală a infracțiunilor sau executarea pedepselor, pentru a se garanta securitatea publică sau securitatea națională ori pentru a se garanta drepturile și libertățile (...) altor persoane.

(34) Orice refuz sau limitare a accesului ar trebui, în principiu, prezentat în scris persoanei vizate și ar trebui să includă (...) motivele de fapt și de drept pe care se bazează decizia.

(35) (...)

(36) 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 este în conformitate cu dispozițiile prevăzute în prezenta directivă. Cu toate acestea, dreptul la rectificare nu ar trebui să afecteze, de exemplu, conținutul depozițiilor martorilor. O persoană fizică (...) poate, de asemenea, să aibă dreptul de a i se restricționa un articol din (...) datele sale cu caracter personal în cazul în care exactitatea este contestată. În special, datele cu caracter personal ar trebui să fie restricționate în loc să fie șterse 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 de date cu caracter personal ar putea include, printre altele, mutarea (...) 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.

(36a) În cazul în care operatorul refuză unei persoane vizate dreptul său de acces, rectificare, ștergere sau restricționare a 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. Când (...) autoritatea de supraveghere intervine în numele persoanei vizate, persoana vizată ar trebui să fie informată de către autoritatea de supraveghere cel puțin că toate verificările și revizuirile necesare efectuate de către autoritatea de supraveghere au avut loc. (...)

(36aa) *În cazul în care datele cu caracter personal sunt prelucrate în cadrul unei anchete penale și al unor acțiuni în instanță în materie penală, (...) exercitarea dreptului la informare, a dreptului de acces, a dreptului de rectificare, a dreptului de ștergere și de restricționare a prelucrării se poate realiza în conformitate cu normele naționale privind procedurile judiciare.*

(37) 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 să fie în măsură să demonstreze (...) conformitatea activităților de prelucrare cu (...) dispozițiile adoptate în temeiul prezentei directive. Aceste măsuri ar trebui să țină seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul la adresa drepturilor și libertăților persoanelor vizate. Atunci când sunt proporționale în raport cu activitățile de prelucrare, măsurile ar trebui să includă punerea în aplicare a unor politici corespunzătoare de protecție a datelor. Aceste politici ar trebui să precizeze aplicarea dispozițiilor privind protecția datelor adoptate în temeiul prezentei directive.

(37a) (...) Riscurile pentru drepturile și libertățile persoanelor vizate, prezentând grade diferite de probabilitate și gravitate, pot fi rezultatul unei prelucrări a datelor care ar putea genera daune 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 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 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, apartenența sindicală; sunt prelucrate date genetice sau date privind sănătatea, viața sexuală sau condamnările penale și infracțiunile sau măsurile de securitate conexe; sunt evaluate aspecte de natură personală, în special analizarea și 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 minori; prelucrarea implică un volum mare de date cu caracter personal și afectează un număr larg de persoane vizate.

(37b) Probabilitatea de a se materializa și gravitatea riscului ar trebui să fie determinate în funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor. 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.

(38) Protecția drepturilor și libertăților persoanelor vizate 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. Pentru a fi în măsură să demonstreze respectarea dispozițiilor adoptate în temeiul prezentei directive, operatorul ar trebui să adopte politici interne și să pună în aplicare măsuri adecvate, care respectă, în special, principiile de protecție a datelor începând cu momentul conceperii și protecție implicită a datelor. Astfel de măsuri 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 relevante în cadrul spațiului de libertate, securitate și justiție.

(39) 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 prezentei directive, 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.

(39a) Efectuarea prelucrării de către o persoană împuternicită de un operator ar trebui să fie reglementată printr-un act juridic care să includă un contract care creează obligații pentru persoana împuternicită de operator în raport cu operatorul și care stipulează, în special, că persoana împuternicită de către operator (...) ar trebui să acționeze numai la instrucțiunile operatorului.

(40) Categoriile de activități de prelucrare a datelor cu caracter personal, inclusiv transferurile în baza unor garanții adecvate și, în situații specifice ar trebui să fie înregistrate de către operator (...) și de către persoana împuternicită de către operator, în scopul de a monitoriza conformitatea cu prezenta directivă. 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 evidente, pentru a putea fi utilizate în scopul monitorizării operațiunilor de prelucrare.

(40a) Înregistrările ar trebui păstrate cel puțin pentru operațiunile din cadrul sistemelor de prelucrare automată, precum colectarea, modificarea, consultarea, divulgarea, combinarea sau ștergerea. Înregistrările ar trebui utilizate pentru verificarea legalității prelucrării datelor, pentru monitorizare proprie și pentru asigurarea integrității și securității datelor. (...) Acest lucru nu împiedică utilizarea înregistrărilor (...) în conformitate cu dreptul statelor membre privind chestiunile operaționale pe parcursul investigațiilor și procedurilor penale.

(41) Pentru a garanta protecția eficientă a drepturilor și libertăților persoanelor vizate (...), operatorul sau persoana împuternicită de operator ar trebui să se consulte cu autoritatea de supraveghere în anumite cazuri înainte de prelucrarea preconizată.

(42) Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate conduce la daune 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, compromiterea reputației, inversarea neautorizată a pseudonimizării, pierderea confidențialității datelor protejate prin secret profesional sau orice alt dezavantaj de natură economică sau socială adus persoanei fizice vizate. Prin urmare, de îndată ce a luat cunoștință de producerea unei (...) încălcări a securității datelor cu caracter personal care poate conduce la (...) daune fizice, materiale sau morale, operatorul ar trebui să o notifice autorității de supraveghere, fără întârzieri nejustificate. Persoanele fizice ale căror (...) drepturi și libertăți (...) ar putea fi afectate grav de încălcare ar trebui să fie informate fără întârzieri nejustificate, pentru a putea să ia măsurile de precauție necesare (...).

(43) Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal nu ar trebui să fie necesară în cazul în care operatorul a pus în aplicare măsuri tehnologice adecvate de protecție și respectivele măsuri au fost aplicate în cazul datelor afectate de încălcarea securității datelor cu caracter personal. Aceste măsuri tehnologice de protecție ar trebui să includă măsurile prin care se asigură că datele devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, în special prin criptarea datelor cu caracter personal. De asemenea, informarea persoanei vizate nu este necesară în cazul în care operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat la adresa drepturilor și libertăților persoanelor vizate afectate nu mai este susceptibil (...) să se materializeze.

(44) (...) O persoană care deține cunoștințe de specialitate în materie de legislație și practici privind protecția datelor poate să acorde asistență operatorului sau persoanei împuternicite de operator pentru monitorizarea conformității la nivel intern cu dispozițiile adoptate în temeiul prezentei directive. Această persoană poate informa și consilia operatorul sau persoana împuternicită de operator, precum și angajații care prelucrează date cu caracter personal, cu privire la obligațiile relevante de protecție a datelor care le revin. Un responsabil cu protecția datelor poate fi numit în comun de mai multe autorități (...) sau organisme competente, luând în considerare structura organizatorică și dimensiunea acestora (...). Acești responsabili cu protecția datelor trebuie să fie în măsură să își îndeplinească îndatoririle și sarcinile în mod independent (...).

(45) Statele membre ar trebui să asigure că transferul către o țară terță sau către o organizație internațională nu are loc decât în cazul în care acest transfer este necesar pentru prevenirea, identificarea, investigarea sau urmărirea penală a infracțiunilor sau pentru executarea pedepselor, precum și în cazul (...)protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, iar autoritatea de control din țara terță sau dintr-o organizație internațională competentă este o autoritate competentă în sensul prezentei directive. Un transfer poate avea loc în cazul în care Comisia decide că țara terță sau organizația internațională în cauză asigură un nivel adecvat de protecție sau că oferă garanții corespunzătoare ori atunci când se aplică derogări pentru situații specifice.

(45a) În cazul transferului de date cu caracter personal de la un stat membru către țări terțe sau către organizații (...) internaționale, acest transfer ar trebui să poată fi efectuat, 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 cu privire la aplicarea legii impun ca, în cazul în care natura unei amenințări la adresa siguranței 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 și/sau (...) organizațiilor internaționale.

(46) Atunci când nu a adoptat o decizie în conformitate cu articolul 41 din Regulamentul (UE) XXX, Comisia poate decide, cu efect în întreaga Uniune, că anumite țări terțe sau un teritoriu ori unul sau mai multe sectoare specificate 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 aceste cazuri, transferurile de date cu caracter personal către țările respective pot avea loc fără a fi necesar să se obțină o autorizație specifică.

(47) În conformitate cu valorile fundamentale pe care se întemeiază Uniunea, în special protecția drepturilor omului, Comisia ar trebui 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.

(48) Comisia ar trebui, de asemenea, să fie în măsură să recunoască faptul că o țară terță, un teritoriu sau un sector specificat 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 la articolele 35-36. 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.

(49) Transferurile care nu se bazează pe o 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 obligatoriu din punct de vedere juridic (...), care să asigure protecția datelor cu caracter personal în cazul în care operatorul (...) a evaluat toate condițiile legate de operațiunea de transfer de date (...) și, pe baza acestei evaluări, consideră că există garanții adecvate în ceea ce privește protecția datelor cu caracter personal. Astfel de instrumente obligatorii din punct de vedere juridic ar putea fi, de exemplu, acorduri bilaterale obligatorii din punct de vedere juridic care au fost încheiate de statele membre și puse în aplicare în ordinea juridică a acestora și pot fi aplicate de către persoanele vizate din respectivele state membre, asigurând (...) respectarea cerințelor în materie de protecție a datelor și drepturile persoanelor vizate, inclusiv dreptul de acces la căi de atac administrative sau judiciare efective. Operatorul poate lua 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 condițiilor legate de operațiunea de transfer de date. Operatorul poate, de asemenea, să ia 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 poate solicita garanții suplimentare.

(49a) (...)

(49aa) 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 acesta este necesar în scopul protejării intereselor vitale ale persoanei vizate sau ale altei 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, sau dacă transferul este necesar pentru prevenirea unei amenințări imediate și grave la adresa siguranței publice a unui stat membru sau a unei țări terțe sau este necesar, într-un caz specific, în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor (...), precum și în scopul protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora ori este necesar, într-un caz specific (...), pentru constatarea, exercitarea sau apărarea unui drept în instanță.

(49b) Autoritățile competente ale statelor membre aplică (...) acordurile internaționale bilaterale sau multilaterale în vigoare, încheiate cu țările 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 ale țărilor terțe implicate. Cu toate acestea, în (...) anumite cazuri individuale, se poate întâmpla ca procedurile prevăzute de acordurile internaționale aplicabile să nu permită schimbul de informații relevante în timp util, astfel încât autoritățile competente ale statelor membre trebuie să transfere date cu caracter personal direct destinatarilor stabiliți în țări terțe. Acesta ar putea fi cazul (...) atunci când infracțiunile au fost săvârșite prin intermediul tehnologiei de comunicații electronice, cum ar fi rețelele sociale, sau în cazul în care datele obținute prin tehnologii de comunicare sunt relevante ca dovadă a săvârșirii unei infracțiuni sau în cazul în care 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 o victimă a unei infracțiuni. Chiar dacă acest schimb (...) între autoritățile competente și beneficiarii stabiliți în țări terțe (...) ar trebui să aibă loc numai în (...) cazuri individuale și specifice, prezenta directivă ar trebui să prevadă condițiile (...) pentru reglementarea acestor 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 plus față de alte norme ale directivei, în special (...) cele cu privire la legalitatea prelucrării și (...) din capitolul V.

(50) (...)

(51) Instituirea în statele membre a unor autorități de supraveghere care să își exercite atribuțiile în deplină independență este 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 să contribuie la (...) aplicarea consecventă a acestora în întreaga Uniune, în scopul asigurării protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. În acest sens, autoritățile de supraveghere ar trebui să coopereze între ele și cu Comisia.

(52) Statele membre pot încredința unei autorități de supraveghere deja existente (...), în conformitate cu Regulamentul UE/XXX, responsabilitatea pentru sarcinile care urmează să fie îndeplinite de către autoritățile naționale de supraveghere care urmează a fi înființate în conformitate cu prezenta directivă.

(53) 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.

(53a) (...) 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. (...)

(54) 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 ar trebui să fie numiți de parlamentul și/sau de guvernul ori șeful de stat al statului membru în cauză ori de către un organism independent împuternicit prin dreptul statului membru să facă numirea prin intermediul unei proceduri transparente (...).

(55) 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 își exercită atribuțiile 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 pot, de asemenea, să prevadă că prelucrarea datelor cu caracter personal ale altor autorități judiciare independente, atunci când acționează în calitatea lor judiciară, de exemplu ministerul public, nu poate fi acoperită de competența autorității de supraveghere. În orice caz, respectarea normelor prezentei directive de către instanțe și alte autorități judiciare independente ar trebui să fie supusă întotdeauna unei supravegheri independente în conformitate cu articolul 8 alineatul (3) din Carta drepturilor fundamentale a UE.

(56) *Fiecare autoritate de supraveghere ar trebui să trateze plângerile depuse de orice persoană vizată și ar trebui să investigheze cazul. 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.*

(57) Pentru a se asigura consecvența monitorizării și a aplicării prezentei directive în întreaga Uniune, autoritățile de supraveghere ar trebui să aibă în fiecare stat membru aceleași sarcini și competențe efective, inclusiv competențe de investigare (...), (...) corective (...), (...) și de consultare. Cu toate acestea, competențele acestora nu ar trebui să afecteze normele specifice stabilite pentru procedurile penale, inclusiv 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 și/sau de a se implica în proceduri judiciare. (...)

Competențele autorităților de supraveghere ar trebui exercitate în conformitate cu garanții procedurale adecvate prevăzute în dreptul Uniunii și în dreptul statelor membre, 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 prezentei directive, 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 intern, cum ar fi obligația de a obține în prealabil o autorizare judiciară.(...)

(...) Adoptarea unei (...) decizii obligatorii (...) ar trebui să facă obiectul (...) controlului jurisdicțional în statul membru al autorității de supraveghere care a adoptat decizia.

(58) Autoritățile de supraveghere ar trebui să își acorde reciproc asistență în îndeplinirea sarcinilor care le revin, pentru a se asigura coerența aplicării și a asigurării aplicării dispozițiilor adoptate în temeiul prezentei directive.

(59) Comitetul european pentru protecția datelor, instituit prin Regulamentul UE/XXX, ar trebui să contribuie la aplicarea coerentă a prezentei directive în întreaga Uniune, inclusiv prin oferirea de consultanță Comisiei și prin promovarea cooperării autorităților de supraveghere în întreaga Uniune.

(60) Orice persoană vizată ar trebui (...) să aibă dreptul de a depune o plângere la o singură autoritate de supraveghere (...), precum și dreptul la o cale de atac eficientă în conformitate cu articolul 47 din Carta drepturilor fundamentale, în cazul în care persoana vizată consideră că drepturile sale în temeiul dispozițiilor adoptate în conformitate cu prezenta directivă 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 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 pe suport electronic, fără a exclude alte mijloace de comunicare.

(61) 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 această 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, acest drept nu include 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. Respectivale 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*.

(62) 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, o organizație sau o asociație care are drept obiectiv asigurarea protecției drepturilor și a intereselor persoanelor vizate în ceea ce privește protecția datelor acestora și este constituit(ă) în conformitate cu dreptul unui stat membru, (...) să depună o plângere în numele său (...) la o autoritate de supraveghere sau să exercite dreptul la o cale de atac. (...) Dreptul de reprezentare a persoanelor vizate ar trebui să se aplice fără a aduce atingere dreptului procedural național care poate impune reprezentarea în mod obligatoriu a persoanelor vizate de un avocat, astfel cum este definită în Directiva 77/249/CEE, în fața instanțelor naționale.

(63) (...)

(64) Orice daună pe care o persoană o poate suferi ca urmare a (...) unei prelucrări care nu este în conformitate cu dispozițiile adoptate în temeiul prezentei directive ar trebui să fie compensată de operator sau de orice altă autoritate competentă în conformitate cu dreptul intern (...). Conceptul de daune ar trebui interpretat, în sens larg, din perspectiva jurisprudenței Curții de Justiție a Uniunii Europene, într-un mod care să reflecte pe deplin obiectivele prezentei directive. Această dispoziție nu aduce atingere niciunei cereri de despăgubiri care rezultă din încălcarea altor norme din dreptul Uniunii sau al statelor membre.

Atunci când se face trimitere la o prelucrare care este ilegală sau nu este în conformitate cu prevederile adoptate în conformitate cu prezenta directivă, trimiterea vizează și prelucrarea care nu este în conformitate cu (...) actele de punere în aplicare adoptate în conformitate cu prezenta directivă. Persoanele vizate ar trebui să primească despăgubiri integrale și efective pentru daunele pe care le-au suferit. (...)

(65) Ar trebui impuse sancțiuni oricărei persoane fizice sau juridice, de drept privat sau public, care nu respectă dispozițiile adoptate în conformitate cu prezenta directivă. Statele membre ar trebui să se asigure că sancțiunile sunt eficace, proporționale și cu efect de descurajare și ar trebui să adopte toate măsurile pentru punerea în aplicare a sancțiunilor.

(66) (...)

(67) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentei directive, Comisia ar trebui investită cu competențe de executare pentru a stabili: (...) nivelul adecvat de protecție oferit de o țară terță, de un teritoriu sau de un sector specific din țara terță respectivă sau dintr-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 Comitetul european pentru protecția datelor. (...) Competențele respective ar trebui să fie exercitate în conformitate cu 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 ¹².

(68) 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 specific din țara terță respectivă sau dintr-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 Comitetul european pentru protecția datelor, (...) ținând seama de faptul că actele respective au un caracter general.

(69) 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, un teritoriu sau un sector specificat din țara terță respectivă sau la o organizație internațională care nu mai asigură un nivel de protecție adecvat.

(70) Întrucât obiectivele prezentei directive, și anume protejarea drepturilor și a libertăților fundamentale ale persoanelor vizate, 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 și, prin urmare, din cauza dimensiunilor sau a efectelor acțiunii, pot fi realizate mai bine la nivelul Uniunii, Uniunea poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum se prevede la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este enunțat la articolul respectiv, prezenta directivă nu depășește ceea ce este necesar pentru atingerea acestui obiectiv.

¹² JO L 55, 28.2.2011, p. 13.

(71) Decizia-cadru 2008/977/JAI a Consiliului ar trebui abrogată prin prezenta directivă. Prelucrările în derulare la data intrării în vigoare a prezentei directive ar trebui să fie aduse în conformitate cu prezenta directivă în termen de trei ani de la data intrării în vigoare a prezentei directive. Cu toate acestea, în cazul în care o astfel de prelucrare este în conformitate cu dreptul Uniunii aplicabil înainte de intrarea 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 înainte de intrarea în vigoare a prezentei directive, având în vedere că aceste cerințe, prin însăși natura lor, trebuie să fie îndeplinite înainte de prelucrare.

(72) Dispozițiile specifice ale actelor 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 sistemele de informare stabilite în conformitate cu tratatele, ar trebui să rămână neafectate, cum ar fi, de exemplu, dispozițiile specifice referitoare la protecția datelor cu caracter personal aplicate în conformitate cu Decizia 2008/615/JAI ¹³ a Consiliului, sau la articolul 23 din Convenția privind asistența reciprocă în materie penală între statele membre ale Uniunii Europene (2000/C 197/01) ¹⁴ . 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 informatizate instituite în conformitate cu tratatele, pentru a evalua necesitatea alinierii acestor dispoziții specifice cu prezenta directivă.

(73) În vederea asigurării unei protecții globale și coerente a datelor cu caracter personal în cadrul Uniunii, acordurile internaționale încheiate de către statele membre înainte de intrarea în vigoare a prezentei directive (...) și care sunt în conformitate cu dispozițiile relevante din dreptul Uniunii aplicabil înainte de intrarea în vigoare a prezentei directive, ar trebui să rămână în vigoare până la data la care sunt modificate, înlocuite sau abrogate. (...).

(74) Prezenta directivă se aplică fără a aduce atingere normelor privind combaterea abuzului sexual, a exploatarii sexuale a copiilor și a pornografiei infantile, astfel cum se prevede în Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011. ¹⁵

¹³ 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.

¹⁴ Actul Consiliului din 29 mai 2000 de elaborare, în conformitate cu articolul 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.

¹⁵ JO L 335, 17.12.2011, p. 1.

(75) În conformitate cu articolul 6a din Protocolul privind poziția Regatului Unit și a Irlandei în ceea ce privește spațiul de libertate, securitate și justiție, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Regatul Unit și Irlanda nu au obligații în temeiul normelor stabilite în prezenta directivă referitoare la prelucrarea datelor cu caracter personal de către statele membre în exercitarea activităților aflate sub incidența domeniului de aplicare a părții a treia titlul V capitolul 4 sau 5 din tratatul menționat, atât timp cât Regatul Unit sau Irlanda nu au 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 Tratatul privind funcționarea Uniunii Europene.

(76) În conformitate cu articolele 2 și 2a din Protocolul privind poziția Danemarcei, astfel cum a fost anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu are obligații în temeiul normelor stabilite în prezenta directivă sau nu face obiectul aplicării lor în ceea ce privește prelucrarea datelor cu caracter personal de către statele membre în exercitarea activităților aflate sub incidența domeniului de aplicare a părții a treia titlul V capitolul 4 sau 5 din Tratatul privind funcționarea Uniunii Europene. Având în vedere faptul că prezenta directivă reprezintă o completare a acquis-ului Schengen, în temeiul părții a treia titlul V din Tratatul privind funcționarea Uniunii Europene, Danemarca, în conformitate cu articolul 4 din protocolul menționat, decide, în termen de șase luni de la adoptarea prezentei directive, dacă o va transpune în dreptul său național.

(77) În ceea ce privește Islanda și Norvegia, prezenta directivă constituie o dezvoltare a dispozițiilor acquis-ului Schengen, în conformitate cu acordul încheiat de Consiliul Uniunii Europene și de Republica Islanda și Regatul Norvegiei privind asocierea acestor două state la implementarea, aplicarea și dezvoltarea acquis-ului Schengen ¹⁶.

(78) 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 ¹⁷.

¹⁶ JO L 176, 10.7.1999, p. 36.

¹⁷ JO L 53, 27.2.2008, p. 52.

(79) 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 ¹⁸.

(80) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, astfel cum sunt consacrate în tratat, 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.

(81) În conformitate cu declarația politică comună a statelor membre și a Comisiei privind documentele explicative din 28 septembrie 2011, statele membre s-au angajat să atașeze la notificarea măsurilor de transpunere, în cazuri justificate, unul sau mai multe documente care explică relația dintre elementele unei directive și părțile corespunzătoare ale instrumentelor naționale de transpunere. În ceea ce privește această directivă, legiuitorul consideră că transmiterea unor astfel de documente este justificată.

(82) Prezenta directivă nu ar trebui să împiedice statele membre să pună în aplicare exercitarea drepturilor persoanelor vizate cu privire la informare, acces, rectificare, ștergere și limitarea prelucrării datelor lor cu caracter personal în cadrul procedurilor penale, precum și eventualele limitări ale acestor drepturi în normele naționale privind procedura penală,

¹⁸ JO L 160, 18.6.2011, p. 19.

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, identificării, investigării, urmăririi penale a infracțiunilor *sau al executării pedepselor sau al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.*
- (1a) Prezenta directivă nu împiedică statele membre 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.
- (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 intern sau dreptul Uniunii, nu este limitat sau interzis din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

Articolul 2 *Domeniu 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 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) (...)
- (3) „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;
- (4) „restricționarea prelucrării” înseamnă marcarea datelor cu caracter personal stocate, cu scopul de a limita prelucrarea viitoare a acestora;
- (4a) „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 identificate sau identificabile.
- (5) „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;
- (6) „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 dreptul unui stat membru, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi stabilite prin dreptul Uniunii sau dreptul statului membru;

- (7) „persoană împuternicită de operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care prelucrează datele cu caracter personal în numele operatorului;
- (8) „destinatar” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism (...) căruia îi sunt dezvăluite datele cu caracter personal, indiferent dacă este sau nu o parte terță; (...) cu toate acestea, autoritățile naționale care pot primi date în cadrul unei anumite anchete nu sunt considerate destinatari;
- (9) „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;
- (10) „date genetice” înseamnă toate datele cu caracter personal (...) referitoare la caracteristicile genetice ale unei persoane care au fost moștenite sau dobândite și care oferă informații unice privind fiziologia sau sănătatea persoanei respective, astfel cum rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;
- (11) (...);
- (12) „date privind sănătatea” înseamnă (...) date legate de sănătatea fizică sau mentală a unei persoane, care dezvăluie informații despre starea de sănătate a acesteia;
- (12a) „creare de profiluri” înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea acestor date pentru a (...) evalua aspecte personale referitoare la (...) o persoană fizică, în special pentru a analiza și a preconiza aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale sau interesele, fiabilitatea sau comportamentul, localizarea sau deplasările;
- (...)

(14) „autoritate (...) competentă” înseamnă orice autoritate (...) publică abilitată în fiecare stat membru în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor *sau al executării pedepselor*, al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora sau orice organism/entitate însărcinat (însărcinată) în conformitate cu dreptul intern să îndeplinească sarcini publice sau să exercite atribuții publice în scopurile (...) stabilite la articolul 1 alineatul (1) (...).

(15) „autoritate de supraveghere” înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 39;

(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, precum și Interpol.

CAPITOLUL II

PRINCIPII

Articolul 4

Principii legate de prelucrarea datelor cu caracter personal

(1) Statele membre prevăd dispoziții potrivit cărora datele cu caracter personal trebuie:

(a) să fie prelucrate în mod legal și echitabil;

(b) să fie colectate în scopuri determinate, explicite și legitime (...) și să nu (...) fie prelucrate într-un mod (...) incompatibil cu aceste scopuri (...);

(c) să fie adecvate, relevante și neexcesive în ceea ce privește scopurile în care sunt prelucrate;

(d) să fie exacte și, dacă este necesar, actualizate; (...)

(e) să fie păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor pentru care sunt prelucrate datele cu caracter personal;

(ee) să fie prelucrate într-un mod care să asigure securitatea adecvată a datelor cu caracter personal;

(...)

(1a) (...)

(2) (...) Prelucrarea de către același operator sau de către un altul, pentru alte scopuri stabilite la articolul 1 alineatul (1) decât cele pentru care datele au fost colectate (...) este permisă în măsura în care:

(...)

(b) operatorul este autorizat să prelucreze astfel de date cu caracter personal în scopurile respective, în conformitate cu dispozițiile legale aplicabile și

(c) prelucrarea este necesară și proporțională în raport cu acest alt scop.

(3) Prelucrarea de către același operator sau de către un altul poate include (...) arhivarea în interes public și (...) utilizarea 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).

Articolul 5

Distincția între diferitele categorii de persoane vizate

(...)

Articolul 6

Verificarea calității datelor transmise sau puse la dispoziție

(1) Statele membre prevăd dispoziții potrivit cărora 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 transmiterilor de date cu caracter personal, (...) se adaugă informațiile necesare care să permită autorității competente destinate să evalueze gradul de exactitate, caracterul integral, gradul de actualitate și fiabilitate al datelor cu caracter personal.

(2) În cazul în care se constată transmiterea unor date cu caracter personal inexacte sau transmiterea unor date în mod ilegal, acest lucru trebuie comunicat de îndată destinatarului. În acest caz, datele cu caracter personal trebuie să fie rectificate, șterse sau restricționate în conformitate cu articolul 15.

Articolul 7

Legalitatea prelucrării

Statele membre prevăd că prelucrarea datelor cu caracter personal este legală numai și în măsura în care aceasta este necesară (...) pentru îndeplinirea unei sarcini de către o autoritate competentă (...) pentru scopurile stabilite la articolul 1 alineatul (1) și că aceasta este întemeiată pe dreptul Uniunii sau dreptul statelor membre (...).

(b) (...)

(c) (...)

(d) (...)

Articolul 7a

Condiții specifice de prelucrare

(1) Datele cu caracter personal colectate de autoritățile competente pentru 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 statelor membre (...).

În aceste cazuri, pentru această prelucrare se aplică Regulamentul UE/XXX, cu excepția cazului în care prelucrarea este efectuată în cadrul unei activități care nu intră sub incidența dreptului Uniunii.

(1a) În cazul în care autoritățile competente sunt abilitate prin dreptul unui stat membru să îndeplinească sarcini în alte scopuri decât cele stabilite la articolul 1 alineatul (1), Regulamentul UE/XXX se aplică pentru prelucrarea în astfel de scopuri, inclusiv în scopuri de arhivare (...) în interes public sau (...) în scopuri științifice, statistice sau istorice (...), cu excepția cazului în care prelucrarea este efectuată în cadrul unei activități care nu intră sub incidența dreptului Uniunii.

(1b) Statele membre prevăd că, în cazul în care dreptul Uniunii sau dreptul intern aplicabil autorității (...) competente care a transmis datele prevede condiții specifice (...) de prelucrare a datelor cu caracter personal, autoritatea competentă care a transmis datele informează destinatarul cărui îi sunt transmise datele cu privire la aceste condiții și la obligația de a le respecta.

(2) Statele membre prevăd că autoritatea (...) competentă care a transmis datele nu aplică condițiile prevăzute la alineatul (1b) destinatarilor din alte state membre sau agențiilor, oficiilor și organismelor instituite în conformitate cu titlul V capitolele IV și V din Tratatul privind funcționarea Uniunii Europene, altele decât cele aplicabile transmiterii (...) similare de date în statul membru al autorității competente care a transmis datele.

(2a) (...)

Articolul 8

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, apartenența la sindicate și prelucrarea datelor genetice sau a datelor privind sănătatea sau viața sexuală este autorizată doar în cazul în care este strict necesar și sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei vizate și numai în cazul în care:

(a) (...) este autorizată de dreptul Uniunii sau de dreptul intern al statului membru (...) sau (...);

- (b) (...) protejează interesele vitale ale persoanei vizate sau ale unei alte persoane sau
(...)
(c) prelucrarea se referă la date care sunt făcute publice în mod manifest de persoana vizată.

Articolul 9

(...) Procesul decizional automatizat (...)

[...] Statele membre se asigură că o decizie bazată 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 al statului membru 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. (...).

(1a) (...)

CAPITOLUL III

DREPTURILE PERSOANEI VIZATE

Articolul 10

Comunicare și modalități de exercitare a drepturilor persoanei vizate

(1) (...)

(2) Statele membre prevăd dispoziții potrivit cărora operatorul (...) ia (...) toate măsurile rezonabile pentru a furniza persoanei vizate orice informații menționate la articolul 10a (...) și orice comunicări în temeiul articolelor 12, 15 și 29 referitoare la prelucrarea datelor cu caracter personal, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Informațiile se furnizează prin orice mijloace adecvate, inclusiv (...) pe cale electronică (...) Ca regulă generală operatorul furnizează informațiile în același format în care a fost primită cererea (...).

(3) Statele membre prevăd dispoziții potrivit cărora operatorul ia toate măsurile rezonabile (...) pentru facilitarea exercitării drepturilor persoanelor vizate în conformitate cu articolele 12 și 15 (...).

(4) (...)

(5) Statele membre prevăd dispoziții potrivit cărora informațiile furnizate în conformitate cu articolul 10a (...) și orice comunicări în temeiul articolelor 12, 15 și 29 sunt furnizate (...) gratuit. În cazul în care cererile sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, (...) operatorul poate refuza să le trateze. În acest caz, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii (...).

(5a) În cazul în care operatorul are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea menționată la articolele (...) 12 și 15, acesta poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

Articolul 10a

Informații pentru persoana vizată

1. Statele membre prevăd dispoziții potrivit cărora operatorul pune la dispoziția persoanelor vizate cel puțin următoarele informații:
 - (a) identitatea și datele de contact ale operatorului; operatorul include, de asemenea, datele de contact ale responsabilului cu protecția datelor, dacă acesta există;
 - (b) *scopurile în care sunt prelucrate datele cu caracter personal;*
 - (c) (...)
 - (d) (...)
 - (e) *dreptul de a depune o plângere în fața (...) unei autorități de supraveghere (...).*
2. Statele membre prevăd în dreptul lor (...) că operatorul furnizează persoanei vizate informații în plus față de cele menționate la alineatul (1), (...) în cazul în care acest lucru este necesar (...) într-un anumit caz și pentru a permite exercitarea drepturilor sale, în special (...) atunci când datele sunt colectate fără știrea persoanei respective.
3. Statele membre pot adopta măsuri legislative de amânare, restricționare sau omitere a dispoziției privind informațiile pentru persoana vizată 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 interesele legitime ale persoanei vizate:
 - (a) pentru evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau juridice;
 - (b) pentru a nu prejudicia prevenirea, identificarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;
 - (c) pentru garantarea siguranței publice;
 - (d) pentru garantarea securității naționale;
 - (e) pentru garantarea drepturilor și libertăților celorlalți.

Articolul 11

Informații care trebuie furnizate în cazul în care datele sunt colectate de la persoana vizată

(...)

Articolul 11a

Informații care trebuie furnizate în cazul în care datele nu au fost obținute de la persoana vizată

(...)

Articolul 11b

Limitarea dreptului de acces la informații

(...)

Articolul 12

Dreptul de acces al persoanei vizate

(1) Sub rezerva articolului 13, statele membre prevăd dispoziții privind dreptul persoanei vizate de a obține din partea operatorului, la intervale rezonabile și în mod gratuit, o confirmare a prelucrării sau nu a datelor cu caracter personal care o privesc și, în cazul în care aceste date cu caracter personal sunt prelucrate, de a obține accesul la datele respective și la următoarele informații prin mijloace adecvate:

- (a) scopurile prelucrării;
- (b) (...)
- (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) (...) perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau normele aplicabile la calcularea acestei perioade;
- (e) existența dreptului de a solicita de la operator rectificarea, ștergerea sau restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată;
- (f) dreptul de a depune o plângere (...) la o autoritate de supraveghere (...);

- (g) comunicarea datelor cu caracter personal care sunt în curs de prelucrare și, dacă este necesar, a oricărei informații disponibile cu privire la originea datelor.
- (h) (...)
- (1a) (...)
- (2) (...)
- (2a) (...)

Articolul 13

Limitarea dreptului de acces

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

- (a) pentru evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau juridice;
- (b) pentru a nu prejudicia prevenirea, identificarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;
- (c) pentru garantarea siguranței publice;
- (d) pentru garantarea securității naționale;
- (e) pentru garantarea drepturilor și libertăților celorlalți.

(2) (...)

(3) În cazurile prevăzute la alineatul (1) (...), statele membre prevăd dispoziții potrivit cărora operatorul informează în scris persoana vizată cu privire la refuzarea sau limitarea accesului (...) și la motivele refuzului sau ale limitării. (...) Această dispoziție nu se aplică (...) în cazul în care furnizarea acestor informații ar contraveni unuia dintre obiectivele de la alineatul (1). Statele membre prevăd dispoziții potrivit cărora operatorul informează persoana vizată cu privire la posibilitățile de a depune o plângere (...) la (...) autoritatea de supraveghere sau de a introduce o cale de atac judiciară.

(4) Statele membre se asigură că operatorul justifică (...) motivele de fapt și de drept care stau la baza deciziei.

Articolul 14

Modalități suplimentare de exercitare a dreptului de acces

(...)

Articolul 15

Dreptul la rectificare, la ștergere și la restricționarea prelucrării

(1) Statele membre prevăd dispoziții potrivit cărora 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 prelucrării în cauză, (...) statele membre prevăd ca persoana vizată să aibă dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

(1a) Statele membre prevăd dispoziții potrivit cărora operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate, iar persoana vizată are dreptul de a obține de la operator ștergerea datelor cu caracter personal (...) care o privesc, fără întârzieri nejustificate, în cazul în care prelucrarea nu respectă dispozițiile adoptate în conformitate cu articolele 4, (...) 7 și 8 din prezenta directivă, sau în cazul în care datele trebuie șterse pentru respectarea unei obligații legale care îi revine operatorului.

(1b) (...) În cazul în care exactitatea unor date cu caracter personal este contestată de persoana vizată, iar exactitatea sau inexactitatea datelor respective nu se poate stabili cu certitudine, se poate restricționa prelucrarea acelor date.

(2) Statele membre prevăd dispoziții potrivit cărora operatorul informează în scris persoana vizată cu privire la orice refuz de rectificare, ștergere sau restricționare a prelucrării și la motivele refuzului. (...) Statele membre pot adopta măsuri legislative care limitează, integral sau parțial, obligația de a furniza astfel de informații (...) (...) în măsura în care o astfel de limitare constituie o măsură necesară și proporțională într-o societate democratică, ținându-se seama în mod corespunzător de interesele legitime ale persoanei fizice vizate:

(a) pentru evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau juridice;

(b) pentru a nu prejudicia prevenirea, identificarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;

(c) pentru garantarea siguranței publice;

(d) pentru garantarea securității naționale;

(e) pentru garantarea drepturilor și libertăților celorlalți.

Statele membre prevăd dispoziții potrivit cărora operatorul informează persoana vizată cu privire la posibilitățile de a depune o plângere (...) la (...) autoritatea de supraveghere sau de a introduce o cale de atac judiciară.

(3) Statele membre prevăd dispoziții potrivit cărora, în cazurile menționate la alineatele (1), (1a) și (1b), operatorul informează destinatarii și că destinatarii rectifică, șterg sau restricționează prelucrarea datelor cu caracter personal aflate sub responsabilitatea lor.

Articolul 15a

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

(1) (...)

(1a) În cazurile menționate la articolul 13 alineatul (3) și la articolul 15 alineatul (2), statele membre pot adopta măsuri prin care se prevede că drepturile persoanei vizate pot fi, de asemenea, exercitate prin intermediul autorității de supraveghere competente.

(2) (...)

(3) Atunci când este exercitat dreptul menționat la alineatul (1a), autoritatea de supraveghere informează persoana vizată cel puțin că au fost realizate toate verificările necesare sau o revizuire de către autoritatea de supraveghere. (...)

Articolul 16

Dreptul la ștergere

(...)

Articolul 17

Drepturile persoanelor vizate în cadrul investigațiilor și procedurilor penale

Statele membre pot să prevadă dispoziții potrivit cărora exercitarea drepturilor (...) menționate la articolele (...) 10a, 12 și 15 se efectuează 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 prelucrate pe parcursul investigațiilor și procedurilor penale.

CAPITOLUL IV
OPERATORUL ȘI PERSOANA ÎMPUTERNICITĂ DE OPERATOR
SECȚIUNEA 1
OBLIGAȚII GENERALE

Articolul 18

Obligațiile operatorului

(1) Statele membre prevăd dispoziții potrivit cărora, ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de probabilitatea de a se materializa și de gravitatea riscului la adresa drepturilor și libertăților persoanelor fizice, operatorul pune în aplicare măsuri adecvate și este în măsură să demonstreze că prelucrarea datelor cu caracter personal se efectuează în conformitate cu dispozițiile adoptate în temeiul prezentei directive.

(1a) 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 care specifică aplicarea normelor naționale de protecție a datelor (...) care pun în aplicare prezenta directivă.

(2) (...)

Articolul 19

Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

(1) Având în vedere tehnologia disponibilă și costul punerii în aplicare și ținând seama (...) de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de probabilitatea de materializare și de gravitatea riscului la adresa drepturilor și libertăților persoanelor fizice, statele membre prevăd dispoziții potrivit cărora operatorii pun în aplicare (...) măsuri tehnice și organizatorice (...) adecvate pentru activitatea de prelucrare desfășurată și pentru obiectivele acesteia, cum ar fi pseudonimizarea, în așa fel încât prelucrarea să îndeplinească cerințele dispozițiilor adoptate în temeiul prezentei directive și să protejeze drepturile persoanelor vizate.

(2) Statele membre prevăd dispoziții potrivit cărora operatorul pune în aplicare măsuri adecvate (...), în special în cazul prelucrării automate, 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; acest lucru se aplică volumului de (...) date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor.

Articolul 20

Operatori asociați

(1) Statele membre prevăd dispoziții potrivit cărora în cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare a datelor cu caracter personal, aceștia sunt operatori asociați. Ei stabilesc într-un mod transparent (...) responsabilitățile fiecăruia în ceea ce privește respectarea dispozițiilor adoptate în temeiul prezentei directive, în special în ceea ce privește (...) exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute la articolul 10a (...), cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite de dreptul Uniunii sau al unui stat membru care se aplică operatorilor. (...) Statele membre pot desemna care dintre operatorii asociați poate acționa ca punct unic de contact pentru exercitarea de către persoanele vizate a drepturilor lor.

(1a) (...) Fără a se aduce atingere articolului 17, statele membre (...) pot prevedea dispoziții potrivit cărora persoana vizată își poate exercita drepturile în conformitate cu dispozițiile adoptate în temeiul prezentei directive cu privire la și în raport cu fiecare dintre operatori.

Articolul 21

Persoana împuternicită de operator

1. Statele membre prevăd dispoziții potrivit cărora operatorul utilizează numai (...) persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a măsurilor tehnice și organizatorice adecvate (...), astfel încât prelucrarea să respecte cerințele dispozițiilor adoptate în temeiul prezentei directive (...).

(1a) Statele membre prevăd dispoziții potrivit cărora persoana împuternicită de operator nu recrutează o altă persoană împuternicită fără a primi în prealabil consimțământul scris, specific sau general, al operatorului. În acest ultim caz, persoana împuternicită de operator ar trebui să informeze întotdeauna operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel operatorului posibilitatea de a formula obiecții față de aceste modificări.

(2) Statele membre prevăd dispoziții potrivit cărora efectuarea prelucrării de către o persoană împuternicită de un operator este reglementată printr-un act juridic în conformitate cu dreptul Uniunii sau al unui stat membru, inclusiv printr-un contract, care creează obligații pentru persoana împuternicită de operator în raport cu operatorul, care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate, drepturile operatorului și care prevede în special că respectiva persoană împuternicită acționează numai pe baza instrucțiunilor primite de la operator (...).

(3) (...)

Articolul 22

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

(...)

Articolul 23

Evidențe ale categoriilor de activități de prelucrare a datelor cu caracter personal

(1) Statele membre prevăd dispoziții potrivit cărora operatorul (...) menține o evidență a tuturor categoriilor de activități de prelucrare a datelor cu caracter personal (...) (...) aflate în responsabilitatea sa. Aceste evidențe cuprind (...) următoarele informații:

- (a) numele și datele de contact ale operatorului și ale oricărui operator asociat (...) (...), precum și ale responsabilului cu protecția datelor, dacă aceștia există;
- (b) scopurile prelucrării;
- (c) (...) categoriile de destinatari cărora le-au fost sau le vor fi dezvăluite datele cu caracter personal, în special destinatarii din țări terțe;
- (ca) o descriere a categoriilor de date cu caracter personal referitoare la (...) persoanele vizate;
- (d) acolo unde este cazul, categoriile de transferuri de date cu caracter personal către țări terțe sau organizații internaționale (...);
- (e) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
- (f) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 27 alineatul (1).

(2) (...)

(2a) Statele membre prevăd dispoziții potrivit cărora fiecare persoană împuternicită de operator păstrează evidențe ale tuturor categoriilor de activități de prelucrare a datelor cu caracter personal 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); (...);
- (b) numele și datele de contact ale responsabilului cu protecția datelor, dacă acesta există;
- (c) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;
- (d) (...)
- (e) (...)
- (f) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 27 alineatul (1).

(2b) Evidențele prevăzute la alineatele (1) și (2a) se păstrează în scris, inclusiv în formă electronică sau în altă formă ilizibilă, care să poată fi convertită într-o formă lizibilă.

(3) *La cerere*, operatorul și persoana împuternicită de acesta pun evidențele la dispoziția autorității de supraveghere.

Articolul 24

Înregistrarea

(1) Cu excepția situației în care se dovedește a fi imposibil sau necesită un efort disproporționat, statele membre se asigură că (...) se înregistrează cel puțin următoarele operațiuni de prelucrare din cadrul sistemelor de prelucrare automată: colectarea, modificarea, consultarea, divulgarea, combinarea sau ștergerea. Înregistrările consultărilor și ale divulgărilor indică (...) scopul, data și momentul acestor operațiuni și, în măsura în care este posibil, identificarea persoanei care a consultat sau a divulgat date cu caracter personal.

(2) Înregistrările sunt utilizate (...) pentru (...) verificarea legalității prelucrării datelor, monitorizare proprie și asigurarea integrității și securității datelor.

Articolul 25

Cooperarea cu autoritatea de supraveghere

(...)

Articolul 26

Consultarea prealabilă a autorității de supraveghere

(1) Statele membre se asigură că operatorul sau persoana împuternicită 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) urmează a fi prelucrate categorii speciale de date cu caracter personal, menționate la articolul 8;
- (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.

(1a) (...) Statele membre se asigură că autoritatea de supraveghere este consultată în cadrul procesului de pregătire a propunerilor de măsuri legislative sau de reglementare care prevăd prelucrarea datelor cu caracter personal menționată la alineatul (1).

(2) Statele membre pot prevedea dispoziții potrivit cărora autoritatea de supraveghere stabilește o listă a operațiunilor de prelucrare care fac obiectul consultării prealabile, în conformitate cu alineatul (1).

(3) Statele membre prevăd dispoziții potrivit cărora, în cazul în care autoritatea de supraveghere consideră că prelucrarea preconizată, menționată la alineatul (1), nu este în conformitate cu dispozițiile adoptate în temeiul prezentei directive, în special în cazul în care riscurile nu sunt suficient identificate sau atenuate, autoritatea de supraveghere, în termen de maxim 6 săptămâni de la depunerea cererii de consultare, oferă consiliere operatorului de date, în scris. Această perioadă poate fi prelungită cu o lună, ținându-se seama de complexitatea prelucrării preconizate. În cazul în care se aplică prelungirea, operatorul sau persoana împuternicită de operator este informată cu privire la motivele amânării, în termen de o lună de la primirea cererii.

SECȚIUNEA 2

SECURITATEA DATELOR

Articolul 27

Securitatea prelucrării

- (1) Având în vedere tehnologia disponibilă și costurile punerii în aplicare și ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de probabilitatea de materializare și gravitatea riscului la adresa drepturilor și libertăților persoanelor fizice, statele membre prevăd dispoziții potrivit cărora operatorul și persoana împuternicită de acesta pun în aplicare măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc (...).
- (2) În ceea ce privește prelucrarea automată a datelor, fiecare stat membru prevede dispoziții potrivit cărora operatorul sau persoana împuternicită de operator, în urma unei evaluări a riscurilor, pune în aplicare măsuri menite:
- (a) să împiedice accesul persoanelor neautorizate la echipamentele de prelucrare a datelor utilizate pentru prelucrarea datelor cu caracter personal (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 și inspectarea, modificarea sau ștergerea neautorizată a datelor cu caracter personal stocate (controlul stocării);
 - (d) să împiedice utilizarea sistemelor de prelucrare automată a datelor 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 a datelor au acces numai la datele 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 a datelor, momentul introducerii acestora 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);
- (3) (...)

Articolul 28

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

- (1) Statele membre prevăd dispoziții potrivit cărora în cazul în care are loc o încălcare a securității datelor cu caracter personal care este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor vizate, (...) operatorul notifică încălcarea securității datelor cu caracter personal autorității de supraveghere fără întârzieri nejustificate (...) și, în cazul în care este posibil, în termen de cel mult 72 de ore după ce a luat cunoștință de aceasta (...). Notificarea autorității de supraveghere este însoțită de o explicație motivată în cazul în care nu are loc în termen de 72 de ore.
- (1a) Notificarea menționată la alineatul (1) nu este necesară dacă informarea persoanei vizate nu este necesară în conformitate cu articolul 29 alineatul (3) literele (a) și (b). (...)
- (2) Persoana împuternicită de operator alertează și informează operatorul fără întârzieri nejustificate după ce a luat cunoștință de o încălcare a securității datelor cu caracter personal.
- (3) Notificarea menționată la alineatul (1) trebuie, cel puțin:
 - (a) să descrie natura încălcării securității datelor cu caracter personal;
 - (b) să comunice identitatea și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
 - (c) (...)
 - (d) să descrie consecințele probabile, identificate de operator, ale încălcării securității datelor cu caracter personal;

(e) să descrie măsurile luate sau propuse de operator pentru a remedia problema încălcării securității datelor cu caracter personal și

(f) dacă este cazul, să indice măsuri de atenuare a eventualelor efecte negative ale încălcării respective.

(3a) În cazul în care și în măsura în care furnizarea informațiilor menționate la alineatul (3) literele (d), (e) și (f) în același timp cu informațiile menționate la alineatul (3) literele (a) și (b) nu este posibilă, operatorul furnizează informațiile respective fără întârzieri nejustificate.

(4) Statele membre prevăd dispoziții potrivit cărora 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, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație trebuie să permită autorității de supraveghere să verifice conformitatea cu prezentul articol. (...)

(4a) Sub rezerva alineatului (1a), statele membre prevăd dispoziții potrivit cărora, 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.

(5) (...)
(6) (...)

Articolul 29

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

(1) Sub rezerva dispozițiilor din prezentul articol alineatele (3) și (4), statele membre prevăd dispoziții potrivit cărora, în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților (...) persoanei vizate, (...) 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), se include o descriere a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile prevăzute la articolul 28 alineatul (3) literele (b), (e) și (f).

(3) Informarea (...) persoanei vizate, menționată la alineatul (1), nu este necesară în cazul în care:

- (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 devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea sau
- (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 sau
- (c) aceasta ar necesita un efort disproporționat, în special ca urmare a numărului de cazuri implicate. 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) Informarea persoanei vizate menționată la alineatul (1) poate fi întârziată, restricționată sau omisă din motivele menționate la articolul 10a alineatul (3).

SECȚIUNEA 3

RESPONSABILUL CU PROTECȚIA DATELOR

Articolul 30

Desemnarea responsabilului cu protecția datelor

(1) Statele membre pot să prevadă sau, în cazul în care dreptul Uniunii o impune, (...) prevăd dispoziții potrivit cărora operatorul sau persoana împuternicită de operator desemnează un responsabil cu protecția datelor.

(2) Responsabilul cu protecția datelor este desemnat pe baza calităților 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 32, în special în absența oricărui conflict de interese.

(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 prevăd dispoziții potrivit cărora operatorul sau 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.*

(5) *Operatorul sau persoana împuternicită de operator se asigură că responsabilul cu protecția datelor are la dispoziție mijloacele pentru îndeplinirea (...) cu eficacitate a sarcinilor menționate la articolul 32 și că poate acționa în mod independent în ceea ce privește exercitarea sarcinilor sale (...).*

Articolul 31

Funcția responsabilului cu protecția datelor

(...)

Articolul 32

Sarcinile responsabilului cu protecția datelor

Statele membre prevăd dispoziții potrivit cărora operatorul sau persoana împuternicită de operator încredințează responsabilului cu protecția datelor (...) următoarele sarcini:

- (a) informarea și consilierea operatorului sau a persoanei împuternicite de operator (...) cu privire la obligațiile care le revin în conformitate cu dispozițiile adoptate în temeiul prezentei directive și al altor dispoziții ale Uniunii sau ale statelor membre referitoare la protecția datelor (...);
- (b) monitorizarea respectării dispozițiilor adoptate în temeiul prezentei directive, a altor dispoziții ale Uniunii sau ale statelor membre 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, sensibilizarea și formarea personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
- (c) (...)
- (d) (...)
- (e) (...)
- (f) (...)
- (g) monitorizarea răspunsurilor la cererile adresate de autoritatea de supraveghere și, în limitele competenței responsabilului cu protecția datelor, cooperarea cu autoritatea de supraveghere, la cererea acesteia sau din propria inițiativă a responsabilului cu protecția datelor;
- (h) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrarea datelor cu caracter personal, inclusiv consultarea prealabilă menționată la articolul 26, precum și, dacă este cazul, consultarea (...) cu privire la orice altă chestiune (...).

CAPITOLUL V

TRANSFERUL DATELOR CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Articolul 33

Principii generale pentru transferurile de date cu caracter personal

- (1) Statele membre prevăd dispoziții potrivit cărora orice transfer de date cu caracter personal de către autoritățile (...) competente (...) către o țară terță sau către o organizație internațională, inclusiv, ulterior, transferul în continuare către o altă țară terță sau organizație internațională, poate avea loc numai dacă:
- (a) transferul este necesar în scopurile stabilite la articolul 1 alineatul (1) și
 - (b) (...)
 - (c) operatorul din țara terță sau organizația internațională este o autoritate competentă în sensul articolului 1 alineatul (1) și
 - (d) 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 și
 - (e) Comisia a decis, în temeiul articolului 34, că țara terță sau organizația internațională în cauză asigură un nivel adecvat de protecție sau, în absența unei decizii privind caracterul adecvat al nivelului de protecție în temeiul articolului 34, în cazul în care se oferă sau există garanții în conformitate cu articolul 35. (...)
- (2) Statele membre prevăd dispoziții potrivit cărora transferurile fără autorizarea prealabilă de către un alt stat membru, în conformitate cu litera (d) sunt permise numai dacă transferul de date cu caracter personal este necesar pentru prevenirea unei amenințări imediate și grave la adresa siguranței 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) Statele membre prevăd că, în lipsa unei decizii privind caracterul adecvat în temeiul articolului 34 sau a unor garanții adecvate în conformitate cu articolul 35, un transfer poate avea loc doar în cazul în care se aplică derogări pentru situații specifice în temeiul articolului 36 și se respectă condițiile descrise la prezentul articol alineatul (1) literele (a), (c) și (d) și, după caz, (...) alineatul (2).

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

- (1) Statele membre prevăd dispoziții potrivit cărora un transfer de date cu caracter personal către o țară terță ori un teritoriu ori unul sau mai multe sectoare specificate dintr-o țară terță sau către o organizație internațională poate avea loc în cazul în care Comisia a decis, în conformitate cu articolul 41 din Regulamentul UE/XXX sau în conformitate cu alineatul (3) din prezentul articol, că țara terță sau un teritoriu sau un sector specificat din acea țară terță sau organizația internațională respectivă asigură un nivel adecvat de protecție. Transferurile realizate în aceste condiții nu necesită autorizări speciale.
- (2) În cazul în care nu se aplică nicio decizie adoptată în conformitate cu articolul 41 din Regulamentul UE/XXX (...), Comisia evaluează caracterul adecvat al nivelului de protecție, ținând seama în special de următoarele elemente:
- (a) statul de drept, respectarea drepturilor omului și a libertăților fundamentale, legislația relevantă, atât generală, cât și sectorială, normele de protecție a datelor (...) inclusiv privind securitatea publică, apărarea, securitatea națională și dreptul penal, precum 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 respectivă sau de organizația internațională respectivă, precum și existența unor drepturi efective și exercitabile ale persoanelor vizate și a unor căi de atac administrative și judiciare efective 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 jurisdicția 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 Uniune și din statele membre; și
 - (c) angajamentele internaționale la care a aderat țara terță sau organizația internațională în cauză sau alte obligații care decurg din participarea acesteia la sisteme multilaterale sau regionale, mai ales în domeniul protecției datelor cu caracter personal.

- (2a) Comitetul european pentru protecția datelor emite un aviz către Comisie 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, o organizație internațională sau un sector specificat nu mai asigură un nivel de protecție adecvat.
- (3) Comisia, după ce evaluează caracterul adecvat al nivelului de protecție, poate decide, în cadrul domeniului de aplicare al prezentei directive, că o țară terță, un teritoriu sau unul sau mai multe sectoare specificate din acea țară terță sau o organizație internațională asigură un nivel de protecție adecvat în sensul alineatului (2). Actul de punere în aplicare menționează aplicarea teritorială și sectorială și, după caz, identifică autoritatea (autoritățile) de supraveghere menționată (menționate) la alineatul (2) litera (b). Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 57 alineatul (2).
- (4) (...)
- (4a) Comisia monitorizează funcționarea deciziilor adoptate în temeiul alineatului (3)(...).
- (5) Comisia poate decide, în cadrul domeniului de aplicare al prezentei directive, 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) și poate, dacă este necesar, să abroge, să modifice sau să suspende decizia respectivă fără efect retroactiv. Actele (...) de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 57 alineatul (2) sau, în cazuri de extremă urgență, în conformitate cu procedura menționată la articolul 57 alineatul (3).
- (5a) (...) *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).*
- (6) Statele membre se asigură că, în cazul în care este luată o decizie în temeiul alineatului (5), respectiva decizie (...) nu aduce atingere transferurilor de date cu caracter personal către țara terță, teritoriul sau sectorul specificat din acea țară terță sau către organizația internațională în cauză în conformitate cu articolele 35 și 36 (...).

- (7) Comisia publică în *Jurnalul Oficial al Uniunii Europene* o listă a țărilor terțe, a teritoriilor și sectoarelor specificate din țările terțe respective și a organizațiilor internaționale cu privire la care au fost luate decizii în temeiul alineatelor (3) (...) și (5).
- (8) (...)

Articolul 35

Transferuri în baza unor garanții adecvate

- (1) (...) În absența unei decizii luate în conformitate cu articolul 34 alineatul (3), statele membre prevăd dispoziții potrivit cărora (...) poate avea loc un transfer de date cu caracter personal către o țară terță sau către o organizație internațională în cazul în care:
- (a) s-au prezentat garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal printr-un instrument cu caracter juridic obligatoriu (...); sau
 - (b) operatorul (...) a evaluat toate circumstanțele aferente transferului de date cu caracter personal și a concluzionat că există garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal. Respectiva evaluare poate ține seama de acordurile de cooperare existente între Europol și/sau Eurojust și țări terțe care permit schimbul de date cu caracter personal.
- (2) (...)

Articolul 36

Derogări pentru (...) situații specifice

- (1) (...) În absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 34 sau a unor garanții adecvate în conformitate cu articolul 35, statele membre prevăd dispoziții potrivit cărora 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:
- (a) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane sau
 - (b) transferul este necesar pentru protejarea intereselor legitime ale persoanei vizate (...) în cazul în care dreptul statului membru care transferă datele cu caracter personal prevede acest lucru; sau
 - (c) transferul datelor este necesar pentru prevenirea unei amenințări imediate și grave la adresa siguranței publice a unui stat membru sau a unei țări terțe; sau

- (d) transferul este necesar în cazuri individuale în scopurile stabilite la articolul 1 alineatul (1); sau
 - (e) transferul este necesar 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 stabilește că (...) drepturile și libertățile fundamentale (...) ale persoanei vizate în cauză prevalează asupra interesului public (...) în cazul transferului prevăzut la literele (d) și (e) de la alineatul (1).

Articolul 36a

(...)

Articolul 36aa

Transferul de date cu caracter personal către (...) destinatari (...) stabiliți în țări terțe

1. Prin derogare de la articolul 33 alineatul (1) litera (c) și fără a aduce atingere niciunui acord internațional la care se face referire la alineatul (2), dreptul Uniunii sau cel al statelor membre poate prevedea că autoritățile competente pot, în cazuri individuale și (...) specifice, transfera date cu caracter personal direct (...) destinatarilor (...) stabiliți în țări terțe numai în cazul în care celelalte dispoziții ale prezentei directive sunt respectate și sunt îndeplinite următoarele condiții:
 - (a) transferul este (...) strict necesar pentru executarea unei sarcini de către autoritatea competentă, astfel cum este prevăzut de dreptul Uniunii sau cel al statului membru pentru scopurile (...) prevăzute la articolul 1 alineatul (1); și
 - (b) (...)
 - (c) (...)
 - (d) autoritatea competentă 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.
- (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. (...)

Articolul 37

Condiții specifice pentru transferul datelor cu caracter personal

Articolul 38

Cooperarea internațională în domeniul protecției datelor cu caracter personal

(...)

CAPITOLUL VI
AUTORITĂȚI DE SUPRAVEGHERE INDEPENDENTE

SECȚIUNEA 1

STATUTUL INDEPENDENT

Articolul 39

Autoritatea de supraveghere

- (1) Fiecare stat membru prevede dispoziții potrivit cărora una sau mai multe autorități publice independente sunt responsabile cu monitorizarea aplicării dispozițiilor adoptate în temeiul prezentei directive.
- (1a) 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.
- (2) Statele membre pot prevedea dispoziții potrivit cărora o autoritate de supraveghere instituită (...) în conformitate cu Regulamentul UE/XXX poate fi 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.
- (3) 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 european pentru protecția datelor.

Articolul 40

Independență

- (1) Statele membre se asigură că fiecare autoritate de supraveghere beneficiază de independență deplină în îndeplinirea sarcinilor și exercitarea competențelor care îi sunt încredințate.
- (2) (...) Statele membre prevăd dispoziții potrivit cărora membrul sau (...) membrii (...) fiecărei autorități de supraveghere, în cadrul îndeplinirii sarcinilor și al exercitării competențelor sale (lor) în conformitate cu prezenta directivă, 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) (...)
- (4) (...)

- (5) (...) Statele membre 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 competențelor sale în mod eficace, inclusiv a celor care urmează să fie realizate în contextul asistenței reciproce, al cooperării și al participării active în cadrul Comitetului european pentru protecția datelor.
- (6) (...) Statele membre se asigură că fiecare autoritate de supraveghere trebuie să dispună de personal propriu, care (...) se află sub conducerea membrului sau (...) membrilor autorității de supraveghere.
- (7) Statele membre se asigură că fiecare autoritate de supraveghere face obiectul unui control financiar care nu aduce atingere independenței sale. Statele membre se asigură că fiecare autoritate de supraveghere dispune de bugete publice anuale distincte, care pot face parte din bugetul general de stat sau național.

Articolul 41

Condiții generale aplicabile membrilor autorității de supraveghere

- (1) Statele membre prevăd dispoziții potrivit cărora membrul sau (...) membrii fiecărei autorități de supraveghere trebuie numit (numiți) fie de parlament și/sau de guvern, fie de șeful statului membru în cauză sau de un organism independent împuternicit prin dreptul statului membru să facă numirea prin intermediul unei proceduri transparente.
- (2) Membrul sau membrii în cauză dispune (dispun) de calificările, experiența și competențele necesare pentru îndeplinirea atribuțiilor și exercitarea competențelor sale (lor).
- (3) (...) Atribuțiile unui membru încetează în cazul expirării mandatului, în cazul demisiei sau destituirii în conformitate cu (...) dreptul statului membru (...).(...)
- (4) (...)
- (5) (...)

Articolul 42

Norme privind instituirea autorității de supraveghere

- (1) Statele membre prevăd în dreptul lor următoarele:
- (a) instituirea fiecărei autorități de supraveghere (...);
 - (b) (...) calificările (...) necesare pentru îndeplinirea atribuțiilor care le revin membrilor autorității de supraveghere;
 - (c) normele și procedurile pentru numirea membrului sau membrilor fiecărei autorități de supraveghere (...);
 - (d) durata mandatului membrului sau membrilor fiecărei autorități de supraveghere, care nu este mai mică de patru ani, cu excepția primului mandat după intrarea în vigoare a prezentei directive, din care o parte poate fi pe o perioadă mai scurtă în cazul în care acest lucru este necesar pentru a proteja independența autorității de supraveghere printr-o procedură de numiri eşalonate;
 - (e) dacă și de câte ori este eligibil pentru reînnoire mandatul membrului sau membrilor fiecărei autorități de supraveghere;
 - (f) condițiile (...) care reglementează obligatiile membrului sau membrilor și ale personalului fiecărei autorități de supraveghere, interdicții privind acțiunile și ocupațiile incompatibile cu acestea în cursul mandatului și după încetarea acestuia, precum și normele care reglementează încetarea contractului de angajare.
 - (g) (...)

(1a) Statele membre prevăd că membrul sau membrii și personalul fiecărei autorități de supraveghere au obligația, în conformitate cu dreptul Uniunii sau al statului membru, 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 atribuțiilor (...) sau al exercitării competențelor lor.

Articolul 43

Secretul profesional

(...)

SECȚIUNEA 2

SARCINI ȘI COMPETENȚE

Articolul 44

Abilitări

- (1) Statele membre prevăd dispoziții potrivit cărora fiecare autoritate de supraveghere este abilitată pe teritoriul statului membru de care aparține să îndeplinească sarcinile și să exercite (...) competențele care îi sunt conferite în conformitate cu prezenta directivă. (...)
- (2) Statele membre prevăd dispoziții potrivit cărora autoritatea de supraveghere nu are competența de a supraveghea operațiunile de prelucrare ale (...) instanțelor atunci când acestea acționează în exercițiul funcției lor jurisdicționale. Statele membre pot prevedea dispoziții potrivit cărora autoritatea de supraveghere nu are competența de a supraveghea operațiunile de prelucrare ale altor autorități judiciare independente atunci când acestea acționează în calitatea lor judiciară.

Articolul 45

Sarcini

- (1) Statele membre prevăd dispoziții potrivit cărora fiecare autoritate de supraveghere, pe teritoriul său:
 - (a) monitorizează și asigură aplicarea dispozițiilor adoptate în temeiul prezentei directive și al măsurilor de punere în aplicare aferente acesteia;
 - (aa) promovează acțiuni de sensibilizare și de înțelegere în rândul publicului a riscurilor, normelor, garanțiilor și drepturilor în materie de prelucrare a datelor cu caracter personal;
 - (ab) 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 vizate în ceea ce privește prelucrarea datelor cu caracter personal;
 - (ac) promovează acțiuni de sensibilizare a operatorilor și a persoanelor împuternicite de aceștia cu privire la obligațiile care le revin în conformitate cu dispozițiile adoptate în temeiul prezentei directive;
 - (ad) la cerere, furnizează informații oricărei persoane vizate în legătură cu exercitarea drepturilor sale în conformitate cu dispozițiile adoptate în temeiul prezentei directive și, dacă este cazul, cooperează cu autoritățile de supraveghere din alte state membre în acest scop;

- (b) tratează plângerile depuse de o persoană vizată, un organism, o organizație sau o asociație care reprezintă o persoană vizată și care este împuternicită în mod corespunzător de aceasta, (...), și investighează într-o măsură adecvată obiectul plângerii și informează persoana vizată sau organismul, organizația sau asociația în cauză cu privire la evoluția și rezultatul investigației, într-un termen rezonabil, în special când este necesară efectuarea unei investigații mai amănunțite sau coordonarea cu o altă autoritate de supraveghere;
 - (c) verifică legalitatea prelucrării datelor în conformitate cu articolul 15a (...) și informează persoana vizată, într-un termen rezonabil, cu privire la rezultatul verificării în temeiul articolului 15a alineatul (3) sau la motivele pentru care nu a avut loc verificarea;
 - (d) cooperează, inclusiv prin schimb de informații, cu alte autorități de supraveghere și își oferă asistență reciprocă pentru a asigura consecvența aplicării și respectării dispozițiilor adoptate în temeiul prezentei directive;
 - (e) desfășoară investigații privind aplicarea dispozițiilor adoptate în temeiul prezentei directive (...), inclusiv pe baza unor informații primite de la o altă autoritate de supraveghere sau o altă autoritate publică, (...) (...);
 - (f) monitorizează evoluțiile relevante, în măsura în care acestea au impact asupra protecției datelor cu caracter personal, în special evoluția tehnologiilor informațiilor și comunicațiilor (...);
 - (g) (...)
 - (h) oferă consiliere cu privire la operațiunile de prelucrare menționate la articolul 26;
 - (i) contribuie la activitățile Comitetului european pentru protecția datelor.
- (2) (...)
- (3) (...)
- (4) (...)
- (5) Statele membre prevăd dispoziții potrivit cărora îndeplinirea sarcinilor fiecărei autorități de supraveghere este gratuită pentru persoana vizată și pentru responsabilul cu protecția datelor, dacă acesta există.
- (6) Statele membre prevăd dispoziții potrivit cărora(...) în cazul în care cererile sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, autoritatea de supraveghere poate refuza să le trateze. Sarcina de a demonstra caracterul evident nefondat sau excesiv al cererii revine autorității de supraveghere.

Competențe

(1) Fiecare stat membru prevede în dreptul său dispoziții care conferă autorității sale de supraveghere (...) competențe de investigare efective, (...) 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;

(1a) Fiecare stat membru prevede în dreptul său dispoziții care conferă (...) autorității sale de supraveghere 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 prevăzute să încalce dispozițiile adoptate în temeiul prezentei directive;

(b) (...)

(c) (...)

(d) 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, restricționarea sau ștergerea datelor, în conformitate cu articolul 15;

(e) de a impune o limitare temporară sau definitivă asupra prelucrării.

(f) (...)

(1b) Fiecare stat membru prevede în dreptul său dispoziții care conferă autorității sale de supraveghere competențele de consultare efective (...) de a oferi consiliere operatorului în conformitate cu procedura de consultare prealabilă menționată la articolul 26 și 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.

(2) Exercitarea competențelor conferite autorității de supraveghere în temeiul prezentului articol face obiectul unor garanții adecvate, inclusiv căi de atac judiciare eficace și procese echitabile, prevăzute în dreptul Uniunii și al statelor membre în conformitate cu Carta drepturilor fundamentale a Uniunii Europene.

- (3) Fiecare stat membru prevede în dreptul său dispoziții care conferă autorității sale de supraveghere 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 47

Raport de activitate

Statele membre prevăd dispoziții potrivit cărora fiecare autoritate de supraveghere trebuie să întocmească un raport anual cu privire la activitățile sale. Raportul se transmite parlamentului național, guvernului și altor autorități desemnate de legislația națională. Acesta se pune la dispoziția publicului, a Comisiei Europene și a Comitetului european pentru protecția datelor.

CAPITOLUL VII

COOPERAREA

Articolul 48

Asistență reciprocă

- (1) Statele membre prevăd dispoziții potrivit cărora autoritățile de supraveghere își furnizează asistență reciprocă pentru a transpune și a pune în aplicare dispozițiile adoptate în temeiul prezentei directive (...) și instituie măsuri de cooperare eficace între ele. Asistența reciprocă se referă, în special, la cereri de informații și măsuri de control, cum ar fi cereri în vederea efectuării de (...) inspecții și investigații.
- (2) Statele membre prevăd dispoziții conform cărora o autoritate de supraveghere ia toate măsurile corespunzătoare necesare pentru a răspunde cererii unei alte autorități de supraveghere, fără întârzieri nejustificate și cel târziu în termen de o lună de la data primirii cererii. (...)
- (...)
- (2b) Statele membre prevăd dispoziții potrivit cărora o autoritate de supraveghere căreia i se adresează o cerere de asistență nu poate refuza să îi dea curs, 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 contraveni dispozițiilor adoptate în temeiul prezentei directive sau dreptului Uniunii sau al unui stat membru sub incidența căruia intră autoritatea de supraveghere care a primit cererea.
- (3) 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 (2b), autoritatea de supraveghere căreia i s-a adresat cererea explică motivele pentru refuzarea acesteia.
- (3a) Ca regulă, autoritățile de supraveghere furnizează informațiile solicitate de alte autorități de supraveghere prin mijloace electronice. (...)
- (3b) Pentru acțiunile întreprinse în urma unei cereri de asistență reciprocă nu se percepe nicio taxă. Autoritățile de supraveghere pot conveni împreună cu alte autorități de supraveghere asupra unor norme privind compensațiile din partea acestor alte autorități de supraveghere în cazul unor cheltuieli specifice rezultate în urma acordării de asistență reciprocă în situații excepționale.

(3c) Comisia poate specifica 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 Comitetul european pentru protecția datelor. (...) Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 57 alineatul (2).

Articolul 49

Sarcinile Comitetului european pentru protecția datelor

- (1) Comitetul european pentru protecția datelor, instituit prin Regulamentul (UE).../ XXX exercită următoarele sarcini în ceea ce privește prelucrarea care intră sub incidența prezentei directive:
- (a) 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;
 - (b) examinează, *din proprie inițiativă* sau *la cererea unuia dintre membrii săi sau la cererea* Comisiei, orice chestiune referitoare la punerea în aplicare a dispozițiilor adoptate în temeiul prezentei directive și emite orientări, recomandări și bune practici (...) pentru a încuraja aplicarea uniformă a respectivelor dispoziții;
 - (ba) elaborează orientări destinate autorităților de supraveghere, referitoare la aplicarea măsurilor menționate la articolul 46 alineatele (1) și (1b) (...);
 - (c) revizuieste aplicarea practică a orientărilor, recomandărilor și bunelor practici menționate la literele (b) și (ba) (...);
 - (d) transmite Comisiei un aviz privind nivelul de protecție în țările terțe sau organizațiile internaționale;
 - (e) promovează cooperarea și schimbul eficient bilateral și multilateral de informații și practici între autoritățile de supraveghere;
 - (f) promovează programe comune de formare și facilitează schimburile de personal între autoritățile de supraveghere, precum și, după caz, cu autoritățile de supraveghere ale țărilor terțe sau organizațiilor internaționale;
 - (g) promovează 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.
- (2) În cazul în care Comisia consultă Comitetul european pentru protecția datelor, aceasta poate indica un termen limită (...), ținând seama de caracterul urgent al chestiunii.

- (3) Comitetul european pentru protecția datelor își transmite avizele, orientările, recomandările și bunele practici Comisiei și comitetului menționat la articolul 57 alineatul (1) și le publică.
- (4) Comisia informează Comitetul european pentru protecția datelor cu privire la măsurile pe care le-a luat în urma avizelor, orientărilor, recomandărilor și bunelor practici emise de Comitetul european pentru protecția datelor.

CAPITOLUL VIII

CĂI DE ATAC, RĂSPUNDERE ȘI SANCTIUNI

Articolul 50

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 dispun că orice persoană vizată are 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 nu respectă dispozițiile adoptate în temeiul prezentei directive.

(1a) Statele membre adoptă dispoziții care prevăd că, în cazul în care plângerea nu este depusă la autoritatea de supraveghere competentă în temeiul articolul 44 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.

(1b) Statele membre prevăd dispoziții potrivit cărora autoritatea de supraveghere la care s-a depus plângerea oferă asistență suplimentară la cererea persoanei vizate.

(2) (...)

(2a) (...) 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 51.

(3) (...)

Articolul 51

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, statele membre dispun că 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 eficace în cazul în care autoritatea de supraveghere competentă în conformitate cu articolul 44 alineatul (1) nu soluționează plângerea (...) sau nu informează persoana vizată în termen de trei luni sau în orice termen mai scurt prevăzut în dreptul Uniunii sau al statului membru cu privire la progresele sau la soluționarea plângerii depuse în conformitate cu articolul 50.

(3) Statele membre prevăd dispoziții potrivit cărora acțiunile introduse împotriva unei autorități de supraveghere sunt înaintate instanțelor din statul membru în care este stabilită autoritatea de supraveghere.

Articolul 52

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

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 conformitate cu articolul 50, statele membre prevăd dispoziții potrivit cărora persoanele vizate au dreptul la exercitarea unei căi de atac judiciare eficiente, în cazul în care consideră că drepturile de care beneficiază conform dispozițiilor adoptate în temeiul prezentei directive au fost încălcate ca urmare a prelucrării datelor cu caracter personal ale acestora efectuate încălcând dispozițiile respective.

Articolul 53

(...) Reprezentarea persoanelor vizate

[...] În conformitate cu dreptul național procedural, statele membre prevăd dispoziții potrivit cărora persoana vizată are dreptul de a mandata un organism, o organizație sau o asociație, care au fost constituite în mod corespunzător, în conformitate cu dreptul unui stat membru, și ale căror obiective statutare includ protecția 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 50, 51 și 52.

(2) (...)

(3) (...)

Articolul 54

(...) Dreptul la despăgubiri (...)

(1) Statele membre prevăd dispoziții potrivit cărora orice persoană care a suferit (...) prejudicii ca urmare a (...) unei operațiuni de prelucrare nelegale sau a oricărei acțiuni incompatibile cu dispozițiile (...) naționale adoptate în temeiul prezentei directive are dreptul (...) să obțină despăgubiri pentru prejudiciul suferit de la operator sau de la o altă autoritate competentă în temeiul dreptului intern (...).

(2) (...)

(3) (...)

(4) (...)

(5) (...)

Articolul 55

Sancțiuni

Statele membre definesc normele privind sancțiunile aplicabile în cazul încălcării 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 eficace, proporționale și disuasive.

CAPITOLUL IX
(...) ACTE DE PUNERE ÎN APLICARE

Articolul 56

Exercitarea delegării de competențe

(...)

Articolul 57

Procedura comitetului

- (1) Comisia este asistată de comitetul înființat prin articolul 87 din Regulamentul (UE) XXX. Acesta este 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 58

Abrogări

- (1) Decizia-cadru 2008/977/JAI a Consiliului se abrogă cu efect de la data menționată la articolul 62 alineatul (1).
- (2) Trimiterile la decizia-cadru abrogată menționată la alineatul (1) se interpretează ca trimiteri la prezenta directivă.

Articolul 59

Relația cu actele Uniunii adoptate anterior în domeniul cooperării judiciare în materie penală și al cooperării polițienești

Dispozițiile specifice referitoare la protecția datelor cu caracter personal din actele Uniunii adoptate în domeniul cooperării judiciare în materie penală și al cooperării polițienești (...), 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 temeiul tratatelor și care intră în domeniul de aplicare a prezentei directive nu sunt afectate.

Articolul 60

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 intrarea în vigoare a prezentei directive și care sunt în conformitate cu dreptul Uniunii aplicabil înainte de intrarea în vigoare a prezentei directive, rămân în vigoare până la modificarea, înlocuirea sau revocarea lor.
(...)

Articolul 61

Evaluarea

- (1) Comisia evaluează aplicarea prezentei directive. În contextul acestei evaluări, Comisia examinează în special aplicarea și funcționarea dispozițiilor articolului 36aa.

- (2) În termen de cinci ani de la intrarea în vigoare a prezentei directive, Comisia revizuieste alte acte adoptate de Uniunea Europeană care reglementează prelucrarea datelor cu caracter personal de către autoritățile competente în scopurile prevăzute la articolul 1 alineatul (1), inclusiv actele adoptate de Uniune menționate la articolul 59, pentru a evalua necesitatea de a le alinia la prezenta directivă și prezintă, după caz, propunerile necesare de modificare a acestor acte pentru a asigura o abordare uniformă privind protecția datelor cu caracter personal care intră în domeniul de aplicare al prezentei directive.
- (3) Comisia transmite Parlamentului European și Consiliului, la intervale regulate, rapoarte privind evaluarea și revizuirea prezentei directive în temeiul alineatului (1). Primele rapoarte sunt transmise în termen de cel mult patru ani de la data intrării în vigoare a prezentei directive. Ulterior, următoarele rapoarte sunt transmise o dată la patru ani. Comisia transmite, dacă este necesar, propuneri corespunzătoare în vederea modificării prezentei directive, precum și a alinierii altor instrumente juridice. Raportul se publică.

Articolul 62

Punerea în aplicare

- (1) Statele membre adoptă și publică, până la cel târziu [data/ trei ani de la intrarea în vigoare], 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 xx.xx.201x [data/ **trei** ani de la intrarea în vigoare].
- 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) Statele membre comunică Comisiei textul principalelor dispoziții de drept intern pe care le adoptă în domeniul reglementat de prezenta directivă.

Articolul 63

Intrare în vigoare (...)

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

Articolul 64

Destinatari

Prezenta directivă se adresează statelor membre.
