DIRECTIVE

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

din 27 aprilie 2016

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

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Regiunilor ([1]),

hotărând în conformitate cu procedura legislativă ordinară ([2]),

întrucât:

(1) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal reprezintă un drept fundamental. Articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene (Carta) și articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc.

(2) Principiile și normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal ar trebui, indiferent de cetățenia sau de locul de reședință al persoanelor fizice, să respecte drepturile și libertățile fundamentale ale acestora, în special dreptul la protecția datelor cu caracter personal. Prezenta directivă urmărește să contribuie la realizarea unui spațiu de libertate, securitate și justiție.

(3) Evoluțiile tehnologice rapide și globalizarea au generat noi provocări pentru protecția datelor cu caracter personal. Amploarea colectării și a schimbului de date cu caracter personal a crescut în mod semnificativ. Tehnologia permite prelucrarea datelor cu caracter personal la un nivel fără precedent în cadrul activităților precum prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor ori executarea pedepselor.

(4) Libera circulație a datelor cu caracter personal între autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora în cadrul Uniunii, și transferul de astfel de date cu caracter personal către țări terțe și organizații internaționale, ar trebui facilitate asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal. Aceste evoluții impun realizarea unui cadru solid și mai coerent în materie de protecție a datelor cu caracter personal în Uniune, însoțit de o aplicare riguroasă a normelor.

(5) Directiva 95/46/CE a Parlamentului European și a Consiliului ([3]) se aplică oricărei prelucrări de date cu caracter personal în statele membre, atât în sectorul public, cât și în cel privat. Cu toate acestea, directiva menționată nu se aplică prelucrării datelor cu caracter personal în cursul exercitării unei activități care nu se înscrie în domeniul de aplicare a dreptului comunitar, cum sunt activitățile în domeniul cooperării judiciare în materie penală și al cooperării polițienești.

([1]) JO C 391, 18.12.2012, p. 127.
([2]) Poziția Parlamentului European din 12 martie 2014 (nepublicată încă în Jurnalul Oficial) și Poziția în primă lectură a Consiliului din 8 aprilie 2016 (nepublicată încă în Jurnalul Oficial). Poziția Parlamentului European din 14 aprilie 2016.
([3]) Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO L 281, 23.11.1995, p. 31).

(6) Decizia-cadru 2008/977/JAI a Consiliului ([1]) se aplică în domeniul cooperării judiciare în materie penală și al cooperării polițienești. Domeniul de aplicare a deciziei-cadru menționate este limitat la prelucrarea datelor cu caracter personal transmise sau puse la dispoziție între statele membre.

(7) Asigurarea unui nivel omogen și ridicat de protecție a datelor cu caracter personal ale persoanelor fizice și facilitarea schimbului de date cu caracter personal între autoritățile competente ale statelor membre sunt esențiale pentru a se garanta eficacitatea cooperării judiciare în materie penală și a cooperării polițienești. În acest scop, nivelul de protecție a drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora, ar trebui să fie echivalent în toate statele membre. Protecția efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea drepturilor persoanelor vizate și a obligațiilor celor care prelucrează date cu caracter personal, ci și competențe echivalente pentru monitorizarea și asigurarea conformității cu normele în materie de protecție a datelor cu caracter personal în statele membre.

(8) Articolul 16 alineatul (2) din TFUE mandatează Parlamentul European și Consiliul să stabilească normele privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal, precum și normele privind libera circulație a acestor date.

(9) Pe această bază, Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([2]) stabilește normele generale pentru protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și garantarea liberei circulații a acestor date în cadrul Uniunii.

(10) În Declarația nr. 21 cu privire la protecția datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești, anexată la actul final al Conferinței interguvernamentale care a adoptat Tratatul de la Lisabona, conferința a recunoscut că s-ar putea dovedi necesare norme specifice privind protecția datelor cu caracter personal și libera circulație a datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești în temeiul articolului 16 din TFUE, având în vedere natura specifică a acestor domenii.

(11) Prin urmare, domeniile menționate ar trebui să fie reglementate printr-o directivă care să stabilească norme specifice privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora, cu respectarea naturii speciale a activităților în cauză. Pot reprezenta astfel de autorități competente nu numai autoritățile publice, precum autoritățile judiciare, poliția sau alte autorități de aplicare a legii, ci și orice alt organism sau altă entitate însărcinată prin dreptul intern să exercite autoritatea publică și competențe publice în sensul prezentei directive. În cazul în care un astfel de organism sau de entitate prelucrează date cu caracter personal în alte scopuri decât cele urmărite de prezenta directivă, se aplică Regulamentul (UE) 2016/679. Regulamentul (UE) 2016/679 se aplică, prin urmare, în cazurile în care un organism sau o entitate colectează date cu caracter personal în alte scopuri și ulterior prelucrează datele cu caracter personal respective în vederea respectării unei obligații legale care îi revine. De exemplu, în scopul depistării, investigării sau urmăririi infracțiunilor, instituțiile financiare păstrează anumite date cu caracter personal care sunt prelucrate de către acestea și furnizează datele cu caracter personal respective numai autorităților naționale competente în cazuri specifice și în conformitate cu dreptul intern. Unui organism sau entități care prelucrează date cu caracter personal în numele acestor autorități, în cadrul domeniului de aplicare al prezentei directive, ar trebui să îi revină obligații în temeiul unui contract sau al altui act juridic și al dispozițiilor aplicabile persoanelor împuternicite de către operatori în conformitate cu prezenta directivă, fără ca prin aceasta să se aducă atingere aplicării Regulamentului (UE) 2016/679 în ceea ce privește prelucrarea datelor cu caracter personal de către persoana împuternicită de către operator, atunci când această prelucrare nu intră sub incidența prezentei directive.

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

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

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

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

(13) Noțiunea de infracțiune, în sensul prezentei directive, ar trebui să constituie o noțiune autonomă de drept al Uniunii astfel cum este interpretat de Curtea de Justiție a Uniunii Europene („Curtea de Justiție").

(14) Având în vedere că prezenta directivă nu ar trebui să se aplice prelucrării datelor cu caracter personal în cadrul unei activități care nu intră sub incidența dreptului Uniunii, activitățile privind securitatea națională, activitățile agențiilor sau ale unităților specializate pe probleme de securitate națională și prelucrarea datelor cu caracter personal de către statele membre atunci când acestea desfășoară activități circumscrise domeniului de aplicare al titlului V capitolul 2 din Tratatul privind Uniunea Europeană (TUE) nu ar trebui să fie considerate activități care se încadrează în domeniul de aplicare al prezentei directive.

(15) În vederea asigurării aceluiași nivel de protecție pentru persoanele fizice prin drepturi garantate din punct de vedere juridic în întreaga Uniune și a preîntâmpinării discrepanțelor care împiedică schimbul de date cu caracter personal între autoritățile competente, prezenta directivă ar trebui să prevadă norme armonizate pentru protecția și libera circulație a datelor cu caracter personal prelucrate în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. Armonizarea drepturilor statelor membre nu ar trebui să aibă ca rezultat diminuarea nivelului de protecție a datelor cu caracter personal pe care îl oferă statele respective, ci ar trebui, dimpotrivă, să urmărească să asigure un înalt nivel de protecție în cadrul Uniunii. Statele membre nu ar trebui să fie împiedicate să prevadă garanții mai mari decât cele stabilite în prezenta directivă pentru protecția drepturilor și libertăților persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente.

(16) Prezenta directivă nu aduce atingere principiului accesului publicului la documente oficiale. În temeiul Regulamentului (UE) 2016/679, datele cu caracter personal din documentele oficiale deținute de o autoritate publică sau de un organism public sau privat pentru îndeplinirea unei atribuții de interes public pot fi divulgate de autoritatea sau organismul respectiv în conformitate cu dreptul Uniunii sau cu dreptul intern sub incidența căruia intră autoritatea sau organismul, pentru a stabili un echilibru între accesul public la documente oficiale și dreptul la protecția datelor cu caracter personal.

(17) Protecția conferită de prezenta directivă ar trebui să vizeze persoanele fizice, indiferent de cetățenia sau de locul de reședință al acestora, în ceea ce privește prelucrarea datelor cu caracter personal ale acestora.

(18) Pentru a preîntâmpina un risc serios de eludare, protecția persoanelor fizice ar trebui să fie neutră din punct de vedere tehnologic și nu ar trebui să depindă de tehnicile utilizate. Protecția persoanelor fizice ar trebui să se aplice în ceea ce privește prelucrarea datelor cu caracter personal prin mijloace automate, precum și prelucrarea manuală, în cazul în care datele cu caracter personal sunt cuprinse sau destinate să fie cuprinse într-un sistem de evidență. Dosarele sau seturile de dosare, precum și copertele acestora, care nu sunt structurate în conformitate cu criterii specifice, nu ar trebui să intre sub incidența prezentei directive.

(19) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ([1]) se aplică prelucrării datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii. Regulamentul (CE) nr. 45/2001 și alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal ar trebui adaptate la principiile și normele stabilite prin Regulamentul (UE) 2016/679.

(20) Prezenta directivă nu împiedică statele membre să precizeze operațiunile și procedurile de prelucrare în normele naționale privind procedurile penale în ceea ce privește prelucrarea datelor cu caracter personal de către instanțe și alte autorități judiciare, în special în ceea ce privește datele cu caracter personal conținute într-o hotărâre judecătorească sau în înregistrările legate de proceduri penale.

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

(21) Principiile protecției datelor ar trebui să se aplice oricărei informații referitoare la o persoană fizică identificată sau identificabilă. Pentru a se determina dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană în scopul identificării, în mod direct sau indirect, a persoanei fizice respective. Pentru a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace în scopul identificării persoanei fizice, ar trebui luați în considerare toți factorii obiectivi, precum costurile și intervalul de timp necesare pentru identificare, ținându-se seama de tehnologia disponibilă la momentul prelucrării și de dezvoltarea tehnologică. Principiile protecției datelor ar trebui, prin urmare, să nu se aplice informațiilor anonime, adică informațiilor care nu sunt legate de o persoană fizică identificată sau identificabilă, sau datelor cu caracter personal care sunt anonimizate astfel încât persoana vizată nu mai este identificabilă.

(22) Autoritățile publice cărora le sunt divulgate date cu caracter personal în conformitate cu o obligație legală pentru exercitarea misiunii lor oficiale, cum ar fi autoritățile fiscale și vamale, unitățile de investigare financiară, autoritățile administrative independente sau autoritățile piețelor financiare, responsabile de reglementarea și de supravegherea piețelor valorilor mobiliare, nu ar trebui să fie considerate drept destinatari în cazul în care primesc date cu caracter personal care sunt necesare pentru desfășurarea unei anumite anchete de interes general, în conformitate cu dreptul Uniunii sau cu dreptul intern. Cererile de divulgare transmise de autoritățile publice ar trebui să se facă întotdeauna în scris, să fie motivate și ocazionale și nu ar trebui să se refere la totalitatea unui sistem de evidență sau să conducă la interconectarea sistemelor de evidență. Prelucrarea datelor cu caracter personal de către respectivele autorități publice ar trebui să respecte normele aplicabile privind protecția datelor, în conformitate cu scopurile prelucrării.

(23) Datele genetice ar trebui definite drept date cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice despre fiziologia sau starea de sănătate a persoanei respective, și care rezultă în urma unei analize a unei mostre de material biologic al persoanei fizice în cauză, în special a analizei cromozomiale, a unei analize a acidului dezoxiribonucleic (ADN) sau a acidului ribonucleic (ARN) sau în urma analizei oricărui alt element care permite obținerea unor informații echivalente. Având în vedere complexitatea și sensibilitatea informațiilor genetice, există un risc ridicat de utilizare abuzivă și de reutilizare în diverse scopuri neautorizate de către operator. Orice discriminare bazată pe caracteristici genetice ar trebui să fie, în principiu, interzisă.

(24) Datele cu caracter personal privind sănătatea ar trebui să includă toate datele având legătură cu starea de sănătate a persoanei vizate, care să dezvăluie informații despre starea de sănătate fizică sau mentală trecută, prezentă sau viitoare a persoanei vizate. Acestea includ informații privind persoana fizică colectate în cursul înscrierii acesteia la serviciile de asistență medicală sau în cadrul acordării serviciilor respective persoanei fizice în cauză, astfel cum sunt menționate în Directiva 2011/24/UE a Parlamentului European și a Consiliului ([1]); un număr, un simbol sau un semn distinctiv atribuit unei persoane fizice pentru identificarea singulară a acesteia în scopuri medicale; informații rezultate din testarea sau examinarea unei părți a corpului sau a unei substanțe corporale, inclusiv din date genetice și eșantioane de material biologic; precum și orice informații privind, de exemplu, o boală, un handicap, un risc de îmbolnăvire, istoricul medical, tratamentul clinic sau starea fiziologică sau biomedicală a persoanei vizate, indiferent de sursa acestora, ca de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro.

(25) Toate statele membre sunt afiliate la Organizația Internațională de Poliție Criminală (Interpol). Pentru a-și îndeplini misiunea, Interpol primește, stochează și difuzează date cu caracter personal pentru a ajuta autoritățile competente să prevină și să combată criminalitatea internațională. Prin urmare, este adecvat să se consolideze cooperarea dintre Uniune și Interpol prin promovarea unui schimb eficient de date cu caracter personal, asigurând, în același timp, respectarea drepturilor și libertăților fundamentale în ceea ce privește prelucrarea automată a datelor cu caracter personal. Atunci când se transferă date cu caracter personal din Uniune către Interpol și către țările care au membri delegați la Interpol, ar trebui să se aplice prezenta directivă, în special dispozițiile privind transferurile internaționale. Prezenta directivă nu ar trebui să aducă atingere normelor specifice stabilite în Poziția comună 2005/69/JAI a Consiliului ([2]) și în Decizia 2007/533/JAI a Consiliului ([3]).

(26) Orice prelucrare a datelor cu caracter personal trebuie să fie legală, echitabilă și transparentă față de persoanele fizice în cauză, iar prelucrarea trebuie să fie făcută numai pentru scopuri specifice prevăzute de lege. Acest lucru nu împiedică, în sine, autoritățile de aplicare a legii să desfășoare activități precum investigațiile sub acoperire sau supravegherea video. Aceste activități pot fi întreprinse în scopul prevenirii, depistării, investigării sau urmăririi

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

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

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

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

(27) Pentru prevenirea, investigarea și urmărirea penală a infracțiunilor, autoritățile competente trebuie să prelucreze datele cu caracter personal colectate în contextul prevenirii, depistării, investigării sau urmăririi penale a anumitor infracțiuni dincolo de acest context pentru a înțelege mai bine activitățile infracționale și pentru a face legături între diferitele infracțiuni detectate.

(28) În vederea menținerii securității în ceea ce privește prelucrarea și a prevenirii prelucrărilor care nu respectă prezenta directivă, datele cu caracter personal ar trebui prelucrate într-un mod care să asigure un nivel corespunzător de securitate și confidențialitate, inclusiv prin prevenirea accesului neautorizat la acestea sau a utilizării neautorizate a datelor și a echipamentului utilizat pentru prelucrare și luând în considerare stadiul actual al tehnologiei disponibile, costurile punerii acesteia în aplicare în raport cu riscurile și natura datelor cu caracter personal a căror protecție trebuie asigurată.

(29) Colectarea datelor cu caracter personal ar trebui să fie efectuată în scopuri determinate, explicite și legitime în cadrul domeniului de aplicare al prezentei directive, iar prelucrarea acestora nu ar trebui să se facă în scopuri care sunt incompatibile cu obiectivele prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau ale executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. În cazul în care datele cu caracter personal sunt prelucrate de către același sau de către un alt operator într-un scop care se încadrează în domeniul de aplicare al prezentei directive, dar este diferit de scopul în care au fost colectate, o astfel de prelucrare ar trebui să fie permisă cu condiția ca o astfel de prelucrare să fie autorizată în conformitate cu dispozițiile legale aplicabile și este necesară și proporțională în raport cu acest alt scop.

(30) Principiul exactității datelor ar trebui aplicat luând în considerare natura și scopul prelucrării în cauză. În special în cadrul procedurilor judiciare, declarațiile care conțin date cu caracter personal se bazează pe o percepție subiectivă a persoanelor fizice și nu sunt întotdeauna verificabile. În consecință, acest principiu nu ar trebui să se aplice exactității unei declarații, ci doar faptului că o anumită declarație a fost făcută.

(31) Prelucrarea datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești presupune prelucrarea datelor cu caracter personal referitoare la diferite categorii de persoane. Prin urmare, ar trebui să se facă o distincție clară, după caz și în măsura posibilului, între datele cu caracter personal ale diferitelor categorii de persoane vizate, cum ar fi suspecții, persoanele condamnate pentru comiterea unei infracțiuni, victimele și alte părți, cum ar fi martorii, persoanele care dețin informații sau contacte relevante și complicii suspecților și ai infractorilor condamnați. Acest lucru nu ar trebui să împiedice aplicarea dreptului la prezumția de nevinovăție, astfel cum este garantat de Cartă și de CEDO, după cum a fost interpretat de jurisprudența Curții de Justiție și, respectiv, a Curții Europene a Drepturilor Omului.

(32) Autoritățile competente ar trebui să se asigure că nu se transmit sau nu se pun la dispoziție date cu caracter personal care sunt inexacte, incomplete sau nu mai sunt actuale. Pentru a asigura protecția persoanelor fizice și exactitatea, caracterul integral sau gradul de actualitate și fiabilitatea datelor cu caracter personal transmise sau puse la dispoziție, autoritățile competente ar trebui, pe cât posibil, să adauge informațiile necesare în toate transmiterile de date cu caracter personal.

(33) Atunci când prezenta directivă face trimitere la dreptul intern, la un temei juridic sau la o măsură legislativă, aceasta nu necesită neapărat un act legislativ adoptat de către un parlament, fără a aduce atingere cerințelor care

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

(34) Prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora, ar trebui să acopere orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal sau seturilor de date cu caracter personal în aceste scopuri efectuată prin mijloace automate sau în alt mod, precum colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, alinierea sau combinarea, restricționarea prelucrării, ștergerea sau distrugerea. În special, normele din prezenta directivă ar trebui să se aplice transmiterii datelor cu caracter personal în sensul prezentei directive către un destinatar care nu face obiectul prezentei directive. Un astfel de destinatar ar trebui să includă o persoană fizică sau juridică, o autoritate publică, o agenție sau orice alt organ căruia îi sunt divulgate în mod legal datele cu caracter personal de către autoritățile competente. În cazul în care datele cu caracter personal au fost inițial colectate de către o autoritate competentă în unul dintre scopurile prezentei directive, Regulamentul (UE) 2016/679 ar trebui să se aplice prelucrării acestor date în alte scopuri decât cele ale prezentei directive atunci când o astfel de prelucrare este autorizată de dreptul Uniunii sau de dreptul intern. În special, normele din Regulamentul (UE) 2016/679 ar trebui să se aplice la transmiterea de date cu caracter personal în scopuri care nu intră sub incidența prezentei directive. Prelucrarea datelor cu caracter personal de către un destinatar care nu este sau nu acționează în calitate de autoritate competentă în sensul prezentei directive și căruia îi sunt divulgate în mod legal date cu caracter personal de către o autoritate competentă, ar trebui să intre sub incidența Regulamentului (UE) 2016/679. La punerea în aplicare a prezentei directive, statele membre ar trebui, de asemenea, să poată aduce precizări suplimentare cu privire la aplicarea normelor din Regulamentul (UE) 2016/679, sub rezerva condițiilor prevăzute în regulamentul respectiv.

(35) Pentru a fi legală, prelucrarea datelor cu caracter personal în temeiul prezentei directive ar trebui să fie necesară pentru îndeplinirea unei atribuții de interes public de către o autoritate competentă în temeiul dreptului Uniunii sau al dreptului intern, în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. Aceste activități ar trebui să acopere protejarea intereselor vitale ale persoanei vizate. Îndeplinirea sarcinilor de prevenire, depistare, investigare sau urmărire penală a infracțiunilor, conferită în mod instituțional prin lege autorităților competente, le permite acestora să solicite sau să impună persoanelor fizice să respecte cerințele formulate. În acest caz, consimțământul persoanei vizate, astfel cum este definit în Regulamentul (UE) 2016/679, nu ar trebui să constituie un temei juridic pentru prelucrarea datelor cu caracter personal de către autoritățile competente. În cazul în care i se solicită persoanei vizate să respecte o obligație legală, persoana vizată nu dispune cu adevărat de libertatea de alegere, astfel încât reacția persoanei vizate nu poate fi considerată ca o manifestare liberă a voinței sale. Acest lucru nu ar trebui să împiedice statele membre să prevadă prin lege că persoana vizată poate accepta prelucrarea datelor sale cu caracter personal în scopurile prezentei directive, cum ar fi testele ADN în anchetele penale sau monitorizarea localizării persoanei vizate prin dispozitive electronice pentru executarea pedepselor.

(36) Statele membre ar trebui să prevadă că, în cazul în care dreptul Uniunii sau dreptul intern aplicabil autorității competente care a transmis datele prevede condiții specifice aplicabile în situații specifice prelucrării datelor cu caracter personal, cum ar fi folosirea unor coduri de utilizare, autoritatea competentă care a transmis datele ar trebui să informeze destinatarul respectivelor date cu caracter personal cu privire la astfel de condiții și obligația de a le respecta. Astfel de condiții ar putea include, de exemplu, interdicția de a transmite datele cu caracter personal altor destinatari sau de a le utiliza în alte scopuri decât cele pentru care au fost transmise destinatarului, sau de a informa persoana vizată în cazul unei limitări a dreptului la informare fără aprobarea prealabilă a autorității competente care a transmis datele. Obligațiile menționate ar trebui să se aplice, de asemenea, transferurilor realizate de autoritatea competentă care a transmis datele către destinatari din țări terțe sau către organizații internaționale. Statele membre ar trebui să garanteze neaplicarea de către autoritatea competentă care a transmis datele nu aplică în cazul destinatarilor din alte state membre sau în cazul agențiilor, oficiilor și organelor instituite în conformitate cu titlul V capitolele 4 și 5 din TFUE, alte condiții decât cele aplicabile transmiterii similare de date în statul membru al autorității competente respective.

(37) Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale necesită o protecție specifică, deoarece contextul prelucrării acestora ar putea genera riscuri considerabile la adresa drepturilor și libertăților fundamentale. Aceste date cu caracter personal ar trebui să includă datele cu caracter personal care dezvăluie originea rasială sau etnică, utilizarea termenului „origine rasială”

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

(38) Persoana vizată ar trebui să aibă dreptul de a nu face obiectul unei decizii care evaluează aspecte cu caracter personal referitoare la propria persoană, care se bazează exclusiv pe prelucrarea automată și care produce efecte juridice negative care privesc propria persoană sau o afectează în mod semnificativ. În orice caz, o astfel de prelucrare ar trebui să facă obiectul unor garanții corespunzătoare, inclusiv o informare specifică a persoanei vizate și dreptul acesteia de a obține intervenție umană, în special de a-și exprima punctul de vedere, de a primi o explicație privind decizia luată în urma unei astfel de evaluări sau de a contesta decizia. Crearea de profiluri care are drept rezultat discriminarea persoanelor fizice pe baza datelor cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale este interzisă în condițiile prevăzute la articolele 21 și 52 din Cartă.

(39) Pentru ca persoana vizată să își poată exercita drepturile, toate informațiile adresate persoanei vizate ar trebui să fie ușor accesibile, inclusiv pe site-ul internet al operatorului, și ușor de înțeles, fiind necesar ca limbajul folosit să fie simplu și clar. Respectivele informații ar trebui să fie adaptate la nevoile persoanelor vulnerabile, cum ar fi copiii.

(40) Ar trebui să fie prevăzute modalități de facilitare a exercitării de către persoana vizată a drepturilor care îi sunt conferite prin dispozițiile adoptate în temeiul prezentei directive, inclusiv mecanismele prin care aceasta poate solicita și, după caz obține, în mod gratuit, în special, acces la datele cu caracter personal, precum și rectificarea sau ștergerea acestora și restricționarea prelucrării. Operatorul ar trebui să aibă obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate, cu excepția cazului în care operatorul aplică limitări ale drepturilor persoanelor vizate în conformitate cu prezenta directivă. În plus, în cazul în care cererile sunt în mod vădit nefondate sau excesive, de exemplu atunci când persoana vizată solicită informații în mod nejustificat și repetat sau atunci când persoana vizată abuzează de dreptul său de a primi informații, de exemplu prin furnizarea de informații false sau înșelătoare în momentul efectuării cererii, operatorul ar trebui să poată percepe o taxă rezonabilă sau să refuze să dea curs cererii.

(41) Atunci când operatorul solicită furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate, respectivele informații ar trebui să fie prelucrate numai în acest scop specific și nu ar trebui să fie stocate pentru o perioadă mai lungă decât cea necesară în acest scop specific.

(42) Cel puțin următoarele informații ar trebui să fie puse la dispoziția persoanei vizate: identitatea operatorului, existența operațiunii de prelucrare, scopurile prelucrării, dreptul de a înainta o plângere și existența dreptului de a solicita operatorului accesul la prelucrare, precum și rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării. Acest lucru ar putea să se realizeze pe site-ul internet al autorității competente. În plus, în cazuri specifice și pentru a-i permite persoanei vizate să își exercite drepturile, persoana vizată ar trebui să fie informată cu privire la temeiul juridic al prelucrării și cu privire la cât timp vor fi stocate datele, în măsura în care astfel de informații suplimentare sunt necesare, având în vedere circumstanțele specifice în care sunt prelucrate datele, pentru a garanta o prelucrare echitabilă în ceea ce privește persoana vizată.

(43) O persoană fizică ar trebui să aibă drept de acces la datele colectate care o privesc și ar trebui să își exercite acest drept cu ușurință și la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia. Orice persoană vizată ar trebui, prin urmare, să aibă dreptul de a cunoaște și de a i se comunica în ce scopuri sunt prelucrate datele, pentru ce perioadă sunt acestea prelucrate și care este identitatea destinatarilor datelor, inclusiv din țările terțe. Când respectiva comunicare include informații cu privire la originea datelor cu caracter personal, astfel de informații nu ar trebui să dezvăluie identitatea persoanelor fizice, în special a surselor confidențiale. Pentru ca acest drept să fie respectat, este suficient ca persoana vizată să dețină o sinteză completă a respectivelor date într-o formă inteligibilă, adică o formă care să permită persoanei vizate să ia cunoștință de aceste date și să verifice că acestea sunt exacte și prelucrate în conformitate cu prezenta directivă,

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

(44) Statele membre ar trebui să aibă posibilitatea de a adopta măsuri legislative în vederea amânării, a restricționării sau a omiterii informării persoanelor vizate sau în vederea restricționării, integrale sau parțiale, a accesului la datele lor cu caracter personal, în măsura în care și atât timp cât o astfel de măsură constituie o măsură necesară și proporțională într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice în cauză, pentru a se evita obstrucționarea cercetărilor, a anchetelor sau a procedurilor oficiale sau judiciare, pentru a nu se afecta prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea pedepselor, pentru a se apăra securitatea publică sau securitatea națională ori pentru a se apăra drepturile și libertățile altor persoane. Operatorul ar trebui să evalueze, prin intermediul unei examinări concrete și individuale a fiecărui caz în parte, dacă dreptul de acces ar trebui să fie limitat parțial sau complet.

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

(46) Orice limitare a drepturilor persoanei vizate trebuie să fie în conformitate cu Carta și cu CEDO, după cum a fost interpretată de jurisprudența Curții de Justiție și, respectiv, a Curții Europene a Drepturilor Omului și, îndeosebi, trebuie să respecte esența drepturilor și libertăților respective.

(47) O persoană fizică ar trebui să aibă dreptul de a obține rectificarea datelor cu caracter personal inexacte care o privesc, mai ales când acestea se referă la fapte, precum și dreptul la ștergerea datelor în cazul în care prelucrarea datelor respective nu respectă prezenta directivă. Cu toate acestea, dreptul la rectificare nu ar trebui să afecteze, de exemplu, conținutul depozițiilor martorilor. O persoană fizică ar trebui să aibă, de asemenea, dreptul la restricționarea prelucrării atunci când această persoană contestă exactitatea datelor cu caracter personal și nu se poate stabili exactitatea sau inexactitatea lor sau în cazul în care datele cu caracter personal trebuie să fie păstrate ca mijloace de probă. În special, în loc ca datele cu caracter personal să fie șterse, prelucrarea ar trebui să fie restricționată dacă într-un caz specific există motive întemeiate să se considere că ștergerea lor ar putea afecta interesele legitime ale persoanei vizate. În acest caz, datele restricționate ar trebui să fie prelucrate doar în scopul care a împiedicat ștergerea lor. Metodele de restricționare a prelucrării ar putea include, printre altele, transferul datelor selectate în alt sistem de prelucrare, de exemplu în scopuri de arhivare, sau anularea accesului utilizatorilor la datele selectate. În ceea ce privește sistemele automatizate de evidență a datelor, restricționarea prelucrării de date cu caracter personal ar trebui, în principiu, asigurată prin mijloace tehnice; faptul că prelucrarea datelor cu caracter personal este restricționată ar trebui indicat în sistem în așa fel încât să se înțeleagă clar că această restricționare are loc. O astfel de rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării ar trebui să fie comunicată destinatarilor cărora le-au fost divulgate datele și autorităților competente de la care provin datele inexacte. Operatorii ar trebui, de asemenea, să nu comunice mai departe astfel de date.

(48) În cazul în care operatorul refuză unei persoane vizate drepturile acesteia la informare, acces ori la rectificarea sau ștergerea datelor cu caracter personal sau la restricționarea prelucrării, persoana vizată ar trebui să aibă dreptul de a solicita ca autoritatea națională de supraveghere să verifice legalitatea prelucrării. Persoana vizată ar trebui să fie informată cu privire la acest drept. Atunci când autoritatea de supraveghere acționează în numele persoanei vizate, persoana vizată ar trebui să fie informată de către autoritatea de supraveghere cel puțin cu privire la faptul că toate verificările sau revizuirile necesare au fost efectuate de către autoritatea de supraveghere. Autoritatea de supraveghere ar trebui, de asemenea, să informeze persoana vizată în legătură cu dreptul de a introduce o cale de atac.

(49) În cazul în care datele cu caracter personal sunt prelucrate în cadrul unei anchete penale și al unor acțiuni în instanță în materie penală, statele membre ar trebui să poată garanta exercitarea drepturilor la informare, acces și de rectificare sau ștergere a datelor cu caracter personal și de restricționare a prelucrării în conformitate cu normele naționale privind procedurile judiciare.

(50) Ar trebui să se stabilească responsabilitatea și răspunderea operatorului pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său. În special, operatorul ar trebui să fie obligat să pună în aplicare măsuri adecvate și eficace și să fie în măsură să demonstreze că activitățile de prelucrare respectă prezenta directivă. Măsurile respective ar trebui să țină seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul la adresa drepturilor și libertăților persoanelor fizice. Măsurile luate de operator ar trebui să includă elaborarea și punerea în aplicare a unor garanții specifice cu privire la tratamentul datelor cu caracter personal ale persoanelor vulnerabile, în special ale copiilor.

(51) Riscurile la adresa drepturilor și libertăților persoanelor fizice, prezentând grade diferite de probabilitate și gravitate, pot fi rezultatul unei prelucrări a datelor care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care: prelucrarea poate genera discriminare, furtul sau uzurparea identității, prejudiciu financiar, compromiterea reputației, pierderea confidențialității datelor protejate prin secret profesional,

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

(52) Probabilitatea și gravitatea riscului ar trebui să fie determinate în raport de natura, domeniul de aplicare, contextul și scopurile prelucrării. Riscul ar trebui să facă obiectul unei evaluări obiective, prin care să se stabilească dacă operațiunile de prelucrare a datelor prezintă un risc ridicat. Un risc ridicat este un risc deosebit de prejudiciere a drepturilor și libertăților persoanelor vizate.

(53) Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare pentru a se asigura îndeplinirea cerințelor din prezenta directivă. Punerea în aplicare a unor astfel de măsuri nu ar trebui să se întemeieze doar pe considerente economice. Pentru a fi în măsură să demonstreze respectarea prezentei directive, operatorul ar trebui să adopte politici interne și să pună în aplicare măsuri care să adere, în special, la principiul protecției datelor începând cu momentul conceperii și al protecției implicite a datelor. În cazul în care operatorul a realizat o evaluare a impactului asupra protecției datelor în temeiul prezentei directive, ar trebui să se țină cont de rezultatele acesteia la elaborarea măsurilor și procedurilor respective. Măsurile ar putea consta, printre altele, în utilizarea pseudonimizării, cât mai curând posibil. Utilizarea pseudonimizării în sensul prezentei directive poate servi ca instrument care ar putea facilita, în special, libera circulație a datelor cu caracter personal în cadrul spațiului de libertate, securitate și justiție.

(54) Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și a persoanelor împuternicite de către operator, inclusiv în ceea ce privește monitorizarea de către autoritățile de supraveghere și măsurile adoptate de acestea, necesită o atribuire clară a responsabilităților stabilite prin prezenta directivă, inclusiv în cazul în care un operator stabilește scopurile și mijloacele prelucrării împreună cu alți operatori sau în cazul în care o operațiune de prelucrare este efectuată în numele unui operator.

(55) Efectuarea prelucrării de către o persoană împuternicită de către un operator ar trebui să fie reglementată printr-un act juridic care să includă un contract care creează obligații pentru persoana împuternicită de către operator în raport cu operatorul și care să stipuleze, în special, că persoana împuternicită de către operator ar trebui să acționeze numai la instrucțiunile operatorului. Persoana împuternicită de către operator ar trebui să țină cont de principiul protecției datelor începând cu momentul conceperii și al protecției implicite a datelor.

(56) În vederea demonstrării conformității cu prezenta directivă, operatorul sau persoana împuternicită de către operator ar trebui să păstreze evidențe ale tuturor categoriilor de activități de prelucrare aflate în responsabilitatea sa. Fiecare operator și fiecare persoană împuternicită de către operator ar trebui să aibă obligația de a coopera cu autoritatea de supraveghere și de a pune la dispoziția acesteia, la cerere, aceste evidențe, pentru a putea fi utilizate în scopul monitorizării respectivelor operațiuni de prelucrare. Operatorul sau persoana împuternicită de către operator care prelucrează date cu caracter personal în sisteme de prelucrare neautomată ar trebui să dispună de metode eficiente pentru a demonstra legalitatea prelucrării, a permite monitorizarea proprie și a garanta integritatea și securitatea datelor, precum înregistrări sau alte forme de evidențe.

(57) Înregistrările ar trebui păstrate cel puțin pentru operațiunile din cadrul sistemelor de prelucrare automată, precum colectarea, modificarea, consultarea, divulgarea, inclusiv transferurile, combinarea sau ștergerea. Identificarea persoanei care a consultat sau divulgat date cu caracter personal ar trebui să fie înregistrată și, plecând de la identificarea respectivă, ar putea fi posibil să se stabilească justificarea operațiunilor de prelucrare. Înregistrările ar trebui să fie utilizate numai pentru verificarea legalității prelucrării, monitorizarea proprie, asigurarea integrității și securității datelor și pentru proceduri penale. Monitorizarea proprie include, de asemenea, proceduri disciplinare interne ale autorităților competente.

(58) Operatorul ar trebui să realizeze o evaluare a impactului asupra protecției datelor în cazurile în care operațiunile de prelucrare pot avea drept rezultat, prin natura, domeniul de aplicare sau scopurile lor, un risc ridicat la adresa drepturilor și libertăților persoanelor vizate, evaluare care ar trebui să includă în special măsurile, garanțiile și mecanismele preconizate în vederea asigurării protecției datelor cu caracter personal și a atestării conformității cu prezenta directivă. Evaluările impactului ar trebui să acopere sistemele și procesele relevante aferente operațiunilor de prelucrare, și nu cazuri individuale.

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

(60) În vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezenta directivă, operatorul sau persoana împuternicită de către operator ar trebui să evalueze riscurile inerente prelucrării și să pună în aplicare măsuri pentru atenuarea acestor riscuri, precum criptarea. Măsurile respective ar trebui să asigure un nivel corespunzător de securitate, inclusiv de confidențialitate, luând în considerare stadiul actual al tehnologiei, costurile punerii lor în aplicare în raport cu riscurile și natura datelor cu caracter personal a căror protecție trebuie asigurată. La evaluarea riscurilor la adresa securității datelor, ar trebui să se acorde atenție riscurilor pe care le prezintă prelucrarea datelor, cum ar fi distrugerea, pierderea sau modificarea accidentală sau ilegală, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, care pot duce în special la prejudicii fizice, materiale sau morale. Operatorul și persoana împuternicită de către operator ar trebui să se asigure că prelucrarea datelor cu caracter personal nu se realizează de către persoane neautorizate.

(61) Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate genera prejudicii fizice, materiale sau morale persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau uzurpare de identitate, prejudiciu financiar, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt prejudiciu important de natură economică sau socială cauzat acelei persoane fizice. Prin urmare, de îndată ce a luat cunoștință de producerea unei încălcări a securității datelor cu caracter personal, operatorul ar trebui să notifice încălcarea securității datelor cu caracter personal autorității de supraveghere fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore după ce a luat cunoștință de existența acesteia, cu excepția cazului în care operatorul este în măsură să demonstreze, în conformitate cu principiul responsabilității, că încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. Atunci când notificarea nu se poate realiza în termen de 72 de ore, aceasta ar trebui să cuprindă motivele întârzierii, iar informațiile pot fi furnizate treptat, fără altă întârziere.

(62) Persoanele fizice ar trebui să fie notificate fără întârziere în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, pentru a le permite acestora să ia măsurile de precauție necesare. Notificarea ar trebui să descrie natura încălcării securității datelor cu caracter personal și să formuleze recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative. Notificarea persoanelor vizate ar trebui să fie efectuate în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu autoritatea de supraveghere și în conformitate cu orientările furnizate de aceasta sau de alte autorități relevante. De exemplu, necesitatea de a atenua un risc imediat de producere a unor prejudicii ar presupune notificarea cu promptitudine a persoanelor vizate, în timp ce necesitatea de a pune în aplicare măsuri corespunzătoare împotriva încălcării în continuare a securității datelor sau împotriva unor încălcări similare ale securității datelor ar putea justifica un termen mai îndelungat. În cazul în care evitarea obstrucționării cercetărilor, a anchetelor sau a procedurilor oficiale sau judiciare, evitarea aducerii de prejudicii la adresa prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau a executării pedepselor, a protejării securității publice, a protejării securității naționale sau a apărării drepturilor și libertăților altora nu pot fi obținute prin amânarea sau restricționarea comunicării unei încălcări a securității datelor cu caracter personal către persoana fizică în cauză, o astfel de comunicare ar putea fi omisă în circumstanțe excepționale.

(63) Operatorul ar trebui să desemneze o persoană care să îi acorde asistență pentru a monitoriza respectarea, la nivel intern, a dispozițiilor adoptate în temeiul prezentei directive, cu excepția cazului în care un stat membru decide să exonereze instanțele și alte autorități judiciare independente atunci când acționează în exercițiul funcției lor judiciare. Persoana respectivă ar putea fi un membru al personalului existent al operatorului care a beneficiat de o formare specială în materie de legislație și practici privind protecția datelor pentru a dobândi cunoștințe de specialitate în domeniul respectiv. Nivelul necesar al cunoștințelor de specialitate ar trebui să se stabilească în special în funcție de prelucrarea efectuată asupra datelor și de gradul de protecție impus pentru datele cu caracter personal prelucrate de către operator. Îndeplinirea sarcinilor sale poate fi efectuată cu normă întreagă sau cu fracțiune de normă. Un responsabil cu protecția datelor poate fi numit în comun de mai mulți operatori, ținând seama de structura organizatorică și de dimensiunea acestora, de exemplu în caz de resurse comune în unitățile centrale. Persoana respectivă poate fi, de asemenea, numită în posturi diferite în cadrul structurii operatorilor relevanți. Persoana respectivă ar trebui să îl ajute pe operator și pe angajații care prelucrează date cu caracter personal, prin informarea și consilierea acestora cu privire la respectarea obligațiilor relevante ale acestora în materie de protecție a datelor. Astfel de responsabili cu protecția datelor ar trebui să fie în măsură să își îndeplinească îndatoririle și sarcinile în mod independent, în conformitate cu dreptul intern.

(64) Statele membre ar trebui să asigure că transferul către o țară terță sau către o organizație internațională are loc numai în cazul în care acest transfer este necesar pentru prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau pentru executarea pedepselor, inclusiv pentru protejarea împotriva amenințărilor la adresa

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

(65) În cazul transferului de date cu caracter personal de la un stat membru către țări terțe sau către organizații internaționale, un astfel de transfer ar trebui să aibă loc, în principiu, numai după ce statul membru de la care au fost obținute datele a acordat o autorizație în ceea ce privește transferul. Interesele unei cooperări eficiente în domeniul aplicării legii impun ca, în cazul în care natura unei amenințări la adresa securității publice a unui stat membru sau a unei țări terțe sau la adresa intereselor fundamentale ale unui stat membru este atât de urgentă încât să facă imposibilă obținerea unei autorizații prealabile în timp util, autoritatea competentă ar trebui să poată transfera datele cu caracter personal relevante către țara terță sau organizația internațională în cauză fără o astfel de autorizație prealabilă. Statele membre ar trebui să prevadă că orice condiții specifice pentru transfer ar trebui să fie comunicate țărilor terțe sau organizațiilor internaționale. Transferurile ulterioare de date cu caracter personal ar trebui să facă obiectul autorizării prealabile de către autoritatea competentă care a realizat transferul inițial. Atunci când decide cu privire la o cerere de autorizare a unui transfer ulterior, autoritatea competentă care a realizat transferul inițial ar trebui să țină seama în mod corespunzător de toți factorii relevanți, inclusiv de gravitatea infracțiunii, de condițiile specifice transferului și de scopul pentru care datele au fost transferate inițial, de natura și condițiile executării pedepsei, precum și de nivelul de protecție a datelor cu caracter personal din țara terță sau dintr-o organizație internațională către care datele cu caracter personal sunt transferate ulterior. Autoritatea competentă care a realizat transferul inițial ar trebui, de asemenea, să poată aplica transferului ulterior condiții specifice. Astfel de condiții specifice pot fi descrise, de exemplu, în coduri de utilizare.

(66) Comisia ar trebui să poată decide, cu efect în întreaga Uniune, că anumite țări terțe, un teritoriu ori unul sau mai multe sectoare determinate dintr-o țară terță sau o organizație internațională oferă un nivel adecvat de protecție a datelor, furnizând astfel securitate juridică și uniformitate în întreaga Uniune în ceea ce privește țările terțe sau organizațiile internaționale care sunt considerate a furniza un astfel de nivel de protecție. În astfel de cazuri, transferurile de date cu caracter personal către țările respective ar trebui să se poată realiza fără a fi necesară obținerea unei autorizații speciale, cu excepția cazului în care un alt stat membru de la care au fost obținute datele trebuie să își dea autorizația pentru transfer.

(67) În conformitate cu valorile fundamentale pe care se întemeiază Uniunea, în special apărarea drepturilor omului, Comisia ar trebui, în evaluarea sa referitoare la țara terță sau la un teritoriu sau la un sector determinat dintr-o țară terță, să ia în considerare modul în care o anumită țară terță respectă statul de drept, accesul la justiție, precum și normele și standardele internaționale în materie de drepturi ale omului și legislația sa generală și sectorială, inclusiv legislația privind securitatea publică, apărarea și securitatea națională, precum și ordinea publică și dreptul penal. Adoptarea unei decizii privind caracterul adecvat al nivelului de protecție în ceea ce privește un teritoriu sau un sector determinat dintr-o țară terță ar trebui să țină seama de criterii clare și obiective, cum ar fi activitățile specifice de prelucrare și domeniul de aplicare al standardelor juridice aplicabile și legislația în vigoare în țara terță respectivă. Țara terță ar trebui să garanteze un nivel adecvat de protecție, echivalent în esență celui asigurat în cadrul Uniunii, în special atunci când datele sunt prelucrate în unul sau mai multe sectoare specifice. În special, țara terță ar trebui să asigure o supraveghere efectivă independentă în materie de protecție a datelor și să prevadă mecanisme de cooperare cu autoritățile de protecție a datelor din statele membre, iar persoanele vizate ar trebui să beneficieze de drepturi efective și opozabile și de reparații efective pe cale administrativă și judiciară.

(68) Pe lângă angajamentele internaționale asumate de țara terță sau de organizația internațională, Comisia ar trebui să țină seama și de obligațiile care decurg din participarea țării terțe sau a organizației internaționale la sistemele multilaterale sau regionale, în special în ceea ce privește protecția datelor cu caracter personal, precum și de punerea în aplicare a unor astfel de obligații. În special, ar trebui să fie luată în considerare aderarea țării terțe la Convenția Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal și la protocolul adițional la aceasta. Comisia ar trebui să consulte

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

(69) Comisia ar trebui să monitorizeze funcționarea deciziilor privind nivelul de protecție dintr-o țară terță, un teritoriu sau un sector determinat dintr-o țară terță sau dintr-o organizație internațională. În ceea ce privește deciziile sale privind caracterul adecvat al nivelului de protecție, Comisia ar trebui să prevadă un mecanism de revizuire periodică a funcționării acestora. Această revizuire periodică ar trebui să se realizeze în consultare cu țara terță sau cu organizația internațională în cauză și ar trebui să ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională.

(70) Comisia ar trebui, de asemenea, să fie în măsură să constate faptul că o țară terță, un teritoriu sau un sector determinat dintr-o țară terță ori o organizație internațională nu mai asigură un nivel corespunzător de protecție a datelor. În consecință, transferul de date cu caracter personal către țara terță sau organizația internațională respectivă ar trebui să fie interzis, cu excepția cazului când sunt îndeplinite cerințele prevăzute în prezenta directivă referitoare la transferul de date sub rezerva unor garanții adecvate și a unor derogări în situații specifice. Ar trebui să se prevadă proceduri de consultare între Comisie și astfel de țări terțe sau organizații internaționale. Comisia ar trebui ca, în timp util, să informeze țara terță sau organizația internațională cu privire la aceste motive și să inițieze consultări cu aceasta pentru remedierea situației.

(71) Transferurile care nu se întemeiază pe o astfel de decizie privind caracterul adecvat al nivelului de protecție ar trebui să fie permise numai în cazul în care au fost prezentate garanții corespunzătoare într-un instrument cu caracter juridic obligatoriu, care să asigure protecția datelor cu caracter personal, sau în cazul în care operatorul a evaluat toate circumstanțele legate de datele transferate și, pe baza acestei evaluări, consideră că există garanții adecvate în ceea ce privește protecția datelor cu caracter personal. Astfel de instrumente cu caracter juridic obligatoriu ar putea fi, de exemplu, acorduri bilaterale cu caracter juridic obligatoriu care au fost încheiate de statele membre și puse în aplicare în ordinea juridică a acestora și a căror respectare poate fi impusă de către persoanele vizate din respectivele state membre, asigurând respectarea cerințelor în materie de protecție a datelor și drepturile persoanelor vizate, inclusiv dreptul de a obține reparații efective pe cale administrativă sau judiciară. Operatorul ar trebui să ia în considerare acordurile de cooperare încheiate între Europol sau Eurojust și țări terțe care permit schimbul de date cu caracter personal atunci când se efectuează evaluarea tuturor circumstanțelor legate de transferul de date. Operatorul ar trebui, de asemenea, să poată lua în considerare faptul că transferul de date cu caracter personal va fi supus obligațiilor de confidențialitate și principiului specificității, asigurându-se că datele nu vor fi prelucrate în alte scopuri decât cel al transferului. În plus, operatorul ar trebui să ia în considerare faptul că datele cu caracter personal nu vor fi folosite pentru a solicita, a pronunța sau a executa pedeapsa cu moartea sau orice altă formă de tratament crud și inuman. Chiar dacă aceste condiții ar putea fi considerate garanții adecvate care să permită transferul de date, operatorul ar trebui să poată solicita garanții suplimentare.

(72) În cazul în care nu există nicio decizie privind caracterul adecvat al nivelului de protecție sau nicio garanție adecvată, un transfer sau o categorie de transferuri poate avea loc numai în situații specifice, dacă este necesar în scopul protejării intereselor vitale ale persoanei vizate sau ale unei alte persoane sau al protejării intereselor legitime ale persoanei vizate, în cazul în care se prevede astfel în dreptul statului membru care transferă datele cu caracter personal; pentru prevenirea unei amenințări imediate și grave la adresa securității publice a unui stat membru sau a unei țări terțe; într-un caz specific, în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv în scopul protejării împotriva amenințărilor la adresa securității publice; sau, într-un caz specific, pentru constatarea, exercitarea sau apărarea unui drept în instanță. Aceste derogări ar trebui interpretate restrictiv și nu ar trebui să permită transferuri frecvente, masive și structurale de date cu caracter personal sau transferuri la scară largă de date, ci ar trebui să se limiteze la datele strict necesare. Astfel de transferuri ar trebui să fie documentate și să fie puse la dispoziția autorității de supraveghere la cerere, în scopul monitorizării legalității transferului.

(73) Autoritățile competente ale statelor membre aplică acordurile internaționale bilaterale sau multilaterale în vigoare, încheiate cu țări terțe în domeniul cooperării judiciare în materie penală și al cooperării polițienești, în schimbul obținerii de informații relevante care să le permită să își îndeplinească sarcinile atribuite în mod legal. În principiu, acest lucru are loc prin intermediul sau cel puțin cu cooperarea autorităților competente din țările terțe implicate în scopul prezentei directive, uneori chiar în absența unui acord internațional bilateral sau multilateral. Cu toate acestea, în anumite cazuri individuale, procedurile obișnuite care necesită contactarea autorității din țara terță pot fi ineficiente sau inadecvate, în special din cauza faptului că transferul nu poate fi efectuat în timp util sau din cauza faptului că autoritatea din țara terță nu respectă statul de drept sau normele și standardele internaționale în materie de drepturi ale omului, astfel încât autoritățile competente ale statelor membre ar putea decide să transfere datele cu caracter personal direct beneficiarilor stabiliți în țări terțe. Acesta ar putea fi cazul atunci când există o nevoie urgentă de a transfera date cu caracter personal pentru a salva viața unei persoane care se află în pericol de a deveni victimă a unei infracțiuni sau în interesul prevenirii săvârșirii iminente a unei infracțiuni, inclusiv a terorismului. Chiar dacă acest transfer între autoritățile competente și destinatarii stabiliți în

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

(74) Fluxul transfrontalier de date cu caracter personal poate expune unui risc sporit capacitatea persoanelor fizice de a-și exercita drepturile în materie de protecție a datelor pentru a se proteja împotriva utilizării sau a divulgării ilegale a acestor date. În același timp, autoritățile de supraveghere pot constata că se află în imposibilitatea de a da curs unor plângeri sau de a efectua investigații referitoare la activitățile desfășurate în afara frontierelor lor. Eforturile lor de a conlucra în context transfrontalier pot fi, de asemenea, îngreunate de insuficiența competențelor de prevenire sau remediere și de caracterul eterogen al regimurilor juridice. Prin urmare, este necesar să se promoveze o cooperare mai strânsă între autoritățile de supraveghere a protecției datelor pentru a le ajuta să facă schimb de informații cu omologii lor străini.

(75) Instituirea în statele membre a unor autorități de supraveghere capabile să își exercite atribuțiile în deplină independență reprezintă un element esențial al protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Autoritățile de supraveghere ar trebui să monitorizeze aplicarea dispozițiilor adoptate în temeiul prezentei directive și ar trebui să contribuie la aplicarea ei consecventă în întreaga Uniune, în scopul asigurării protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. În acest scop, autoritățile de supraveghere ar trebui să coopereze între ele și cu Comisia.

(76) Statele membre pot încredința unei autorități de supraveghere deja înființate în temeiul Regulamentului (UE) 2016/679 responsabilitatea pentru sarcinile care urmează să fie îndeplinite de către autoritățile naționale de supraveghere care urmează a fi înființate în temeiul prezentei directive.

(77) Statele membre ar trebui să aibă posibilitatea de a institui mai multe autorități de supraveghere, pentru a reflecta structura lor constituțională, organizatorică și administrativă. Fiecare autoritate de supraveghere ar trebui să beneficieze de resurse financiare și umane, de localuri și de infrastructura necesare pentru îndeplinirea cu eficacitate a sarcinilor lor, inclusiv a celor legate de asistența reciprocă și cooperarea cu alte autorități de supraveghere în întreaga Uniune. Fiecare autoritate de supraveghere ar trebui să aibă un buget public anual distinct, care poate face parte din bugetul general de stat sau național.

(78) Autoritățile de supraveghere ar trebui să facă obiectul unui control independent sau al unor mecanisme de monitorizare în ceea ce privește cheltuielile lor financiare, cu condiția ca acest control financiar să nu le afecteze independența.

(79) Condițiile generale pentru membrul sau membrii autorității de supraveghere ar trebui stabilite prin dreptul intern și ar trebui, în special, să prevadă că respectivii membri ar trebui să fie numiți de parlamentul și/sau de guvernul ori de șeful de stat al statului membru în cauză, pe baza unei propuneri din partea guvernului sau a unui membru al guvernului ori din partea parlamentului sau camerei acestuia, ori de către un organism independent împuternicit prin dreptul intern să facă numirea prin intermediul unei proceduri transparente. În vederea asigurării independenței autorității de supraveghere, membrul sau membrii acesteia ar trebui să dea dovadă de integritate, nu ar trebui să întreprindă acțiuni incompatibile cu îndatoririle lor, iar, pe durata mandatului, nu ar trebui să desfășoare activități incompatibile, remunerate sau nu. În vederea asigurării independenței autorității de supraveghere, personalul ar trebui să fie ales de autoritatea de supraveghere, ceea ce poate include o intervenție din partea unui organism independent împuternicit în acest sens prin dreptul intern.

(80) Cu toate că prezenta directivă se aplică, de asemenea, activităților instanțelor naționale și ale altor autorități judiciare, prelucrarea datelor cu caracter personal nu ar trebui să fie de competența autorităților de supraveghere atunci când instanțele acționează în exercițiul funcției lor judiciare, în scopul asigurării independenței judecătorilor în îndeplinirea sarcinilor lor judiciare. Această derogare ar trebui să se limiteze la activități judiciare în cadrul acțiunilor în instanță și să nu se aplice altor activități în care judecătorii ar putea fi implicați, în conformitate cu dreptul intern. Statele membre ar trebui, de asemenea, să poată să prevadă faptul că nu este de competența autorității de supraveghere prelucrarea datelor cu caracter personal ale altor autorități judiciare independente care acționează în exercițiul funcției lor judiciare, de exemplu ministerul public. În orice caz, respectarea normelor prezentei directive de către instanțe și alte autorități judiciare independente face întotdeauna obiectul unei supravegheri independente în conformitate cu articolul 8 alineatul (3) din Cartă.

(81) Fiecare autoritate de supraveghere ar trebui să trateze plângerile depuse de orice persoană vizată și ar trebui să investigheze cazul sau să-l transmită autorității de supraveghere competente. Investigația în urma unei plângeri ar trebui să fie efectuată, sub rezerva controlului jurisdicțional, în măsura necesară fiecărui caz. Autoritatea de supraveghere ar trebui să informeze persoana vizată cu privire la evoluția și soluționarea plângerii într-un termen rezonabil. În eventualitatea în care cazul necesită o investigare suplimentară sau coordonarea cu o altă autoritate de supraveghere, ar trebui să se furnizeze informații intermediare persoanei vizate.

(82) Pentru a se asigura eficacitatea, fiabilitatea și consecvența monitorizării respectării și a aplicării prezentei directive în întreaga Uniune, în conformitate cu TFUE, astfel cum a fost interpretat de Curtea de Justiție, autorităților de supraveghere din fiecare stat membru ar trebui să le revină aceleași sarcini și competențe efective, inclusiv competențe de investigare, corective și de consiliere, care constituie mijloace necesare pentru îndeplinirea sarcinilor lor. Cu toate acestea, competențele acestora nu ar trebui să afecteze normele speciale de procedură penală, inclusiv cele referitoare la investigarea și urmărirea penală a infracțiunilor, sau independența justiției. Fără a aduce atingere competențelor autorităților de urmărire penală în temeiul dreptului intern, autoritățile de supraveghere ar trebui să aibă, de asemenea, competența de a aduce în atenția autorităților judiciare cazurile de încălcare a prezentei directive sau de a desfășura proceduri judiciare. Competențele autorităților de supraveghere ar trebui să fie exercitate în conformitate cu garanțiile procedurale adecvate prevăzute în dreptul Uniunii și în dreptul intern, în mod imparțial, echitabil și într-un termen rezonabil. În special, fiecare măsură ar trebui să fie adecvată, necesară și proporțională în scopul de a asigura conformitatea cu prezenta directivă, luând în considerare circumstanțele fiecărui caz în parte, să respecte dreptul oricărei persoane de a fi ascultată înainte de a fi luată orice măsură individuală care ar putea să îi aducă atingere și să evite costurile inutile și 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 din punct de vedere juridic ar trebui să facă obiectul controlului jurisdicțional în statul membru al autorității de supraveghere care a adoptat decizia.

(83) Autoritățile de supraveghere ar trebui să se sprijine reciproc în îndeplinirea sarcinilor care le revin și ar trebui să își acorde asistență reciprocă, pentru a se asigura aplicarea consecventă a dispozițiilor adoptate în temeiul prezentei directive.

(84) Comitetul, ar trebui să contribuie la aplicarea coerentă a prezentei directive în întreaga Uniune, inclusiv prin consilierea Comisiei și prin promovarea cooperării autorităților de supraveghere în întreaga Uniune.

(85) Orice persoană vizată ar trebui să aibă dreptul de a depune o plângere la o singură autoritate de supraveghere și la o cale de atac eficientă în conformitate cu articolul 47 din Cartă, în cazul în care persoana vizată consideră că sunt încălcate drepturile care îi revin în conformitate cu dispozițiile adoptate în temeiul prezentei directive sau în cazul în care autoritatea de supraveghere nu dă curs unei plângeri, respinge sau refuză parțial sau total o plângere sau nu acționează atunci când o astfel de acțiune este necesară pentru asigurarea protecției drepturilor persoanei vizate. Investigația în urma unei plângeri ar trebui să fie efectuată, făcând obiectul controlului jurisdicțional, în măsura în care este necesar, în funcție de caz. Autoritatea de supraveghere competentă ar trebui să informeze persoana vizată cu privire la evoluția și soluționarea plângerii într-un termen rezonabil. În eventualitatea în care cazul necesită o investigare suplimentară sau coordonarea cu o altă autoritate de supraveghere, ar trebui să se furnizeze informații intermediare persoanei vizate. În vederea facilitării depunerii plângerilor, fiecare autoritate de supraveghere ar trebui să ia măsuri precum punerea la dispoziție a unui formular de depunere a plângerii, care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.

(86) Orice persoană fizică sau juridică ar trebui să aibă dreptul la o cale de atac eficientă în fața instanței naționale competente, împotriva unei decizii a unei autorități de supraveghere care produce efecte juridice privind persoana respectivă. O astfel de decizie se referă în special la exercitarea competențelor de investigare, corective și de autorizare de către autoritatea de supraveghere sau la refuzul sau respingerea plângerilor. Cu toate acestea, dreptul respectiv nu privește alte măsuri ale autorităților de supraveghere care nu sunt obligatorii din punct de vedere juridic, cum ar fi avizele emise de autoritatea de supraveghere sau consultanța furnizată de aceasta. Acțiunile inițiate împotriva unei autorități de supraveghere ar trebui să fie aduse în fața instanțelor statului membru în care este stabilită autoritatea de supraveghere și ar trebui să se desfășoare în conformitate cu dreptul intern al statului membru respectiv. Respectivele instanțe ar trebui să își exercite competența deplină, care ar trebui să includă competența de a examina toate aspectele de fapt sau de drept care au relevanță pentru litigiul cu care acestea sunt sesizate.

(87) În cazul în care persoana vizată consideră că drepturile sale în temeiul prezentei directive sunt încălcate, aceasta ar trebui să aibă dreptul să mandateze un organism care are drept obiectiv asigurarea protecției drepturilor și a

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

(88) Orice daună pe care o persoană o poate suferi ca urmare a unei prelucrări care încalcă dispozițiile adoptate în temeiul prezentei directive ar trebui să fie despăgubită de operator sau de orice altă autoritate competentă în conformitate cu dreptul intern respectiv. Conceptul de „prejudiciu" ar trebui interpretat, în sens larg, din perspectiva jurisprudenței Curții de Justiție, într-un mod care să reflecte pe deplin obiectivele prezentei directive. Prezenta dispoziție nu aduce atingere niciunei acțiuni în despăgubire care rezultă din încălcarea altor norme din dreptul Uniunii sau din dreptul intern. Atunci când se face trimitere la o prelucrare care este ilegală sau care încalcă dispozițiile adoptate în temeiul prezentei directive, trimiterea vizează și prelucrarea care nu respectă actele de punere în aplicare adoptate în temeiul prezentei directive. Persoanele vizate ar trebui să primească despăgubiri integrale și efective pentru prejudiciile suferite.

(89) Ar trebui să se aplice sancțiuni oricărei persoane fizice sau juridice, de drept privat sau public, care încalcă prezenta directivă. Statele membre ar trebui să se asigure că sancțiunile sunt eficace, proporționale și disuasive și ar trebui să adopte toate măsurile pentru aplicarea sancțiunilor.

(90) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentei directive, Comisiei ar trebui să i confere competențe de executare referitor la nivelul adecvat de protecție oferit de o țară terță, de un teritoriu sau de un sector determinat din țara terță respectivă sau de o organizație internațională, formatul și procedurile pentru asistență reciprocă și modalitățile de schimb de informații prin mijloace electronice între autoritățile de supraveghere, precum și între autoritățile de supraveghere și comitet. Competențele respective ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([2]).

(91) Procedura de examinare ar trebui să fie utilizată pentru adoptarea actelor de punere în aplicare privind nivelul adecvat de protecție oferit de o țară terță, de un teritoriu sau de un sector determinat din țara terță respectivă sau de o organizație internațională, precum și privind formatul și procedurile pentru asistență reciprocă și modalitățile de schimb de informații prin mijloace electronice între autoritățile de supraveghere și între autoritățile de supraveghere și comitet, ținând seama de faptul că actele respective au un caracter general.

(92) Comisia ar trebui să adopte acte de punere în aplicare imediat aplicabile atunci când acest lucru se impune din motive imperative de urgență, în cazuri justificate în mod corespunzător referitoare la o țară terță, la un teritoriu sau la un sector determinat din țara terță respectivă sau la o organizație internațională care nu mai asigură un nivel de protecție adecvat.

(93) Întrucât obiectivele prezentei directive, și anume protejarea drepturilor și a libertăților fundamentale ale persoanelor fizice, în special dreptul acestora la protecția datelor cu caracter personal și asigurarea liberului schimb de date cu caracter personal de către autoritățile competente în cadrul Uniunii, nu pot fi realizate în mod satisfăcător de către statele membre ci, datorită amplorii sau a efectelor acțiunii, pot fi realizate mai bine la nivelul Uniunii, Uniunea poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este definit la articolul 5 din TUE. În conformitate cu principiul proporționalității, astfel cum este definit la articolul respectiv, prezenta directivă nu depășește ceea ce este necesar pentru realizarea obiectivelor menționate.

(94) Dispozițiile speciale din actele Uniunii adoptate în domeniul cooperării judiciare în materie penală și al cooperării polițienești, care au fost adoptate înainte de data adoptării prezentei directive, care reglementează prelucrarea datelor cu caracter personal între statele membre sau accesul autorităților desemnate ale statelor membre la

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

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

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

(95) În vederea asigurării unei protecții globale și consecvente a datelor cu caracter personal în cadrul Uniunii, acordurile internaționale care au fost încheiate de către statele membre înainte de data intrării în vigoare a prezentei directive și care respectă dispozițiile relevante din dreptul Uniunii aplicabil înainte de data respectivă ar trebui să rămână în vigoare până la data la care sunt modificate, înlocuite sau revocate.

(96) Statelor membre ar trebui să le fie acordat un termen de cel mult doi ani de la data intrării în vigoare a prezentei directive în vederea transpunerii sale. Prelucrările în derulare la data menționată ar trebui să fie aduse în conformitate cu prezenta directivă în termen de doi ani de la data intrării în vigoare a prezentei directive. Cu toate acestea, în cazul în care o astfel de prelucrare respectă dreptul Uniunii aplicabil înainte de data intrării în vigoare a prezentei directive, cerințele din prezenta directivă cu privire la consultarea prealabilă a autorității de supraveghere nu ar trebui să se aplice operațiunilor de prelucrare aflate deja în derulare la data menționată, având în vedere că respectivele cerințe, prin însăși natura lor, trebuie să fie îndeplinite înainte de prelucrare. În cazul în care statele membre aplică termenul mai lung pentru punerea în aplicare, care expiră după șapte ani de la data intrării în vigoare a prezentei directive, pentru îndeplinirea obligațiilor de înregistrare pentru sistemele de prelucrare automată instituite înainte de data respectivă, operatorul sau persoana împuternicită de către operator ar trebui să dispună de metode eficiente pentru a demonstra legalitatea prelucrării datelor, a permite monitorizarea proprie și a garanta integritatea și securitatea datelor, precum înregistrări sau alte forme de evidențe.

(97) Prezenta directivă se aplică fără a aduce atingere normelor privind combaterea abuzului sexual, a exploatării sexuale a copiilor și a pornografiei infantile, astfel cum se prevede în Directiva 2011/93/UE a Parlamentului European și a Consiliului ([3]).

(98) Decizia-cadru 2008/977/JAI a Consiliului ar trebui, prin urmare, să fie abrogată.

(99) În conformitate cu articolul 6a din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei în ceea ce privește spațiul de libertate, securitate și justiție, anexat la TUE și la TFUE, Regatului Unit și Irlandei nu le revin obligații în temeiul normelor stabilite în prezenta directivă referitoare la prelucrarea datelor cu caracter personal de către statele membre în exercitarea activităților care intră în domeniul de aplicare al părții a treia titlul V capitolul 4 sau 5 din TFUE, atât timp cât Regatului Unit sau Irlandei nu le revin obligații în temeiul normelor Uniunii privind formele de cooperare judiciară în materie penală sau de cooperare polițienească care necesită respectarea dispozițiilor stabilite în temeiul articolului 16 din TFUE.

(100) În conformitate cu articolele 2 și 2a din Protocolul nr. 22 privind poziția Danemarcei, astfel cum a fost anexat la TUE și la TFUE, Danemarcei nu îi revin obligații în temeiul normelor stabilite în prezenta directivă și acestea nu i se aplică în ceea ce privește prelucrarea datelor cu caracter personal de către statele membre în exercitarea activităților care intră sub incidența părții a treia titlul V capitolul 4 sau 5 din TFUE. Având în vedere faptul că prezenta directivă constituie o dezvoltare a acquis-ului Schengen, în temeiul părții a treia titlul V din TFUE, Danemarca decide, în conformitate cu articolul 4 din protocolul respectiv, în termen de șase luni de la adoptarea prezentei directive, dacă o va pune în aplicare în dreptul său intern.

(101) În ceea ce privește Islanda și Norvegia, prezenta directivă constituie o dezvoltare a dispozițiilor acquis-ului Schengen, în conformitate cu Acordul încheiat între Consiliul Uniunii Europene și de Republica Islanda și Regatul Norvegiei în ceea ce privește asocierea acestor două state la implementarea, aplicarea și dezvoltarea acquis-ului Schengen ([4]).

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

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

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

([4]) JO L 176, 10.7.1999, p. 36.

(102) În ceea ce privește Elveția, prezenta directivă constituie o dezvoltare a dispozițiilor acquis-ului Schengen, în conformitate cu Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen ([1]).

(103) În ceea ce privește Liechtenstein, prezenta directivă reprezintă o dezvoltare a dispozițiilor acquis-ului Schengen, astfel cum se prevede în Protocolul dintre Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen ([2]).

(104) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de cartă, astfel cum sunt consacrate în TFUE, în special dreptul la respectarea vieții private și de familie, dreptul la protecția datelor cu caracter personal, dreptul la o cale de atac eficientă și la un proces echitabil. Limitările aduse acestor drepturi sunt în conformitate cu articolul 52 alineatul (1) din Cartă întrucât sunt necesare pentru atingerea obiectivelor de interes general recunoscute de Uniune sau pentru a proteja drepturile și libertățile celorlalți.

(105) În conformitate cu Declarația politică comună a statelor membre și a Comisiei din 28 septembrie 2011 privind documentele explicative, statele membre s-au angajat să însoțească, în cazurile justificate, notificarea măsurilor de transpunere cu unul sau mai multe documente care să explice relația dintre componentele unei directive și părțile corespunzătoare din măsurile naționale de transpunere. În ceea ce privește prezenta directivă, legiuitorul consideră că este justificată transmiterea unor astfel de documente.

(106) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 și a emis un aviz la data de 7 martie 2012 ([3]).

(107) Prezenta directivă nu ar trebui să împiedice statele membre să pună în aplicare exercitarea, în cadrul procedurilor penale, a drepturilor persoanelor vizate cu privire la informare, acces și rectificarea sau ștergerea datelor cu caracter personal și restricționare a prelucrării, precum și eventualele limitări ale acestor drepturi în normele procedurale penale de drept intern,

ADOPTĂ PREZENTA DIRECTIVĂ:

CAPITOLUL I

Dispoziții generale

Articolul 1

Obiect și obiective

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

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

(a) protejează drepturile și libertățile fundamentale ale persoanelor fizice, în special dreptul acestora la protecția datelor cu caracter personal; și

(b) se asigură că schimbul de date cu caracter personal de către autoritățile competente în cadrul Uniunii, în cazul în care schimbul respectiv de informații este impus de dreptul Uniunii sau de dreptul intern, nu este limitat sau interzis din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

([1]) JO L 53, 27.2.2008, p. 52.
([2]) JO L 160, 18.6.2011, p. 21.
([3]) JO C 192, 30.6.2012, p. 7.

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

Articolul 2

Domeniul de aplicare

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

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

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

(a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii;

(b) de către instituțiile, organele, oficiile și agențiile Uniunii.

Articolul 3

Definiții

În sensul prezentei directive:

1. „date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

2. „prelucrare” înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

3. „restricționarea prelucrării” înseamnă marcarea datelor cu caracter personal stocate, cu scopul de a limita prelucrarea viitoare a acestora;

4. „creare de profiluri” înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau a preconiza aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, localizarea sau deplasările respectivei persoane fizice;

5. „pseudonimizare” înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, în măsura în care aceste informații suplimentare sunt stocate separat și fac obiectul unor măsuri de natură tehnică și organizatorică destinate să garanteze neatribuirea unei persoane fizice identificate sau identificabile;

6. „sistem de evidență a datelor” înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;

7. „autoritate competentă” înseamnă:

   (a) orice autoritate publică competentă în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor sau de executare a pedepselor, inclusiv în materie de protejare împotriva amenințărilor la adresa securității publice și de prevenire a acestora; sau

   (b) orice alt organism sau entitate împuternicit(ă) de dreptul intern să exercite autoritate publică și competențe publice în scopul în prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora;

8. „operator” înseamnă autoritatea competentă care, singură sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele de prelucrare sunt stabilite prin dreptul Uniunii sau prin dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi stabilite prin dreptul Uniunii sau prin dreptul intern;

9. „persoană împuternicită de către operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

10. „destinatar” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau un alt organism căruia îi sunt transmise datele cu caracter personal, fie că aceasta este sau nu o parte terță; sunt exceptate, cu toate acestea, autoritățile publice care pot primi date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul intern, iar prelucrarea datelor cu caracter personal respective de către acestea respectă normele aplicabile în materie de protecție a datelor în conformitate cu scopurile prelucrării;

11. „încălcarea securității datelor cu caracter personal” înseamnă o încălcare a securității, care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod;

12. „date genetice” înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice care oferă informații unice privind fiziologia sau sănătatea respectivei persoane fizice, astfel cum rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la acea persoană fizică;

13. „date biometrice” înseamnă date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a respectivei persoane fizice, cum ar fi imaginile faciale sau datele dactiloscopice;

14. „date privind sănătatea” înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv acordarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;

15. „autoritate de supraveghere” înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 41;

16. „organizație internațională” înseamnă o organizație și organismele sale subordonate reglementate de dreptul internațional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe țări sau în temeiul unui astfel de acord.

CAPITOLUL II

Principii

Articolul 4

Principii referitoare la prelucrarea datelor cu caracter personal

(1) Statele membre garantează că datele cu caracter personal:

(a) sunt prelucrate în mod legal și echitabil;

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

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

(d) sunt exacte și, dacă este necesar, sunt actualizate; trebuie să se ia toate măsurile rezonabile pentru a asigura faptul că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, să fie șterse sau rectificate fără întârziere;

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

(f) sunt prelucrate într-un mod care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

(2) Prelucrarea de către același operator sau de către un altul, în oricare dintre scopurile stabilite la articolul 1 alineatul (1), altele decât cele pentru care datele cu caracter personal au fost colectate, este permisă în măsura în care:

(a) operatorul este autorizat să prelucreze astfel de date cu caracter personal în scopul respectiv, în conformitate cu dreptul Uniunii sau cu dreptul intern; și

(b) prelucrarea este necesară și proporțională în raport cu respectivul alt scop, în conformitate cu dreptul Uniunii sau cu dreptul intern.

(3) Prelucrarea de către același operator sau de către un altul poate include arhivarea în interes public sau în scopuri științifice, statistice sau istorice pentru scopurile stabilite la articolul 1 alineatul (1), cu condiția unor garanții adecvate pentru drepturile și libertățile persoanelor vizate.

(4) Operatorul este responsabil de respectarea alineatelor (1), (2) și (3) și poate demonstra acest lucru.

Articolul 5

Termene pentru stocare și revizuire

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

Articolul 6

Distincția între diferitele categorii de persoane vizate

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

(a) persoane în privința cărora există motive serioase să se creadă că au săvârșit sau că urmează să săvârșească o infracțiune;

(b) persoane condamnate pentru săvârșirea unei infracțiuni;

(c) victime ale unei infracțiuni sau persoane în privința cărora, în baza anumitor fapte, există motive să se creadă că persoanele respective ar putea fi victimele unei infracțiuni; și

(d) alte părți care au legătură cu infracțiunea, ca de exemplu persoane care ar putea fi chemate să depună mărturie în cadrul anchetelor legate de infracțiuni sau în cadrul procedurilor penale ulterioare sau persoane care pot oferi informații cu privire la infracțiuni sau persoane care sunt în legătură sau asociate cu persoanele menționate la literele (a) și (b).

Articolul 7

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

(1) Statele membre garantează că se face distincție, pe cât posibil, între datele cu caracter personal bazate pe fapte și datele cu caracter personal bazate pe evaluări personale.

(2) Statele membre garantează că autoritățile competente iau toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte, incomplete sau nu mai sunt actuale nu sunt transmise sau puse la dispoziție. În acest scop, fiecare autoritate competentă verifică, în măsura în care este posibil, calitatea datelor cu caracter personal înainte ca acestea să fie transmise sau puse la dispoziție. În măsura în care acest lucru este posibil, în cadrul tuturor transmiterilor de date cu caracter personal, se adaugă informații necesare care permit autorității competente destinatare să evalueze gradul de exactitate, caracterul integral, gradul de fiabilitate și de actualitate al datelor cu caracter personal.

(3) În cazul în care se constată transmiterea unor date cu caracter personal incorecte sau transmiterea unor date cu caracter personal în mod ilegal, acest lucru se comunică de îndată destinatarului. Într-un astfel de caz, datele cu caracter personal sunt rectificate sau șterse sau prelucrarea este restricționată în conformitate cu articolul 16.

Articolul 8

Legalitatea prelucrării

(1) Statele membre garantează legalitatea prelucrării numai dacă și în măsura în care aceasta este necesară pentru îndeplinirea unei sarcini de către o autoritate competentă în scopurile stabilite la articolul 1 alineatul (1) și că aceasta se întemeiază pe dreptul Uniunii sau pe dreptul intern.

(2) Dreptul intern care reglementează prelucrarea care intră sub incidența prezentei directive precizează cel puțin obiectivele prelucrării, datele cu caracter personal care urmează să fie prelucrate și scopurile prelucrării.

Articolul 9

Condiții specifice de prelucrare

(1) Datele cu caracter personal colectate de autoritățile competente în scopurile stabilite la articolul 1 alineatul (1) nu se prelucrează în alte scopuri decât cele stabilite la articolul 1 alineatul (1), cu excepția cazurilor în care o astfel de prelucrare este autorizată în temeiul dreptului Uniunii sau al dreptului intern. În cazurile în care datele cu caracter personal sunt prelucrate în alte scopuri, prelucrării respective i se aplică Regulamentul (UE) 2016/679, cu excepția cazului în care prelucrarea este efectuată în cadrul unei activități care nu intră sub incidența dreptului Uniunii.

(2) În cazul în care autoritățile competente sunt împuternicite prin dreptul intern să îndeplinească alte atribuții decât cele aferente scopurilor stabilite la articolul 1 alineatul (1), pentru prelucrarea în astfel de scopuri se aplică Regulamentul (UE) 2016/679, inclusiv în ce privește prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, cu excepția cazului în care prelucrarea este efectuată în cadrul unei activități care nu intră sub incidența dreptului Uniunii.

(3) Statele membre garantează că, în cazul în care dreptul Uniunii sau dreptul intern aplicabil autorității competente care a transmis datele prevede condiții specifice de prelucrare, autoritatea competentă care a transmis datele informează destinatarul respectivelor date cu caracter personal cu privire la aceste condiții și la obligația de a le respecta.

(4) Statele membre garantează că autoritatea competentă care a transmis datele nu aplică condițiile prevăzute la alineatul (3) destinatarilor din alte state membre sau agențiilor, oficiilor și organismelor instituite în conformitate cu titlul V capitolele 4 și 5 din TFUE, altele decât cele aplicabile transmiterii similare de date în statul membru al autorității competente care a transmis datele.

Articolul 10

Prelucrarea de categorii speciale de date cu caracter personal

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

(a) este autorizată de dreptul Uniunii sau de dreptul intern;

(b) este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane fizice; sau

(c) prelucrarea respectivă se referă la date care sunt făcute publice în mod manifest de persoana vizată.

Articolul 11

Procesul decizional individual automatizat

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

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

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

CAPITOLUL III

Drepturile persoanei vizate

Articolul 12

Comunicare și modalități de exercitare a drepturilor persoanei vizate

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

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

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

(4) Statele membre garantează faptul că transmiterea informațiilor în conformitate cu articolul 13 și orice comunicare transmisă și măsură luată în temeiul articolelor 11, 14-18 și 31 este gratuită. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate:

(a) să perceapă o taxă rezonabilă care să țină cont de costurile administrative pentru transmiterea informațiilor sau a comunicărilor sau pentru luarea măsurilor solicitate; sau

(b) poate refuza să dea curs cererii.

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

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

Articolul 13

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

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

(a) identitatea și datele de contact ale operatorului;

(b) datele de contact ale responsabilului cu protecția datelor, după caz;

(c) scopurile în care sunt prelucrate datele cu caracter personal;

(d) dreptul de a depune o plângere în fața autorității de supraveghere și datele de contact ale autorității de supraveghere;

(e) existența dreptului de a solicita operatorului acces la datele cu caracter personal referitoare la persoana vizată ori rectificarea sau ștergerea acestor date sau restricționarea prelucrării lor.

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

(a) temeiul juridic al prelucrării;

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

(c) dacă este cazul, categoriile de destinatari ai datelor cu caracter personal, inclusiv în țări terțe sau organizații internaționale;

(d) în cazul în care este necesar, informații suplimentare, în special atunci când datele cu caracter personal sunt colectate fără știrea persoanei vizate.

(3) Statele membre pot adopta măsuri legislative de amânare, restricționare sau omitere a furnizării de informații persoanei vizate în conformitate cu alineatul (2) în măsura în care și atât timp cât o astfel de măsură constituie o măsură necesară și proporțională într-o societate democratică, ținând seama de drepturile fundamentale și de interesele legitime ale persoanei fizice, pentru:

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

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

(c) protejarea securității publice;

(d) protejarea securității naționale;

(e) protejarea drepturilor și libertăților celorlalți.

(4) Statele membre pot adopta măsuri legislative pentru a stabili categoriile de prelucrare care pot intra, integral sau parțial, sub incidența oricăreia dintre literele de la alineatul (3).

Articolul 14

Dreptul de acces al persoanei vizate

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

(a) scopurile și temeiul juridic al prelucrării;

(b) categoriile de date cu caracter personal vizate;

(c) destinatarii sau categoriile de destinatari cărora le-au fost divulgate datele cu caracter personal, în special destinatarii din țări terțe sau organizații internaționale;

(d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, în cazul în care acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

(e) existența dreptului de a solicita de la operator rectificarea sau ștergerea datelor cu caracter personal, sau restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată;

(f) dreptul de a depune o plângere în fața autorității de supraveghere și datele de contact ale autorității de supraveghere;

(g) comunicarea datelor cu caracter personal care sunt în curs de prelucrare și a oricărei informații disponibile cu privire la originea datelor.

Articolul 15

Limitarea dreptului de acces

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

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

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

(c) protejarea securității publice;

(d) protejarea securității naționale;

(e) protejarea drepturilor și libertăților celorlalți.

(2) Statele membre pot adopta măsuri legislative pentru a stabili categoriile de prelucrare care se pot intra, integral sau parțial, sub incidența literelor (a)-(e) de la alineatul (1).

(3) În cazurile prevăzute la alineatele (1) și (2), statele membre garantează că operatorul informează în scris persoana vizată, fără întârzieri nejustificate, cu privire la refuzarea sau limitarea accesului și la motivele refuzului sau ale limitării. Astfel de informații pot fi omise atunci când furnizarea lor ar contraveni unuia dintre scopurile de la alineatul (1). Statele membre garantează că operatorul informează persoana vizată cu privire la posibilitatea de a depune o plângere la autoritatea de supraveghere sau de a introduce o cale de atac judiciară.

(4) Statele membre garantează că operatorul justifică motivele de fapt și de drept pe care se întemeiază decizia. Aceste informații se pun la dispoziția autorităților de supraveghere.

Articolul 16

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

(1) Statele membre garantează persoanei vizate dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile prelucrării, statele membre garantează persoanei vizate dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

(2) Statele membre impun operatorului obligația de a șterge datele cu caracter personal fără întârzieri nejustificate și garantează persoanei vizate dreptul de a obține de la operator ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, în cazul în care prelucrarea încalcă dispozițiile adoptate în temeiul articolului 4, 8 sau 10, sau în cazul în care datele cu caracter personal trebuie șterse pentru îndeplinirea unei obligații legale care îi revine operatorului.

(3) În loc de ștergere, operatorul restricționează prelucrarea datelor cu caracter personal în cazul în care:

(a) exactitatea datelor cu caracter personal este contestată de persoana vizată, iar exactitatea sau inexactitatea datelor respective nu poate fi stabilită cu certitudine; sau

(b) datele cu caracter personal trebuie să fie păstrate ca mijloace de probă.

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

(4) Statele garantează că operatorul informează în scris persoana vizată cu privire la orice refuz de rectificare sau de ștergere a datelor cu caracter personal sau de restricționare a prelucrării și cu privire la motivele refuzului. Statele membre pot adopta măsuri legislative care restricționează, integral sau parțial, obligația de a furniza astfel de informații în măsura în care o astfel de restricționare a prelucrării constituie o măsură necesară și proporțională într-o societate democratică, ținându-se seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice vizate pentru:

(a) a evita obstrucționarea cercetărilor, anchetelor sau procedurilor oficiale sau juridice;

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

(c) a proteja securitatea publică;

(d) a proteja securitatea națională;

(e) a proteja drepturile și libertățile celorlalți.

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

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

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

Articolul 17

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

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

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

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

Articolul 18

Drepturile persoanei vizate în cadrul investigațiilor și procedurilor penale

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

CAPITOLUL IV

Operatorul și persoana împuternicită de către operator

Secțiunea 1

Obligații generale

Articolul 19

Obligațiile operatorului

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

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

Articolul 20

Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

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

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

Articolul 21

Operatori asociați

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

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

Articolul 22

Persoana împuternicită de către operator

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

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

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

(a) acționează numai la instrucțiunile operatorului;

(b) garantează faptul că persoanele autorizate să prelucreze date cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație legală de confidențialitate corespunzătoare;

(c) asistă operatorul prin orice mijloace adecvate pentru a asigura respectarea dispozițiilor privind drepturile persoanei vizate;

(d) la alegerea operatorului, șterge sau returnează toate datele cu caracter personal operatorului după încetarea furnizării serviciilor de prelucrare a datelor și elimină copiile existente, cu excepția cazului în care dreptului Uniunii sau dreptul intern prevede stocarea datelor cu caracter personal;

(e) pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea prezentului articol;

(f) respectă condițiile menționate la alineatele (2) și (3) pentru recrutarea unei alte persoane împuternicite de către operator.

(4) Contractul sau un alt act juridic menționat la alineatul (3) se întocmește în scris și poate fi pus la dispoziție în format electronic.

(5) În cazul în care o persoană împuternicită de către operator stabilește, cu încălcarea prezentei directive, scopurile și mijloacele de prelucrare, persoana împuternicită este considerată ca fiind operator în ceea ce privește prelucrarea respectivă.

Articolul 23

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

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

Articolul 24

Evidențe ale activităților de prelucrare

(1) Statele membre garantează că operatorul menține o evidență a tuturor categoriilor de activități de prelucrare aflate în responsabilitatea sa. Respectiva evidență cuprinde toate informațiile următoare:

(a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat și ale responsabilului cu protecția datelor;

(b) scopurile prelucrării;

(c) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;

(d) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;

(e) acolo unde este cazul, utilizarea creării de profiluri;

(f) acolo unde este cazul, categoriile de transferuri de date cu caracter personal către o țară terță sau o organizație internațională;

(g) indicarea temeiului juridic al operațiunii de prelucrare, inclusiv transferurile, pentru care sunt destinate datele cu caracter personal;

(h) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date cu caracter personal;

(i) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 29 alineatul (1).

(2) Statele membre garantează că fiecare persoană împuternicită de către operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, evidență care cuprinde:

(a) numele și datele de contact ale persoanei sau persoanelor împuternicite de către operator, ale fiecărui operator în numele căruia acționează această persoană și, după caz, cele ale responsabilului cu protecția datelor;

(b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;

(c) acolo unde este cazul, transferurile de date cu caracter personal către o țară terță sau către o organizație internațională, inclusiv, identificarea țării terțe sau a organizației internaționale respective, atunci când au primit instrucțiuni explicite în acest sens de la operator;

(d) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 29 alineatul (1).

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

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

Articolul 25

Înregistrarea

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

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

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

Articolul 26

Cooperarea cu autoritatea de supraveghere

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

Articolul 27

Evaluarea impactului asupra protecției datelor

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

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

Articolul 28

Consultarea prealabilă a autorității de supraveghere

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

(a) o evaluare a impactului asupra protecției datelor, prevăzută la articolul 27, indică faptul că prelucrarea ar genera un risc ridicat în absența măsurilor luate de operator pentru atenuarea riscului sau

(b) un tip de prelucrare, în special în cazul în care se utilizează noi tehnologii, mecanisme sau proceduri, implică un risc ridicat la adresa drepturilor și libertăților persoanelor vizate.

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

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

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

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

Secțiunea 2

Securitatea datelor cu caracter personal

Articolul 29

Securitatea prelucrării

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

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

(a) să împiedice accesul persoanelor neautorizate la echipamentele de prelucrare utilizate pentru prelucrare („controlul accesului la echipamente”);

(b) să împiedice orice citire, copiere, modificare sau eliminare neautorizată a suporturilor de date („controlul suporturilor de date”);

(c) să împiedice introducerea neautorizată de date cu caracter personal și inspectarea, modificarea sau ștergerea neautorizată a datelor cu caracter personal stocate („controlul stocării”);

(d) să împiedice utilizarea sistemelor de prelucrare automată de către persoane neautorizate cu ajutorul echipamentelor de comunicare a datelor („controlul utilizatorului”);

(e) să asigure faptul că persoanele autorizate să utilizeze un sistem de prelucrare automată au acces numai la datele cu caracter personal pentru care au autorizare („controlul accesului la date”);

(f) să asigure că este posibilă verificarea și identificarea organismelor cărora le-au fost transmise sau puse la dispoziție sau s-ar putea să le fie transmise sau puse la dispoziție date cu caracter personal utilizându-se echipamente de comunicare a datelor („controlul comunicării”);

(g) să asigure că este posibil ulterior să se verifice și să se identifice datele cu caracter personal introduse în sistemele de prelucrare automată, momentul introducerii datelor cu caracter personal și entitatea care le-a introdus („controlul introducerii datelor”);

(h) să împiedice citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transferurilor de date cu caracter personal sau în timpul transportării suporturilor de date („controlul transportării”);

(i) să asigure posibilitatea recuperării sistemelor instalate în cazul unei întreruperi („recuperarea”);

(j) să asigure funcționarea sistemului, raportarea defecțiunilor de funcționare (fiabilitate) și imposibilitatea coruperii datelor cu caracter personal stocate din cauza funcționării defectuoase a sistemului („integritate”).

Articolul 30

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

(1) Statele membre garantează că, în cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere fără întârzieri nejustificate și, în cazul în care este posibil, în cel mult 72 de ore după ce a luat cunoștință de aceasta, cu excepția cazului în care încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc la adresa drepturilor și libertăților persoanelor fizice. În cazul notificarea se efectuează în termen de 72 de ore, aceasta va fi însoțită de o justificare a întârzierii.

(2) Persoana împuternicită de către operator înștiințează operatorul fără întârzieri nejustificate după ce ia cunoștință de o încălcare a securității datelor cu caracter personal.

(3) Notificarea menționată la alineatul (1) trebuie, cel puțin:

(a) să descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ de persoane vizate în cauză, precum și categoriile și numărul aproximativ de înregistrări de date cu caracter personal în cauză;

(b) să comunice numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;

(c) să descrie consecințele probabile ale încălcării securității datelor cu caracter personal;

(d) să descrie măsurile luate sau propuse de operator pentru a remedia încălcarea securității datelor cu caracter personal, inclusiv, dacă este cazul, măsuri pentru a atenua eventualele efecte adverse ale acesteia.

(4) În cazul în care și în măsura în care furnizarea informațiilor în același timp nu este posibilă, informațiile pot fi furnizate treptat, fără întârzieri nejustificate.

(5) Statele membre garantează că operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, menționate la alineatul (1), care cuprind o descriere a situației în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație trebuie să permită autorității de supraveghere să verifice respectarea prezentului articol.

(6) Statele membre garantează că, în cazul în care încălcarea securității datelor implică date cu caracter personal care au fost transmise de un operator dintr-un alt stat membru sau către un astfel de operator, informațiile prevăzute la alineatul (3) se comunică operatorului din respectivul stat membru fără întârzieri nejustificate.

Articolul 31

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

(1) Statele membre garantează că, în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, operatorul informează persoana vizată, fără întârzieri nejustificate, cu privire la încălcarea securității datelor cu caracter personal.

(2) În informarea transmisă persoanei vizate, prevăzută la alineatul (1) din prezentul articol, se include o descriere într-un limbaj simplu și clar a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile și măsurile menționate la articolul 30 alineatul (3) literele (b), (c) și (d).

(3) Informarea persoanei vizate, menționată la alineatul (1), nu este necesară în cazul în care este îndeplinită oricare dintre următoarele condiții:

(a) operatorul a pus în aplicare măsuri tehnologice și organizatorice adecvate de protecție, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

(b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat la adresa drepturilor și libertăților persoanelor vizate menționat la alineatul (1) nu mai este susceptibil să se materializeze;

(c) aceasta ar necesita un efort disproporționat. În acest caz, informarea se înlocuiește printr-o informare publică sau o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

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

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

Secțiunea 3

Responsabilul cu protecția datelor

Articolul 32

Desemnarea responsabilului cu protecția datelor

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

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

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

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

Articolul 33

Funcția responsabilului cu protecția datelor

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

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

Articolul 34

Sarcinile responsabilului cu protecția datelor

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

(a) informarea și consilierea operatorului și a angajaților care efectuează prelucrarea cu privire la obligațiile care le revin în temeiul prezentei directive și al altor dispoziții de drept al Uniunii sau de drept intern privind protecția datelor;

(b) monitorizarea respectării prezentei directive, a altor dispoziții de drept al Uniunii sau de drept intern privind protecția datelor și a politicilor operatorului în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

(c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu articolul 27;

(d) cooperarea cu autoritatea de supraveghere;

(e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 28, precum și, dacă este cazul, acordarea consultanței cu privire la orice altă chestiune.

CAPITOLUL V

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

Articolul 35

Principii generale pentru transferurile de date cu caracter personal

(1) Statele membre garantează că orice transfer de date cu caracter personal de către autoritățile competente, care sunt în curs de prelucrare sau care sunt destinate prelucrării după transferul către o țară terță sau către o organizație internațională, inclusiv transferurilor ulterioare către o altă țară terță sau organizație internațională, poate avea loc numai sub rezerva respectării altor dispoziții ale prezentei directive, în cazul în care sunt îndeplinite condițiile prevăzute în prezentul capitol, și anume:

(a) transferul este necesar în scopurile stabilite la articolul 1 alineatul (1);

(b) datele cu caracter personal sunt transferate unui operator într-o țară terță sau unei organizații internaționale care este o autoritate competentă în sensul articolului 1 alineatul (1);

(c) în cazul în care datele cu caracter personal sunt transmise sau puse la dispoziție din alt stat membru, acel stat membru a autorizat în prealabil efectuarea transferului, în conformitate cu dreptul său intern;

(d) Comisia a adoptat o decizie privind caracterul adecvat al nivelului de protecție, în temeiul articolului 36, sau, în absența unei astfel de decizii, există sau se oferă garanții adecvate în temeiul articolului 37 sau, în absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 36 sau a unor garanții adecvate în conformitate cu articolul 37, se aplică derogări pentru situații speciale în conformitate cu articolul 38; și

(e) în cazul unui transfer ulterior către o altă țară terță sau organizație internațională, autoritatea competentă care a realizat transferul inițial sau o altă autoritate competentă din același stat membru autorizează transferul ulterior, ținând seama în mod corespunzător de toți factorii relevanți, inclusiv de gravitatea infracțiunii, de scopul în care datele cu caracter personal au fost transferate inițial și de nivelul de protecție a datelor cu caracter personal din țara terță sau din organizația internațională către care sunt transferate ulterior datele cu caracter personal.

(2) Statele membre garantează că transferurile fără autorizarea prealabilă de către un alt stat membru, în conformitate cu litera (c) de la alineatul (1), sunt permise numai dacă transferul de date cu caracter personal este necesar pentru prevenirea unei amenințări imediate și grave la adresa securității publice a unui stat membru sau a unei țări terțe sau a intereselor fundamentale ale unui stat membru, iar autorizarea prealabilă nu poate fi obținută în timp util. Autoritatea responsabilă pentru acordarea unei autorizări prealabile este informată fără întârziere.

(3) Toate dispozițiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice garantat prin prezenta directivă nu este subminat.

Articolul 36

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

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

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

(a) statul de drept, respectarea drepturilor omului și a libertăților fundamentale, legislația relevantă, atât generală, cât și sectorială, inclusiv privind securitatea publică, apărarea, securitatea națională și dreptul penal și accesul autorităților publice la datele cu caracter personal, precum și punerea în aplicare a acestei legislații, a normelor de protecție a datelor, a normelor profesionale și a măsurilor de securitate, inclusiv a normelor privind transferul ulterior de date cu caracter personal către o altă țară terță sau organizație internațională, care sunt respectate în țara respectivă sau de organizația internațională respectivă, jurisprudența, precum și drepturile efective și opozabile ale persoanelor vizate și reparații efective pe cale administrativă și judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate;

(b) existența și funcționarea efectivă a uneia sau a mai multor autorități de supraveghere independente în țara terță sau sub incidența cărora intră o organizație internațională, cu responsabilitate pentru asigurarea și impunerea respectării normelor de protecție a datelor, incluzând competențe adecvate de sancționare, pentru acordarea de asistență și consiliere persoanelor vizate cu privire la exercitarea drepturilor acestora și pentru cooperarea cu autoritățile de supraveghere din statele membre; și

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

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

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

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

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

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

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

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

Articolul 37

Transferuri sub rezerva unor garanții adecvate

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

(a) s-au prezentat garanții adecvate în ceea ce privește protecția datelor cu caracter personal printr-un act cu caracter juridic obligatoriu; sau

(b) operatorul a evaluat toate circumstanțele aferente transferului de date cu caracter personal și a concluzionat că există garanții adecvate în ceea ce privește protecția datelor cu caracter personal.

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

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

Articolul 38

Derogări pentru situații specifice

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

(a) pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane;

(b) pentru protejarea intereselor legitime ale persoanei vizate, în cazul în care dreptul statului membru care transferă datele cu caracter personal prevede acest lucru;

(c) pentru prevenirea unei amenințări imediate și grave la adresa securității publice a unui stat membru sau a unei țări terțe;

(d) în cazuri individuale în scopurile stabilite la articolul 1 alineatul (1); sau

(e) într-un caz individual pentru constatarea, exercitarea sau apărarea unui drept în instanță privind scopurile stabilite la articolul 1 alineatul (1).

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

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

Articolul 39

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

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

(a) transferul este strict necesar pentru executarea unei sarcini de către autoritatea competentă care transferă datele, astfel cum este prevăzut de dreptul Uniunii sau de dreptul intern în scopurile prevăzute la articolul 1 alineatul (1);

(b) autoritatea competentă care transferă datele stabilește că niciunul dintre drepturile și libertățile fundamentale ale persoanei vizate în cauză nu prevalează în fața interesului public care necesită transferul în cazul respectiv;

(c) autoritatea competentă care transferă datele consideră că transferul către o autoritate din țara terță, care este competentă în scopurile menționate la articolul 1 alineatul (1), este ineficient sau necorespunzător, în special din cauză că transferul nu poate fi realizat în timp util;

(d) autoritatea din țara terță, care este competentă în scopurile menționate la articolul 1 alineatul (1), este informată fără întârzieri nejustificate, cu excepția cazului în care această măsură este ineficientă sau necorespunzătoare; și

(e) autoritatea competentă care transferă datele informează destinatarul cu privire la scopul sau scopurile determinate exclusive în care aceasta din urmă poate să prelucreze datele cu caracter personal, cu condiția ca o astfel de prelucrare să fie necesară.

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

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

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

Articolul 40

Cooperarea internațională în domeniul protecției datelor cu caracter personal

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

(a) elaborarea de mecanisme de cooperare internațională pentru a facilita asigurarea efectivă a respectării legislației privind protecția datelor cu caracter personal;

(b) acordarea de asistență internațională reciprocă în asigurarea respectării legislației din domeniul protecției datelor cu caracter personal, inclusiv prin notificări, transferul reclamațiilor, asistență în anchete și schimb de informații, sub rezerva unor garanții adecvate pentru protecția datelor cu caracter personal și a altor drepturi și libertăți fundamentale;

(c) implicarea părților interesate relevante în discuțiile și activitățile care au ca scop consolidarea cooperării internaționale în vederea asigurării respectării legislației din domeniul protecției datelor cu caracter personal;

(d) promovarea schimburilor de legislație și practici în materie de protecție a datelor cu caracter personal și a documentării cu privire la acestea, inclusiv cu privire la conflictele de jurisdicție cu țările terțe.

CAPITOLUL VI

Autorități de supraveghere independente

Secțiunea 1

Statut independent

Articolul 41

Autoritatea de supraveghere

(1) Fiecare stat membru garantează că una sau mai multe autorități publice independente sunt responsabile de monitorizarea aplicării prezentei directive, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea și în vederea facilitării liberei circulații a datelor cu caracter personal în cadrul Uniunii („autoritatea de supraveghere”).

(2) Fiecare autoritate de supraveghere contribuie la aplicarea consecventă a prezentei directive în întreaga Uniune. În acest scop, autoritățile de supraveghere cooperează atât între ele, cât și cu Comisia, în conformitate cu capitolul VII.

(3) Statele membre pot să prevadă că o autoritate de supraveghere instituită în conformitate cu Regulamentul (UE) 2016/679 constituie autoritatea de supraveghere menționată în prezenta directivă și își asumă responsabilitatea pentru sarcinile autorității de supraveghere care urmează să fie instituită în conformitate cu alineatul (1) din prezentul articol.

(4) În cazul în care un stat membru instituie mai multe autorități de supraveghere, statul membru respectiv desemnează autoritatea de supraveghere care reprezintă autoritățile respective în cadrul comitetului menționat la articolul 51.

Articolul 42

Independență

(1) Fiecare stat membru garantează că autoritatea sa de supraveghere beneficiază de independență deplină în îndeplinirea sarcinilor și exercitarea competențelor care le revin în conformitate cu prezenta directivă.

(2) Statele membre garantează că membrii autorităților lor de supraveghere, în îndeplinirea sarcinilor și în exercitarea competențelor care le revin în conformitate cu prezenta directivă, rămân independenți de orice influență externă directă sau indirectă și nici nu solicită, nici nu acceptă instrucțiuni de la nimeni.

(3) Membrii autorităților de supraveghere din statele membre nu întreprind acțiuni incompatibile cu îndatoririle lor, iar, pe durata mandatului, nu desfășoară activități incompatibile, remunerate sau nu.

(4) Fiecare stat membru garantează că autoritatea sa de supraveghere beneficiază de resurse umane, tehnice și financiare, de un sediu și de infrastructura necesară pentru îndeplinirea sarcinilor și exercitarea competențelor în mod eficace, inclusiv a celor care urmează să fie realizate în contextul asistenței reciproce, al cooperării și al participării în cadrul comitetului.

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

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

Articolul 43

Condiții generale aplicabile membrilor autorității de supraveghere

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

— de către parlament;

— de către guvern;

— de către șeful statului membru în cauză; sau

— de către un organism independent împuternicit prin dreptul intern să facă numirea.

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

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

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

Articolul 44

Norme privind instituirea autorității de supraveghere

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

(a) instituirea autorității sale de supraveghere;

(b) calificările și condițiile de eligibilitate necesare pentru a fi numit membru al autorității sale de supraveghere;

(c) normele și procedurile pentru numirea membrului sau a membrilor autorității sale de supraveghere;

(d) durata mandatului membrului sau al membrilor autorității sale de supraveghere, care nu poate fi mai mică de patru ani, cu excepția primului mandat după 6 mai 2016, care poate fi mai scurt în cazul în care acest lucru este necesar pentru a proteja independența autorității de supraveghere printr-o procedură de numiri eșalonate;

(e) dacă și de câte ori este eligibil pentru reînnoire mandatul membrului sau membrilor autorității sale de supraveghere; și

(f) condițiile care reglementează obligațiile membrului sau membrilor și ale personalului autorității sale de supraveghere, interdicțiile privind acțiunile, ocupațiile și beneficiile incompatibile cu acestea în cursul mandatului și după încetarea acestuia, precum și normele care reglementează încetarea activității profesionale.

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

Secțiunea 2

Abilități, sarcini și competențe

Articolul 45

Abilități

(1) Fiecare stat membru garantează că autoritatea sa de supraveghere este abilitată să îndeplinească sarcinile și să exercite competențele care îi revin în conformitate cu prezenta directivă pe teritoriul respectivului stat membru.

(2) Fiecare stat membru garantează că autorității sale de supraveghere îi revine competența să supravegheze operațiunile de prelucrare ale instanțelor atunci când acestea acționează în exercițiul funcției lor judiciare. Statele membre pot să stabilească dispoziții potrivit cărora autorităților sale de supraveghere nu le revine competența să supravegheze operațiunile de prelucrare ale altor autorități judiciare independente atunci când acestea acționează în exercițiul funcției lor judiciare.

Articolul 46

Sarcini

(1) Fiecare stat membru garantează, pe teritoriul său, că autoritatea sa de supraveghere:

(a) monitorizează și asigură respectarea prezentei directive și a măsurilor de punere în aplicare aferente acesteia;

(b) promovează acțiuni de sensibilizare și de înțelegere în rândul publicului a riscurilor, normelor, garanțiilor și drepturilor în materie de prelucrare;

(c) oferă consiliere, în conformitate cu dreptul intern, parlamentului național, guvernului și altor instituții și organisme cu privire la măsurile legislative și administrative referitoare la protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea;

(d) promovează acțiuni de sensibilizare a operatorilor și a persoanelor împuternicite de aceștia cu privire la obligațiile care le revin în temeiul prezentei directive;

(e) furnizează informații, la cerere, oricărei persoane vizate în legătură cu exercitarea drepturilor sale în temeiul prezentei directive și, dacă este cazul, cooperează cu autoritățile de supraveghere din alte state membre în acest scop;

(f) tratează plângerile depuse de o persoană vizată sau de un organism, o organizație sau o asociație, în conformitate cu articolul 55, investighează într-o măsură adecvată obiectul plângerii și informează persoana care a depus plângerea cu privire la evoluția și rezultatul investigației, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigații mai amănunțite sau coordonarea cu o altă autoritate de supraveghere;

(g) verifică legalitatea prelucrării în conformitate cu articolul 17 și informează persoana vizată, într-un termen rezonabil, cu privire la rezultatul verificării în temeiul alineatului (3) al articolului respectiv sau la motivele pentru care nu a avut loc verificarea;

(h) cooperează, inclusiv prin schimb de informații, cu alte autorități de supraveghere și își oferă reciproc asistență pentru a asigura consecvența aplicării și respectării prezentei directive;

(i) desfășoară investigații privind aplicarea prezentei directive, inclusiv pe baza unor informații primite de la o altă autoritate de supraveghere sau autoritate publică;

(j) monitorizează evoluțiile relevante, în măsura în care acestea au impact asupra protecției datelor cu caracter personal, în special evoluția tehnologiilor informațiilor și comunicațiilor;

(k) oferă consiliere cu privire la operațiunile de prelucrare menționate la articolul 28; și

(l) contribuie la activitățile comitetului.

(2) Fiecare autoritate de supraveghere facilitează depunerea plângerilor menționate la alineatul (1) litera (f) prin măsuri precum punerea la dispoziție a unui formular de depunere a plângerii, care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.

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

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

Articolul 47

Competențe

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

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

(a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la probabilitatea ca operațiunile de prelucrare preconizate să încalce dispozițiile adoptate în temeiul prezentei directive;

(b) de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile adoptate în temeiul prezentei directive, specificând, după caz, modalitatea și termenul-limită pentru aceasta; în special dispunând rectificarea sau ștergerea datelor cu caracter personal, sau restricționarea prelucrării, în conformitate cu articolul 16;

(c) de a impune o limitare temporară sau definitivă, inclusiv o interdicție, în ce privește prelucrarea.

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

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

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

Articolul 48

Denunțarea cazurilor de încălcare

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

Articolul 49

Rapoarte de activitate

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

CAPITOLUL VII

Cooperarea

Articolul 50

Asistență reciprocă

(1) Fiecare stat membru garantează că autoritățile sale de supraveghere își furnizează reciproc informațiile relevante și asistență pentru a pune în aplicare și a aplica prezenta directivă în mod consecvent și instituie măsuri de cooperare eficace între ele. Asistența reciprocă se referă, în special, la cereri de informații și măsuri de supraveghere, cum ar fi cereri în vederea efectuării de consultări, inspecții și investigații.

(2) Fiecare stat membru garantează luarea de către fiecare autoritate de supraveghere a tuturor măsurilor corespunzătoare necesare pentru a răspunde cererii unei alte autorități de supraveghere, fără întârziere și în cel mult o lună de la data primirii cererii. Astfel de măsuri pot include, în special, transmiterea informațiilor relevante privind desfășurarea unei investigații.

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

(4) O autoritate de supraveghere căreia i se adresează o cerere de asistență nu poate refuza să îi dea curs, cu excepția cazului în care:

(a) nu are competență cu privire la obiectul cererii sau la măsurile pe care este solicitată să le execute; sau

(b) a da curs cererii ar încălca prezenta directivă sau dreptul Uniunii sau dreptul intern sub incidența căruia intră autoritatea de supraveghere care a primit cererea.

(5) Autoritatea de supraveghere căreia i s-a adresat cererea informează autoritatea de supraveghere care a transmis cererea cu privire la rezultate sau, după caz, la progresele înregistrate ori măsurile întreprinse pentru a răspunde cererii. În cazul unui refuz în temeiul alineatului (4), autoritatea de supraveghere căreia i s-a adresat cererea explică motivele de refuz.

(6) Autoritățile de supraveghere cărora li s-a adresat o cerere furnizează, de regulă, informațiile solicitate de alte autorități de supraveghere prin mijloace electronice, utilizând un formular-standard.

(7) Pentru acțiunile întreprinse în urma unei cereri de asistență reciprocă autoritățile de supraveghere cărora li s-a adresat o cerere nu percep taxă. Autoritățile de supraveghere pot conveni asupra unor compensații reciproce în cazul unor cheltuieli specifice rezultate în urma acordării de asistență reciprocă în situații excepționale.

(8) Comisia poate preciza, prin intermediul unor acte de punere în aplicare, forma și procedurile pentru asistența reciprocă menționată în prezentul articol, precum și modalitățile de schimb de informații prin mijloace electronice între autoritățile de supraveghere și între autoritățile de supraveghere și comitet. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 58 alineatul (2).

Articolul 51

Sarcinile comitetului

(1) Comitetul instituit prin Regulamentul (UE) 2016/679 îndeplinește, în ceea ce privește prelucrarea care intră sub incidența prezentei directive, toate sarcinile următoare:

(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, la cererea unuia dintre membrii săi sau la cererea Comisiei, orice chestiune referitoare la aplicarea prezentei directive și emite orientări, recomandări și bune practici pentru a încuraja aplicarea consecventă a prezentei directive;

(c) elaborează orientări destinate autorităților de supraveghere, referitoare la aplicarea măsurilor menționate la articolul 47 alineatele (1) și (3);

(d) emite orientări, recomandări și bune practici, în conformitate cu litera (b) de la prezentul alineat, pentru stabilirea cazurilor de încălcare a securității datelor cu caracter personal și pentru determinarea întârzierilor nejustificate menționate la articolul 30 alineatele (1) și (2), precum și pentru circumstanțele speciale în care un operator sau o persoană împuternicită de către operator are obligația de a notifica încălcarea securității datelor cu caracter personal;

(e) emite orientări, recomandări și bune practici, în conformitate cu litera (b) de la prezentul alineat, în ceea ce privește circumstanțele în care o încălcare a securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor menționate la articolul 31 alineatul (1);

(f) revizuiește aplicarea practică a orientărilor, a recomandărilor și a bunelor practici menționate la literele (b) și (c);

(g) prezintă Comisiei un aviz pentru evaluarea caracterului adecvat al nivelului de protecție dintr-o țară terță, un teritoriu sau unul sau mai multe sectoare determinate dintr-o țară terță, sau o organizație internațională, inclusiv pentru a evalua dacă o țară terță, un teritoriu, un sector determinat sau o organizație internațională nu mai asigură un nivel de protecție adecvat.

(h) promovează cooperarea și schimbul eficient bilateral și multilateral de informații și cele mai bune practici între autoritățile de supraveghere;

(i) promovează programe comune de formare și facilitează schimburile de personal între autoritățile de supraveghere și, după caz, cu autoritățile de supraveghere ale țărilor terțe sau cu organizațiile internaționale;

(j) promovează schimbul de cunoștințe și de documente privind dreptul și practicile în materie de protecție a datelor cu autoritățile de supraveghere a protecției datelor la nivel mondial.

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

(2) În cazul în care Comisia solicită consiliere din partea comitetului, aceasta poate indica un termen limită, ținând seama de caracterul urgent al chestiunii.

(3) Comitetul își transmite avizele, orientările, recomandările și bunele practici Comisiei și comitetului menționat la articolul 58 alineatul (1) și le publică.

(4) Comisia informează comitetul cu privire la măsurile pe care le-a luat în urma avizelor, orientărilor, recomandărilor și bunelor practici emise de comitet.

CAPITOLUL VIII

Căi de atac, răspundere și sancțiuni

Articolul 52

Dreptul de a depune o plângere la o autoritate de supraveghere

(1) Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, statele membre garantează oricărei persoane vizate dreptul de a depune o plângere la o singură autoritate de supraveghere, în cazul în care persoana vizată consideră că prelucrarea datelor cu caracter personal care o vizează încalcă dispozițiile adoptate în temeiul prezentei directive.

(2) Statele membre garantează că, în cazul în care plângerea nu este depusă la autoritatea de supraveghere competentă în temeiul articolului 45 alineatul (1), autoritatea de supraveghere la care a fost depusă plângerea o transmite autorității de supraveghere competente, fără întârzieri nejustificate. Persoana vizată este informată cu privire la transmitere.

(3) Statele membre garantează că autoritatea de supraveghere la care s-a depus plângerea oferă, la cerere, asistență suplimentară persoanei vizate.

(4) Persoana vizată este informată de către autoritatea de supraveghere competentă cu privire la evoluția și rezultatul plângerii, inclusiv cu privire la posibilitatea de a exercita o cale de atac judiciară în conformitate cu articolul 53.

Articolul 53

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

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

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

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

Articolul 54

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

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

Articolul 55

Reprezentarea persoanelor vizate

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

Articolul 56

Dreptul la despăgubiri

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

Articolul 57

Sancțiuni

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

CAPITOLUL IX

Acte de punere în aplicare

Articolul 58

Procedura comitetului

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

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

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

CAPITOLUL X

Dispoziții finale

Articolul 59

Abrogarea Deciziei-cadru 2008/977/JAI

(1) Decizia-cadru 2008/977/JAI se abrogă începând cu 6 mai 2018.

(2) Trimiterile la decizia abrogată menționată la alineatul (1) se interpretează ca trimiteri la prezenta directivă.

Articolul 60

Actele Uniunii aflate deja în vigoare

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

Articolul 61

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

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

Articolul 62

Rapoartele Comisiei

(1) Până la 6 mai 2022 și, ulterior, la fiecare patru ani, Comisia transmite Parlamentului European și Consiliului, un raport privind evaluarea și revizuirea prezentei directive. Rapoartele sunt făcute publice.

(2) În contextul evaluărilor și revizuirilor menționate la alineatul (1), Comisia examinează, în special, aplicarea și funcționarea capitolului V privind transferul datelor cu caracter personal către țări terțe sau organizații internaționale, acordând o atenție deosebită deciziilor adoptate în temeiul articolului 36 alineatul (3) și al articolului 39.

(3) În scopul alineatelor (1) și (2), Comisia poate solicita informații de la statele membre și de la autoritățile de supraveghere.

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

(5) Comisia transmite, dacă este necesar, propuneri corespunzătoare în vederea modificării prezentei directive, în special ținând seama de evoluțiile din domeniul tehnologiei informației și având în vedere progresele societății informaționale.

(6) Până la 6 mai 2019, Comisia revizuiește celelalte acte adoptate de Uniune care reglementează prelucrarea de către autoritățile competente în scopurile prevăzute la articolul 1 alineatul (1), inclusiv actele menționate la articolul 60, pentru a evalua necesitatea de a le alinia la prezenta directivă și prezintă, după caz, propunerile necesare de modificare a actelor respective pentru a asigura o abordare uniformă privind protecția datelor cu caracter personal care intră în domeniul de aplicare al prezentei directive.

Articolul 63

Transpunerea

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

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

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

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

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

Articolul 64

Intrarea în vigoare

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

Articolul 65

Destinatari

Prezenta directivă se adresează statelor membre.

Adoptată la Bruxelles, 27 aprilie 2016.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT