III

(Acte adoptate în temeiul Tratatului UE)

ACTE ADOPTATE ÎN TEMEIUL TITLULUI VI DIN TRATATUL UE

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

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind Uniunea Europeană, în special articolul 30, articolul 31 și articolul 34 alineatul (2) litera (b),

având în vedere propunerea Comisiei,

având în vedere avizul Parlamentului European [1],

întrucât:

(1) Uniunea Europeană și-a stabilit obiectivul de a menține și de a dezvolta Uniunea ca spațiu de libertate, securitate și justiție în cadrul căruia se va asigura un înalt nivel de siguranță prin acțiunea comună a statelor membre în domeniul cooperării polițienești și judiciare în materie penală.

(2) Acțiunea comună în domeniul cooperării polițienești în temeiul articolului 30 alineatul (1) litera (b) din Tratatul privind Uniunea Europeană și acțiunea comună pentru cooperarea judiciară în materie penală în temeiul articolului 31 alineatul (1) litera (a) din Tratatul privind Uniunea Europeană implică necesitatea prelucrării unor informații relevante care ar trebui să facă obiectul unor dispoziții corespunzătoare privind protecția datelor cu caracter personal.

(3) Legislația care intră sub incidența titlului VI din Tratatul privind Uniunea Europeană ar trebui să favorizeze cooperarea polițienească și judiciară în materie penală cu privire la eficiența, precum și la legitimitatea și conformitatea acesteia cu drepturile fundamentale și, în special, cu dreptul la viață privată și la protecția datelor cu caracter personal. Adoptarea de standarde comune privind prelucrarea și protecția datelor cu caracter personal prelucrate în scopul prevenirii și a combaterii crimei contribuie la realizarea ambelor obiective.

(4) Programul de la Haga pentru consolidarea libertății, securității și justiției în Uniunea Europeană adoptat de Consiliul European la 4 noiembrie 2004 a subliniat necesitatea unei abordări inovatoare a schimbului transfrontalier de informații privind punerea în aplicare a legii, cu stricta respectare a principalelor condiții din domeniul protecției datelor și a invitat Comisia să înainteze propuneri în acest sens până la sfârșitul anului 2005. Aspectul menționat a fost reflectat în Planul de acțiune al Consiliului și al Comisiei de punere în aplicare a Programului de la Haga pentru consolidarea libertății, securității și justiției în Uniunea Europeană [2].

(5) Schimbul de date personale în cadrul cooperării polițienești și judiciare în materie penală, în special în conformitate cu principiul disponibilității informației, astfel cum a fost enunțat în Programul de la Haga, ar trebui sprijinit prin norme clare care să sporească încrederea reciprocă între autoritățile competente și să asigure protecția informațiilor relevante, astfel încât să se excludă orice discriminare în ceea ce privește această cooperare între statele membre, cu respectarea, în același timp a drepturilor fundamentale ale persoanelor fizice. Instrumentele existente la nivel european nu sunt suficiente. Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal și la libera circulație a acestor date [3] nu se aplică în cazul prelucrării datelor cu caracter personal în cursul unei activități care nu se circumscrie domeniului de aplicare a legislației comunitare, astfel cum sunt cele prevăzute la titlul VI din Tratatul privind Uniunea Europeană și nici, în orice caz, operațiilor de prelucrare privind securitatea publică, apărarea, siguranța de stat și activitățile statului în domeniul legii penale.

[1] JO C 125 E, 22.5.2008, p. 154.

[2] JO C 198, 12.8.2005, p. 1.

[3] JO L 281, 23.11.1995, p. 31.

(6) Prezenta decizie-cadru se aplică numai în cazul datelor colectate sau prelucrate de autorități competente, în scopul prevenirii, cercetării, descoperirii sau urmăririi penale a infracțiunilor sau al executării pedepselor. Prezenta decizie-cadru ar trebui să lase la latitudinea statelor membre determinarea mai exactă, la nivel național, a celorlalte obiective considerate ca fiind incompatibile cu scopul pentru care au fost colectate inițial datele personale. În general, prelucrarea suplimentară în scopuri de cercetare istorică, statistice sau de cercetare științifică nu ar trebui să fie considerată incompatibilă cu scopul inițial al prelucrării.

(7) Domeniul de aplicare al prezentei decizii-cadru se limitează la prelucrarea datelor cu caracter personal transmise sau puse la dispoziție între statele membre. Nu ar trebui să se poată deduce nicio concluzie din această restricție privind competența Uniunii de a adopta acte privind colectarea și prelucrarea datelor cu caracter personal la nivel național sau privind oportunitatea unei asemenea acțiuni din partea Uniunii în viitor.

(8) Pentru a facilita schimburile de date în cadrul Uniunii, statele membre urmăresc să asigure faptul că standardele de protecție a datelor realizate în prelucrarea datelor la nivel național corespund celor prevăzute de prezenta decizie-cadru. În ceea ce privește prelucrarea datelor la nivel național, prezenta decizie-cadru nu împiedică statele membre să asigure garanții ale protecției datelor cu caracter personal la un nivel mai ridicat decât cel prevăzut prin prezenta decizie-cadru.

(9) Prezenta decizie-cadru nu ar trebui să se aplice în cazul unor date cu caracter personal pe care un stat membru le-a obținut în temeiul prezentei decizii-cadru și care provin din statul membru respectiv.

(10) Armonizarea legislațiilor statelor membre nu ar trebui să aibă ca rezultat scăderea nivelului de protecție a datelor pe care îl oferă statele respective, ci ar trebui, dimpotrivă, să urmărească asigurarea unui înalt nivel de protecție în cadrul Uniunii.

(11) Este necesar să fie precizate obiectivele de protecție a datelor în cadrul activităților polițienești și judiciare și să se instituie norme privind legalitatea prelucrării datelor cu caracter personal pentru a se asigura că orice informație care poate face obiectul unui schimb a fost prelucrată în mod legal și în conformitate cu principiile fundamentale privind calitatea datelor. În același timp, activitățile legitime ale poliției, ale autorităților vamale, judiciare și ale altor autorități competente nu trebuie să fie periclitate în niciun fel.

(12) Principiul exactității datelor se aplică ținând cont de natura și scopul prelucrării în cauză. De exemplu, în special în cursul procedurilor judiciare, datele se bazează pe percepția subiectivă a indivizilor și, în unele cazuri, sunt imposibil de verificat. Prin urmare, exigența exactității nu se referă la exactitatea declarației, ci la faptul că o anumită declarație a fost făcută.

(13) Arhivarea într-un set separat de date ar trebui să fie permisă numai dacă datele nu mai sunt necesare și nu mai sunt utilizate în scopul prevenirii, al cercetării, al descoperirii sau al urmăririi penale a infracțiunilor sau al executării pedepselor. Arhivarea într-un set separat de date ar trebui, de asemenea, să fie permisă dacă datele arhivate sunt stocate într-o bază de date împreună cu alte date într-un mod care face imposibilă utilizarea lor în continuare în scopul prevenirii, al cercetării, al descoperirii sau al urmăririi penale a infracțiunilor sau al executării pedepselor. Termenul de arhivare corespunzător ar trebui să depindă de scopurile arhivării și de interesele legitime ale persoanei vizate. În cazul arhivării în scopuri de cercetare istorică, se poate avea în vedere un termen foarte lung.

(14) De asemenea, datele se pot șterge prin distrugerea suportului de date.

(15) În ceea ce privește datele inexacte, incomplete sau perimate transmise altui stat membru sau puse la dispoziția acestora și prelucrate în continuare de autorități cvasi-judiciare, și anume de autorități împuternicite să emită decizii cu forță juridică obligatorie, rectificarea, ștergerea sau blocarea acestora ar trebui să se realizeze în conformitate cu legislația națională.

(16) Asigurarea unui înalt nivel de protecție a datelor cu caracter personal ale persoanelor fizice necesită dispoziții comune pentru stabilirea legalității și a calității datelor prelucrate de autoritățile competente în alte state membre.

(17) Este oportun să se instituie la nivel european condițiile care să permită autorităților competente ale statelor membre să transmită și să pună la dispoziția autorităților și entităților private din statele membre datele cu caracter personal primite din celelalte state membre. În numeroase situații, este necesar ca datele cu caracter personal să fie transmise entităților private de către autoritățile judiciare, polițienești sau vamale pentru urmărirea infracțiunilor sau pentru prevenirea unei amenințări imediate și grave a siguranței publice și pentru prevenirea vătămării grave a drepturilor persoanelor fizice, de exemplu, prin emiterea de alerte cu privire la falsificarea garanțiilor financiare către bănci și instituții de credit sau, în cazul criminalității din domeniul autovehiculelor, prin comunicarea de date cu caracter personal companiilor de asigurări pentru a preveni traficul ilicit de autovehicule furate sau pentru a îmbunătăți condițiile de recuperare a autovehiculelor furate din străinătate. Acest lucru nu este echivalent cu transferul sarcinilor polițienești și judiciare către entitățile private.

(18) Normele prezentei decizii-cadru privind transmiterea datelor cu caracter personal de către autoritățile judiciare, polițienești sau vamale către entități private nu se aplică în cazul dezvăluirii datelor către entități private (precum avocații apărării și victimele) în contextul procedurilor penale.

(19) Prelucrarea suplimentară a datelor cu caracter personal primite sau puse la dispoziție de autoritatea competentă a altui stat membru, în special transmiterea sau punerea la dispoziție ulterioară a acestor date, trebuie să se supună normelor comune la nivel european.

(20) În cazul unei posibilități de prelucrare suplimentară a datelor cu caracter personal, după ce statul membru de la care au fost obținute datele și-a dat acordul, fiecare stat membru ar trebui să poată să determine modalitățile aferente acestui acord, inclusiv, de exemplu, printr-un acord general pentru anumite categorii de informații sau pentru anumite categorii de prelucrare suplimentară.

(21) În cazul unei posibilități de prelucrare suplimentară a datelor cu caracter personal în cadrul unor proceduri administrative, aceste proceduri includ, de asemenea, activitățile desfășurate de organismele de reglementare și de control.

(22) Activitățile legitime ale poliției, vămilor, autorităților judiciare și ale altor autorități competente pot necesita transmiterea de informații către autoritățile unor state terțe sau ale unor organisme internaționale, care au obligația prevenirii, cercetării, depistării sau urmăririi penale a infracțiunilor sau a executării pedepselor.

(23) În cazul transferului de date cu caracter personal de la un stat membru către state terțe sau către organisme internaționale, datele respective ar trebui să beneficieze, în principiu, de un nivel corespunzător de protecție.

(24) În cazul transferului de date cu caracter personal de la un stat membru către state terțe sau către organisme internaționale, acest transfer ar trebui să poată fi efectuat, în principiu, numai după ce statul membru de la care au fost obținute datele și-a dat acordul în ceea ce privește transferul. Fiecare stat membru ar trebui să poată să stabilească modalitățile aferente acestui acord, de exemplu, printr-un acord general pentru anumite categorii de informații sau pentru anumite state terțe.

(25) Interesele unei cooperări eficace cu privire la aplicarea legii impun ca, în cazul în care există un pericol imediat la adresa securității publice a unui stat membru sau a unui stat terț, astfel încât este imposibil să se obțină la timp acordul prealabil, autoritatea competentă ar trebui să poată transfera datele cu caracter personal pertinente către statul terț interesat, fără acest acord prealabil. Aceeași situație s-ar putea aplica în cazul în care sunt în joc alte interese fundamentale, de importanță similară, ale unui stat membru, ca de exemplu un pericol grav și iminent pentru infrastructura critică a unui stat membru sau o perturbare gravă a sistemului financiar al unui stat membru.

(26) Poate fi necesară informarea persoanelor vizate cu privire la prelucrarea datelor acestora, în special în cazul în care a existat o încălcare gravă a drepturilor persoanelor respective ca urmare a măsurilor de colectare a datelor secrete, pentru a se asigura posibilitatea unei protecții juridice eficiente a persoanelor vizate.

(27) Statul membru ar trebui să asigure faptul că persoana vizată este informată că datele cu caracter personal ar putea fi sau sunt colectate, prelucrate sau transmise unui alt stat membru în scopul prevenirii, cercetării, descoperirii sau urmăririi penale a infracțiunilor sau al executării pedepselor. Modalitățile aferente dreptului persoanei vizate de a fi informată, precum și excepțiile de la acesta, ar trebui să fie reglementate de legislația națională. Acest lucru poate să se prezinte sub o formă generală, de exemplu, prin intermediul legislației sau prin publicarea unei liste cu operațiile de prelucrare.

(28) Pentru a asigura protecția datelor cu caracter personal fără a periclita interesul cercetărilor penale, este necesar să se definească drepturile persoanei vizate.

(29) Unele state membre au asigurat, în materie penală, dreptul de acces al persoanei vizate prin intermediul unui sistem prin care autoritatea națională de supraveghere, în locul persoanei vizate, are acces la toate datele cu caracter personal privind persoana vizată fără nicio restricție și poate rectifica, șterge sau actualiza datele inexacte. Într-un astfel de caz de acces indirect, legislația națională a acestor state membre poate prevedea că autoritatea națională de supraveghere trebuie să informeze persoana vizată numai în legătură cu faptul că au fost efectuate toate verificările necesare. Cu toate acestea, statele membre respective prevăd, de asemenea, posibilitatea unui acces direct al persoanelor vizate, în anumite situații, precum accesul la cazierele judiciare, pentru a se obține copii ale propriilor caziere judiciare sau documente referitoare la propriile audieri efectuate de către serviciile de poliție.

(30) Este oportună instituirea de norme comune privind confidențialitatea și securitatea prelucrării, răspunderea juridică și sancțiunile pentru utilizarea nelegală de către autoritățile competente, precum și căile de atac de care dispune persoana vizată. Cu toate acestea, natura normelor de responsabilitate delictuală și a sancțiunilor aplicabile în cazul încălcării dispozițiilor interne privind protecția datelor rămâne să fie stabilită de fiecare stat membru.

(31) Prezenta decizie-cadru permite punerea în aplicare a principiilor prevăzute, cu respectarea principiului accesului publicului la documentele oficiale.

(32) În cazul în care se impune protecția datelor cu caracter personal în ceea ce privește prelucrarea, care, din cauza amplorii sau a tipului acesteia, prezintă riscuri specifice pentru drepturile și libertățile fundamentale, ca de exemplu prelucrarea prin intermediul noilor tehnologii, mecanisme sau proceduri, este important să se garanteze că autoritățile naționale de supraveghere competente sunt consultate înainte de crearea unui sistem de evidență destinat prelucrării acestor date.

(33) Instituirea în statele membre a unor autorități de supraveghere care să-și exercite atribuțiile în deplină independență este un element esențial al protecției datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare între statele membre.

(34) Autoritățile de supraveghere deja instituite în statele membre în temeiul Directivei 95/46/CE ar trebui, de asemenea, să poată prelua răspunderea pentru sarcinile care urmează a fi îndeplinite de către autoritățile naționale de supraveghere instituite prin prezenta decizie-cadru.

(35) Autoritățile de supraveghere respective ar trebui să dispună de mijloacele necesare pentru a-și îndeplini atribuțiile, inclusiv de competențe de cercetare și de intervenție, în special în cazul reclamațiilor din partea persoanelor fizice, precum și competența de a acționa în justiție. Autoritățile de supraveghere menționate ar trebui să ajute la asigurarea transparenței prelucrării în statele membre de a căror jurisdicție aparțin. Cu toate acestea, competențele acestora nu ar trebui să afecteze normele specifice stabilite pentru procedurile penale sau independența justiției.

(36) Articolul 47 din Tratatul privind Uniunea Europeană prevede că niciuna dintre dispozițiile sale nu aduce atingere tratatelor de instituire a Comunităților Europene sau tratatele și actele ulterioare de modificare sau completare a acestora. În consecință, prezenta decizie-cadru nu afectează protecția datelor cu caracter personal prevăzută în dreptul comunitar, în special astfel cum a fost reglementată prin Directiva 95/46/CE, 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 [1] și Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor cu caracter personal și protejarea confidențialității în sectorul comunicațiilor electronice (Directiva privind confidențialitatea și comunicațiile electronice) [2].

(37) Prezenta decizie-cadru nu aduce atingere normelor privind accesul ilicit la date, instituite de Decizia-cadru 2005/222/JAI a Consiliului din 24 februarie 2005 privind atacurile împotriva sistemelor informatice [3].

(38) Prezenta decizie-cadru nu aduce atingere obligațiilor și angajamentelor care revin statelor membre sau Uniunii în temeiul unor acorduri bilaterale și/sau multilaterale cu state terțe. Acordurile viitoare ar trebui să respecte normele privind schimburile cu statele terțe.

(39) Mai multe acte adoptate în temeiul titlului VI din Tratatul privind Uniunea Europeană includ dispoziții specifice privind protecția datelor cu caracter personal comunicate sau, în alte cazuri, prelucrate în conformitate cu aceste acte. În anumite cazuri, aceste dispoziții reprezintă un set complet și coerent de norme care tratează toate aspectele relevante privind protecția datelor cu caracter personal (principiul calității datelor, normele referitoarea la securitatea datelor, reglementarea drepturilor și garanțiilor persoanelor vizate, organizarea supravegherii și a răspunderii) și reglementează aceste chestiuni mai amănunțit decât prezenta decizie-cadru. Setul relevant de dispoziții privind protecția datelor cu caracter personal din aceste acte, în special acelea care reglementează funcționarea Europol, a Eurojust, a Sistemului de Informații Schengen (SIS) și a Sistemului de Informații al Vămilor (CIS), ca și acelea care introduc accesul direct pentru autoritățile statelor membre la anumite sisteme de date ale altor state membre, nu ar trebui să aducă atingere prezentei decizii-cadru. De asemenea, acest lucru este valabil și în ceea ce privește dispozițiile privind datele cu caracter personal care reglementează transferul automat între statele membre al profilurilor ADN, al datelor dactiloscopice și al datelor naționale privind înmatricularea vehiculelor, în conformitate cu Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și al criminalității transfrontaliere [4].

(40) În celelalte cazuri, domeniul de aplicare al dispozițiilor privind protecția datelor cu caracter personal din acte, adoptate în temeiul titlului VI din Tratatul privind Uniunea Europeană, este mai restrâns. Aceste dispoziții stabilesc deseori condiții specifice privind scopurile în care pot fi utilizate de către statul membru informațiile care conțin datele cu caracter personal pe care acesta le primește de la un alt stat membru, dar fac trimitere, în ceea ce privește celelalte aspecte ale protecției datelor cu caracter personal, la Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal din 28 ianuarie 1981 sau la legislația internă. În măsura în care dispozițiile acelor acte care impun condiții statelor membre destinatare privind utilizarea datelor cu caracter personal sau transferul acestora mai departe sunt mai restrictive decât cele conținute în dispozițiile corespunzătoare ale prezentei decizii-cadru, vechile dispoziții ar trebui să rămână neschimbate. Cu toate acestea, în ceea ce privește toate celelalte aspecte, ar trebui să se aplice normele stabilite în prezenta decizie-cadru.

(41) Prezenta decizie-cadru nu aduce atingere Convenției Consiliului Europei pentru protecția persoanelor fizice cu privire la prelucrarea automatizată a datelor cu caracter personal, Protocolul adițional la această Convenție din 8 noiembrie 2001 sau convențiile Consiliului Europei privind cooperarea juridică în materie penală.

[1] JO L 8, 12.1.2001, p. 1.
[2] JO L 201, 31.7.2002, p. 37.
[3] JO L 69, 16.3.2005, p. 67.
[4] JO L 210, 6.8.2008, p. 1.

(42) Întrucât obiectivele prezentei decizii-cadru, respectiv stabilirea unor norme comune pentru protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, nu pot fi suficient realizate de statele membre acționând unilateral și, prin urmare, datorită dimensiunii și efectelor măsurii menționate, pot fi mai bine realizate la nivelul Uniunii, Uniunea poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este instituit la articolul 5 din Tratatul de instituire a Comunității Europene și menționat la articolul 2 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum a fost enunțat, de asemenea, la articolul 5 din Tratatul de instituire a Comunității Europene, prezenta decizie-cadru nu depășește ceea ce este necesar pentru a atinge obiectivele menționate.

(43) Regatul Unit participă la prezenta decizie-cadru, în conformitate cu articolul 5 din Protocolul de integrare a acquis-ului Schengen în cadrul Uniunii Europene anexat la Tratatul privind Uniunea Europeană și la Tratatul de instituire a Comunității Europene și cu articolul 8 alineatul (2) din Decizia 2000/365/CE a Consiliului din 29 mai 2000 privind cererea Regatului Unit al Marii Britanii și Irlandei de Nord de a participa la anumite dispoziții ale acquis-ului Schengen ([1]).

(44) Irlanda participă la prezenta decizie-cadru, în conformitate cu articolul 5 din Protocolul de integrare a acquis-ului Schengen în cadrul Uniunii Europene anexat la Tratatul privind Uniunea Europeană și la Tratatul de instituire a Comunității Europene și cu articolul 6 alineatul (2) din Decizia 2002/192/CE a Consiliului din 28 februarie 2002 privind cererea Irlandei de a participa la anumite dispoziții ale acquis-ului Schengen ([2]).

(45) În ceea ce privește Islanda și Norvegia, prezenta decizie-cadru reprezintă o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Acordului încheiat de Consiliul Uniunii Europene și Republica Islanda și Regatul Norvegiei privind asocierea acestor două state la transpunerea, punerea în aplicare și dezvoltarea acquis-ului Schengen ([3]), circumscrise sferei menționate la articolul 1 punctele H și I din Decizia 1999/437/CE a Consiliului ([4]) privind anumite modalități de aplicare a acordului menționat.

(46) În ceea ce privește Elveția, prezenta decizie-cadru reprezintă o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Acordului încheiat între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la transpunerea, punerea în aplicare și dezvoltarea acquis-ului Schengen ([5]), circumscrise sferei menționate la articolul 1 punctele H și I din Decizia 1999/437/CE coroborat cu articolul 3 din Decizia 2008/149/JAI a Consiliului ([6]) privind încheierea, în numele Uniunii Europene, a acordului respectiv.

(47) În ceea ce privește Liechtenstein, prezenta decizie-cadru reprezintă o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Protocolului semnat între 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 transpunerea, punerea în aplicare și dezvoltarea acquis-ului Schengen, circumscrise sferei menționate la articolul 1 punctele H și I din Decizia 1999/437/CE, coroborat cu articolul 3 din Decizia 2008/262/JAI a Consiliului ([7]) privind semnarea, în numele Uniunii Europene, a protocolului respectiv.

(48) Prezenta decizie-cadru respectă drepturile fundamentale și se conformează principiilor recunoscute în special de Carta drepturilor fundamentale a Uniunii Europene ([8]). Prezenta decizie-cadru urmărește să asigure respectarea deplină a drepturilor la viață privată și la protecția datelor cu caracter personal reflectate în articolele 7 și 8 din Cartă,

ADOPTĂ PREZENTA DECIZIE-CADRU:

Articolul 1

Obiectivul și domeniul de aplicare

(1) Obiectivul prezentei decizii-cadru îl constituie asigurarea unui înalt nivel de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice și în special a dreptului acestora la o viață privată, în ceea ce privește prelucrarea datelor cu caracter personal în cadrul cooperării polițienești și judiciare în materie penală, prevăzute la titlul VI din Tratatul privind Uniunea Europeană, cu garantarea, în același timp, a unui înalt nivel de securitate publică.

(2) În conformitate cu prezenta decizie-cadru, statele membre protejează drepturile și libertățile fundamentale ale persoanelor fizice, și în special dreptul acestora la o viață privată în cazul în care, în scopul prevenirii, al cercetării, al descoperirii sau al urmării penale a infracțiunilor sau al executării pedepselor, datele cu caracter personal:

(a) sunt sau au fost transmise sau puse la dispoziție între statele membre;

([1]) JO L 131, 1.6.2000, p. 43.
([2]) JO L 64, 7.3.2002, p. 20.
([3]) JO L 176, 10.7.1999, p. 36.
([4]) JO L 176, 10.7.1999, p. 31.
([5]) JO L 53, 27.2.2008, p. 52.
([6]) JO L 53, 27.2.2008, p. 50.
([7]) JO L 83, 26.3.2008, p. 5.
([8]) JO C 303, 14.12.2007, p. 1.

(b) sunt sau au fost transmise sau puse la dispoziția autorităților sau a sistemelor informatice instituite în temeiul titlului VI din Tratatul privind Uniunea Europeană, de către statele membre; sau

(c) sunt sau au fost transmise sau puse la dispoziția autorităților competente din statele membre de către autoritățile sau a sistemelor informatice instituite în baza Tratatului privind Uniunea Europeană sau a Tratatului de instituire a Comunității Europene.

(3) Prezenta decizie-cadru se aplică în cazul prelucrării, prin mijloace integral sau parțial automatizate, a datelor cu caracter personal, precum în cazul prelucrării cu alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență sau sunt destinate să facă parte dintr-un sistem de evidență.

(4) Prezenta decizie-cadru nu aduce atingere intereselor naționale fundamentale în materie de securitate și nici activităților specifice ale serviciilor de informații în domeniul siguranței naționale.

(5) Prezenta decizie-cadru nu împiedică statele membre să asigure, pentru protecția datelor cu caracter personal colectate sau prelucrate la nivel național, măsuri de garantare la un nivel mai ridicat decât cel prevăzut prin prezenta decizie-cadru.

Articolul 2

Definiții

În înțelesul prezentei decizii-cadru:

(a) „date cu caracter personal" înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un cod numeric personal sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

(b) „prelucrarea datelor cu caracter personal" și „prelucrare" înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau prin punerea la dispoziție în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

(c) „blocare" înseamnă marcarea unor date cu caracter personal stocate în scopul limitării prelucrării pe viitor;

(d) „sistem de evidență a datelor cu caracter personal" și „sistem de evidență" înseamnă orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;

(e) „operator de prelucrare" înseamnă orice organism care prelucrează date cu caracter personal în numele inspectorului;

(f) „destinatar" înseamnă orice organism căruia îi sunt comunicate date;

(g) „consimțământul persoanei vizate" înseamnă orice manifestare de voință, liberă, specifică și informată prin care persoana vizată acceptă să fie prelucrate datele cu caracter personal care o privesc;

(h) „autorități competente" înseamnă agențiile sau organismele instituite în temeiul unor acte juridice adoptate de Consiliu, în conformitate cu titlul VI din Tratatul privind Uniunea Europeană, precum și autoritățile polițienești, vamale, judiciare și alte autorități competente din statele membre care sunt autorizate în cadrul legislației naționale să prelucreze date cu caracter personal, în temeiul prezentei decizii-cadru;

(i) „inspector" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau oricare alt organism care individual sau în comun cu alte organisme stabilește scopurile și modalitățile prelucrării datelor cu caracter personal;

(j) „atribuirea de referințe" înseamnă marcarea datelor cu caracter personal stocate, fără a avea ca scop limitarea prelucrării lor ulterioare;

(k) prin „transformarea în date anonime" se înțelege modificarea datelor cu caracter personal, astfel încât detaliile privind circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile sau să permită atribuirea doar în condițiile unei investiții disproporționate de timp, costuri și forță de muncă.

Articolul 3

Principii de legalitate, proporționalitate și scop

(1) Datele cu caracter personal pot fi colectate de autoritățile competente numai în scopuri specifice, explicite și legitime în cadrul sarcinilor lor și pot fi prelucrate doar în scopurile pentru care au fost colectate. Prelucrarea datelor trebuie să fie legală și adecvată, relevantă și să nu fie excesivă în raport cu scopurile pentru care au fost colectate.

(2) Prelucrarea suplimentară pentru un alt scop este permisă în măsura în care:

(a) este compatibilă cu scopul în care au fost colectate datele;

(b) autoritățile competente sunt autorizate să prelucreze astfel de date în acest alt scop, în conformitate cu dispozițiile legale aplicabile; și

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

Autoritățile competente pot, de asemenea, să prelucreze suplimentar datele cu caracter personal transmise, în scopuri de cercetare istorică, statistice sau de cercetare științifică, sub rezerva furnizării de către statele membre a unor garanții corespunzătoare, cum ar fi cele privind transformarea în date anonime.

Articolul 4

Rectificarea, ștergerea și blocarea

(1) Datele cu caracter personal se rectifică dacă nu sunt exacte și, în cazul în care este posibil și necesar, se completează și se actualizează.

(2) Datele cu caracter personal se șterg sau se trec în anonimat atunci când nu mai sunt necesare în scopurile în care au fost colectate în mod legal sau sunt, în mod legal, prelucrate suplimentar. Prezenta dispoziție nu afectează arhivarea acelor date într-un set separat de date pentru o perioadă de timp corespunzătoare, în conformitate cu dreptul intern.

(3) În loc să fie șterse, datele cu caracter personal se blochează atunci când există motive întemeiate să se considere că ștergerea lor ar putea afecta interesele legitime ale persoanei vizate. Datele blocate se prelucrează doar în scopul care a împiedicat ștergerea lor.

(4) În cazul în care datele cu caracter personal sunt conținute într-o hotărâre judecătorească sau într-un cazier judiciar referitor la emiterea unei hotărâri judecătorești, rectificarea, ștergerea sau blocarea sunt efectuate în conformitate cu reglementările naționale privind procedurile judiciare.

Articolul 5

Stabilirea de termene pentru ștergere și revizuire

Se stabilesc termene corespunzătoare pentru ștergerea datelor cu caracter personal sau pentru o revizuire periodică a necesității de stocare a datelor. Respectarea acestor termene este asigurată prin instituirea unor măsuri procedurale.

Articolul 6

Prelucrarea unor categorii speciale de date

Prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea datelor privind sănătatea sau viața sexuală este permisă numai în cazul în care este strict necesară și când legislația națională prevede garanții corespunzătoare.

Articolul 7

Deciziile individuale bazate pe prelucrarea automatizată

Deciziile care produc un efect juridic advers asupra persoanei vizate sau care o afectează în mod semnificativ și care sunt bazate exclusiv pe prelucrarea automatizată a datelor în scopul evaluării anumitor aspecte cu caracter personal referitoare la persoana vizată sunt permise numai dacă sunt permise de legislația care stabilește și măsuri pentru protecția persoanei vizate.

Articolul 8

Verificarea calității datelor transmise sau puse la dispoziție

(1) Autoritățile competente iau toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte, incomplete sau perimate nu sunt transmise sau puse la dispoziție. În acest scop, autoritățile competente 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, se adaugă informații disponibile care să permită statului membru destinatar să evalueze gradul de exactitate, caracterul integral, gradul de actualitate și fiabilitate. În cazul transmiterii de date cu caracter personal care nu au fost solicitate, autoritatea destinatară verifică de îndată dacă datele respective sunt necesare în scopul în care au fost transmise.

(2) În cazul în care se constată transmiterea unor date inexacte sau transmiterea unor date în mod ilegal, acest lucru trebuie comunicat de îndată destinatarului. Datele trebuie să fie rectificate, șterse sau blocate fără întârziere în conformitate cu articolul 4.

Articolul 9

Termenele

(1) După transmiterea sau la punerea la dispoziție a datelor, autoritatea care transmite datele poate să indice termenele pentru reținerea datelor, în conformitate cu legislația națională și cu articolele 4 și 5, iar după expirarea termenelor respective, destinatarul are obligația de a șterge sau de a bloca datele sau să verifice dacă acestea mai sunt sau nu necesare. Această obligație nu se aplică dacă, la expirarea acestor termene, sunt necesare pentru o cercetare aflată în curs, urmărirea penală a infracțiunilor sau executarea pedepselor.

(2) În cazul în care autoritatea care transmite datele nu a indicat un termen în conformitate cu alineatul (1), se aplică termenele menționate la articolele 4 și 5 pentru reținerea datelor furnizate în conformitate cu legislația națională a statului membru destinatar.

Articolul 10

Luarea în evidență și documentarea

(1) Orice transmitere de date cu caracter personal se ia în evidență sau se documentează pentru verificarea legalității prelucrării datelor, pentru monitorizare proprie și pentru asigurarea integrității și a securității corespunzătoare a datelor.

(2) Luarea în evidență sau documentarea prevăzute la alineatul (1) se comunică la cerere autorității competente de supraveghere pentru controlul protecției datelor. Autoritatea competentă de supraveghere utilizează informațiile respective numai pentru controlul protecției datelor și pentru asigurarea prelucrării corespunzătoare a datelor, precum și integritatea și securitatea datelor.

Articolul 11

Prelucrarea datelor cu caracter personal primite sau puse la dispoziție de un alt stat membru

Datele cu caracter personal primite de la autoritatea competentă a altui stat membru în conformitate cu cerințele articolului 3 alineatul (2) sau puse la dispoziție de către aceasta pot fi prelucrate suplimentar numai în următoarele scopuri, altele decât cele pentru care au fost transmise sau puse la dispoziție:

(a) prevenirea, cercetarea, descoperirea sau urmărirea penală a infracțiunilor sau executarea pedepselor, altele decât cele pentru care au fost transmise sau puse la dispoziție;

(b) alte proceduri judiciare sau administrative direct legate de prevenirea, cercetarea, descoperirea și urmărirea penală a infracțiunilor sau executarea pedepselor;

(c) prevenirea unui pericol iminent și grav la adresa securității publice; sau

(d) orice alt scop doar cu consimțământul prealabil al statului membru care transmite sau cu consimțământul persoanei vizate, în conformitate cu legislația națională.

Autoritățile competente pot, de asemenea, să prelucreze suplimentar datele cu caracter personal transmise, în scopuri de cercetare istorică, statistice sau de cercetare științifică, sub rezerva furnizării de către statele membre a unor garanții corespunzătoare, cum ar fi, de exemplu, cele privind transformarea în date anonime.

Articolul 12

Respectarea restricțiilor naționale privind prelucrarea

(1) Atunci când, în conformitate cu legislația statului membru care efectuează transmiterea datelor, se aplică, în anumite circumstanțe, restricții specifice privind prelucrarea schimburilor de date între autoritățile competente din statul membru respectiv, autoritatea care efectuează transmiterea informează destinatarul în privința acestor restricții. Destinatarul se asigură că aceste restricții privind prelucrarea sunt respectate.

(2) Atunci când aplică alineatul (1), statele membre nu aplică restricții în ceea ce privește transmiterea de date către alte state membre sau către agențiile sau organismele instituite în conformitate cu titlul VI din Tratatul privind Uniunea Europeană, altele decât cele aplicabile transmiterii similare de date la nivel național.

Articolul 13

Transferul către autorități competente din state terțe sau către organisme internaționale

(1) Statele membre dispun ca datele cu caracter personal transmise sau puse la dispoziție de autoritățile competente ale unui alt stat membru să poată fi transferate către state terțe sau organisme internaționale numai dacă:

(a) se impune pentru prevenirea, cercetarea, descoperirea sau urmărirea penală a infracțiunilor sau executarea pedepselor;

(b) autorității destinatare din statul terț sau organismului internațional destinatar îi revine răspunderea pentru prevenirea, cercetarea, descoperirea și urmărirea penală a infracțiunilor sau pentru executarea pedepselor;

(c) statul membru de la care au fost obținute datele și-a dat acordul de a le transfera în conformitate cu legislația națională; și

(d) statul terț sau organismul internațional în cauză asigură un nivel corespunzător de protecție pentru prelucrarea de date urmărită.

(2) Transferul fără acordul prealabil în conformitate cu alineatul (1) este permis numai dacă transferul de date este esențial pentru prevenirea unui pericol iminent și grav la adresa securității publice a unui stat membru sau a unui stat terț sau a intereselor fundamentale ale unui stat membru, iar consimțământul prealabil nu poate fi dat în timp util. Autoritatea responsabilă de acordarea consimțământului este informată fără întârziere.

(3) Prin derogare de la alineatul (1) litera (d), datele cu caracter personal se pot transfera în cazul în care:

(a) legislația națională a statului membru care transferă datele prevede acest lucru, având în vedere:

(i) interesele legitime specifice ale persoanei vizate; sau

(ii) interesele legitime prioritare, în special interese publice importante; sau

(b) statul terț destinatar sau organismul internațional destinatar furnizează garanții considerate a fi corespunzătoare de către statul membru interesat, în conformitate cu legislația națională a acestuia.

(4) Caracterul adecvat al nivelului de protecție menționat la alineatul (1) litera (d), este evaluat în lumina tuturor factorilor prezenți într-o operațiune sau într-un ansamblu de operațiuni de transfer de date. Se acordă o atenție deosebită tipului de date, scopului și duratei prelucrării sau a prelucrărilor propuse, statului de origine și statului sau organismului internațional de destinație finală a datelor, normelor de drept, atât generale, cât și sectoriale aplicabile statului terț sau organismului internațional în cauză, precum și normelor profesionale și măsurilor de securitate aplicabile.

Articolul 14

Transmiterea către entitățile private din statele membre

(1) Statele membre dispun ca datele cu caracter personal primite de la autoritatea competentă dintr-un alt stat membru sau puse la dispoziție de către aceasta pot fi transmise entităților private numai dacă:

(a) autoritatea competentă din statul membru din care datele au fost obținute și-a dat acordul pentru efectuarea transmiterii în conformitate cu legislația națională;

(b) niciun interes specific legitim al persoanei vizate nu împiedică transmiterea; și

(c) în cazuri specifice, transferul este esențial pentru autoritatea competentă care transmite date unei entități private pentru:

(i) îndeplinirea unei sarcini în mod legal atribuite acesteia;

(ii) prevenirea, cercetarea, descoperirea sau urmărirea penală a infracțiunilor sau executarea pedepselor;

(iii) prevenirea unui pericol iminent și grav la adresa securității publice; sau

(iv) prevenirea unei vătămări grave a drepturilor persoanei.

(2) Autoritatea competentă care transmite datele unei entități private o informează pe aceasta din urmă cu privire la scopurile pentru care, în mod exclusiv, pot fi utilizate datele.

Articolul 15

Informații la cererea autorității competente

La cerere, destinatarul informează autoritatea competentă care a transmis sau a pus la dispoziție date cu caracter personal asupra prelucrării lor.

Articolul 16

Informații pentru persoana vizată

(1) Statele membre se asigură că persoana vizată este informată în legătură cu colectarea sau prelucrarea datelor cu caracter personal de către autoritățile competente, în conformitate cu legislația națională.

(2) Atunci când au fost transmise sau puse la dispoziție date cu caracter personal între state membre, fiecare stat membru poate, în conformitate cu prevederile legislației naționale menționate la alineatul (1), să ceară celuilalt stat membru să nu informeze persoana vizată. În acest caz, statul respectiv nu informează persoana vizată fără consimțământul prealabil al celuilalt stat.

Articolul 17

Dreptul de acces

(1) Fiecare persoană vizată are dreptul, la cerere și la intervale rezonabile, să primească fără constrângere și fără întârzieri sau cheltuieli excesive:

(a) cel puțin o confirmare din partea inspectorului sau a autorităților naționale de supraveghere privind transmiterea sau punerea la dispoziție a datelor care o privesc, sau lipsa acestor acțiuni, și informații cu privire la destinatarii sau categoriile de destinatari cărora li s-au dezvăluit datele și comunicarea datelor care fac obiectul prelucrării; sau

(b) cel puțin o confirmare din partea autorității naționale de supraveghere că toate verificările necesare au fost efectuate.

(2) Statele membre pot adopta măsuri legislative care să restricționeze accesul la informații în conformitate cu alineatul (1) litera (a), în cazul în care o astfel de restricție, cu respectarea intereselor legitime ale persoanei vizate, reprezintă o măsură necesară și proporțională:

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

(b) pentru a evita compromiterea prevenirii, a descoperirii, a cercetării și a urmăririi penale a infracțiunilor sau a executării pedepselor;

(c) pentru a proteja securitatea publică;

(d) pentru a proteja siguranța națională;

(e) pentru a proteja persoana vizată sau drepturile și a libertățile celorlalți.

(3) Orice refuz sau restricționare a accesului se comunică în scris persoanei vizate. În același timp, trebuie comunicate persoanei vizate și motivele de fapt sau de drept care au stat la baza deciziei. În cazul existenței unui motiv în temeiul alineatului (2) literele (a)-(e), comunicarea menționată poate lipsi. În toate aceste cazuri, persoana vizată este informată că poate înainta o plângere pe lângă autoritatea națională de supraveghere competentă, pe lângă o autoritate judiciară sau unei curți.

Articolul 18

Dreptul la rectificare, ștergere sau blocare

(1) Persoana vizată are dreptul de a pretinde inspectorului să își îndeplinească obligațiile în conformitate cu articolele 4, 8 și 9 cu privire la rectificarea, ștergerea sau blocarea de date cu caracter personal prevăzute de prezenta decizie-cadru. Statele membre pot să stabilească dacă persoana vizată poate exercita acest drept în mod direct împotriva inspectorului sau prin intermediul autorității naționale de supraveghere competente. În cazul în care inspectorul refuză rectificarea, ștergerea sau blocarea, refuzul trebuie comunicat în scris persoanei vizate, iar aceasta trebuie să fie informată în legătură cu posibilitățile prevăzute de legislația națională pentru depunerea unei plângeri sau exercitarea unei căi de atac. După examinarea plângerii sau a căii de atac, persoana vizată este informată dacă inspectorul a acționat sau nu corespunzător. Statele membre pot dispune, de asemenea, ca persoana vizată să fie informată de către autoritatea națională de supraveghere competentă în legătură cu efectuarea revizuirii.

(2) În cazul în care exactitatea unor date cu caracter personal este contestată de persoana vizată, iar exactitatea sau inexactitatea datelor respective nu se poate stabili cu certitudine, acestora li se pot atribui referințe.

Articolul 19

Dreptul la compensație

(1) Orice persoană care a suferit prejudicii ca urmare a unei prelucrări nelegale sau a oricărei acțiuni incompatibile cu dispozițiile legislației naționale adoptate în temeiul prezentei decizii-cadru are dreptul să obțină despăgubiri pentru prejudiciul suferit de la inspector sau de la o altă autoritate competentă conform legislației naționale.

(2) În cazul în care o autoritate competentă dintr-un stat membru a transmis date cu caracter personal, destinatarul nu poate invoca inexactitatea datelor furnizate drept motiv pentru a se sustrage răspunderii care îi revine față de partea vătămată în conformitate cu legislația națională. În cazul în care destinatarul plătește despăgubiri pentru prejudiciile create ca urmare a utilizării unor date inexacte furnizate, autoritatea competentă care a transmis datele rambursează în totalitate destinatarului suma plătită ca despăgubiri, ținând cont de orice eroare imputabilă destinatarului.

Articolul 20

Căile de atac

Fără a aduce atingere niciunei căi de atac administrative care poate fi prevăzută anterior sesizării autorității judiciare, persoana vizată are dreptul la exercitarea unei căi de atac în cazul oricărei încălcări a drepturilor care îi sunt garantate prin legislația națională aplicabilă.

Articolul 21

Confidențialitatea prelucrării

(1) Orice persoană care are acces la datele cu caracter personal aparținând domeniului prezentei decizii-cadru poate prelucra datele respective numai dacă face parte sau dacă acționează potrivit dispozițiilor unei autorități competente, cu excepția cazului în care există dispoziții legale în acest sens.

(2) Persoanele cărora li se solicită să lucreze pentru o autoritate competentă a unui stat membru au obligația de a respecta toate normele pentru protecția datelor care se aplică autorității competente în cauză.

Articolul 22

Securitatea prelucrărilor

(1) Statele membre dispun aplicarea obligatorie de către autoritățile competente a unor măsuri tehnice și organizatorice adecvate pentru protecția datelor cu caracter personal împotriva distrugerii accidentale sau nelegale, pierderii accidentale, modificării, dezvăluirii sau accesului neautorizat, în special în cazul în care prelucrarea presupune transmiterea datelor într-o rețea sau punerea la dispoziție prin acordarea accesului direct automat, precum și împotriva oricărei alte forme de prelucrare nelegală, având în vedere riscurile speciale pe care le prezintă prelucrarea datelor pentru care este necesară protecția, precum și natura acestora. Având în vedere cele mai noi tehnici din sector și costurile punerii lor în aplicare, aceste măsuri trebuie să asigure un nivel de securitate corespunzător riscurilor pe care le prezintă prelucrarea datelor pentru care este necesară protecția, precum și natura acestor date.

(2) În ceea ce privește prelucrarea automatizată a datelor, fiecare stat membru pune în aplicare măsuri destinate:

(a) să împiedice accesul persoanelor neautorizate la echipamentele de prelucrare a datelor cu caracter personal (controlul accesului la echipamente);

(b) să împiedice citirea, copierea, modificarea sau eliminarea suportului de date în mod neautorizat (controlul suportului de date);

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

(d) să împiedice utilizarea sistemelor de prelucrare automatizată a datelor de către persoane neautorizate cu ajutorul echipamentelor de comunicare a datelor (controlul asupra utilizatorilor);

(e) să asigure că persoanele autorizate care utilizează un sistem de prelucrare automatizată a datelor au acces numai la datele pentru care au autorizare (controlul accesului la date);

(f) să asigure posibilitatea verificării sau stabilirii identității autorităților cărora li s-au transmis sau li se pot transmite sau li se pun la dispoziție date cu caracter personal cu ajutorul echipamentelor de comunicații pentru date (controlul asupra comunicațiilor);

(g) să asigure posibilitatea verificării sau stabilirii ulterioare a datelor cu caracter personal care au fost introduse în sisteme automatizate de prelucrarea datelor, precum și a datei și persoanei care a introdus datele (controlul asupra introducerii datelor);

(h) să împiedice citirea, copierea, modificarea sau ștergerea neautorizate de date cu caracter personal în timpul transferurilor de date cu caracter personal sau în timpul transportului suporturilor de date (control asupra transportului);

(i) să asigure posibilitatea repunerii în funcțiune a sistemelor instalate în cazul unei defecțiuni (recuperarea);

(j) să asigure funcționarea sistemului, raportarea incidenței oricăror erori ale funcțiilor (fiabilitate) și că nicio disfuncționalitate a sistemului nu poate duce la coruperea datelor stocate (integritate).

(3) Statele membre dispun că operatorii de prelucrare pot fi desemnați numai în cazul în care aceștia garantează respectarea măsurilor tehnice și organizaționale în temeiul alineatului (1) și respectarea instrucțiunilor în temeiul articolului 21. Autoritatea competentă monitorizează operatorul de prelucrare în acest sens.

(4) Datele cu caracter personal pot fi prelucrate de un operator de prelucrare doar în temeiul unui act juridic sau a unui contract scris.

Articolul 23

Consultarea prealabilă

Statele membre asigură că autoritățile naționale de supraveghere competente sunt consultate înainte de prelucrarea datelor cu caracter personal care vor face parte dintr-un nou sistem de evidență care urmează a fi creat, în cadrul căruia:

(a) urmează a fi prelucrate categorii speciale de date menționate la articolul 6, sau

(b) tipul de prelucrare, în special cel care implică utilizarea de noi tehnologii, mecanisme sau proceduri, prezintă în caz contrar riscuri specifice pentru drepturile și libertățile fundamentale ale persoanei vizate, și în special pentru viața privată a acesteia.

Articolul 24

Sancțiuni

Statele membre adoptă măsurile corespunzătoare pentru a asigura aplicarea integrală a dispozițiilor prezentei decizii-cadru și, în special, stabilesc sancțiuni eficace, proporționale și disuasive, care urmează să fie aplicate în caz de încălcare a dispozițiilor adoptate în temeiul prezentei decizii-cadru.

Articolul 25

Autoritățile naționale de supraveghere

(1) Fiecare stat membru dispune ca una sau mai multe dintre autoritățile publice să răspundă de informarea și monitorizarea punerii în aplicare pe teritoriul său a dispozițiilor adoptate de statele membre în conformitate cu decizia-cadru. Aceste autorități acționează în deplină independență în exercitarea funcțiilor încredințate lor.

(2) Fiecare autoritate este învestită, în special, cu următoarele:

(a) competențe de cercetare, competențe de acces la datele care fac obiectul unei prelucrări și competențe de colectare a tuturor informațiilor necesare pentru îndeplinirea atribuțiilor de supraveghere;

(b) competențe efective de intervenție, cum ar fi, de exemplu, competența de a emite avize înainte ca operațiunile de prelucrare să fie efectuate și de a asigura publicarea corespunzătoare a acestor avize sau de a ordona blocarea, ștergerea sau distrugerea datelor, de a impune interdicția temporară sau definitivă de prelucrare, de a adresa inspectorului un avertisment sau o mustrare sau de a sesiza parlamentele naționale sau alte instituții politice;

(c) competența de a acționa în justiție, în cazul încălcării dispozițiilor legislației naționale adoptate în temeiul prezentei decizii-cadru sau de a sesiza autoritățile judecătorești cu privire la această încălcare. Deciziile autorităților de supraveghere care fac obiectul unor plângeri pot fi atacate în justiție.

(3) Fiecare autoritate de supraveghere poate fi sesizată de orice persoană printr-o plângere privind protecția drepturilor și libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal. Persoana vizată este informată asupra modului în care s-a soluționat plângerea.

(4) Statele membre prevăd obligația care revine membrilor și personalului autorității de supraveghere de a respecta dispozițiile privind protecția datelor cu caracter personal aplicabile respectivei autorități de supraveghere și faptul că, chiar și după încetarea activității acestora, acestora le revine obligația de a păstra secretul profesional în ceea ce privește informațiile confidențiale la care au acces.

Articolul 26

Legătura cu acordurile încheiate cu state terțe

Prezenta decizie-cadru nu aduce atingere niciunei obligații și niciunui angajament care revin statelor membre sau Uniunii în temeiul unor acorduri bilaterale și/sau multilaterale cu state terțe, existente în momentul adoptării deciziei-cadru.

Pentru aplicarea acestor acorduri, transferul către un stat terț a datelor cu caracter personal obținute de la un alt stat membru se efectuează în conformitate cu articolul 13 alineatul (1) litera (c) și, după caz, alineatul (2).

Articolul 27

Evaluare

(1) Statele membre raportează Comisiei în legătură cu măsurile naționale adoptate pentru a asigura deplina conformitate cu prezenta decizie-cadru și, în special, cu privire la acele dispoziții care trebuie să fie deja respectate la colectarea datelor, până la 27 noiembrie 2013. Comisia examinează cu precădere impactul dispoziției asupra domeniului de aplicare al prezentei decizii-cadru, prevăzut la articolul 1 alineatul (2).

(2) În termen de un an de la rezultatul evaluării menționate la alineatul (1), Comisia prezintă un raport Parlamentului European și Consiliului, raportul fiind însoțit de propuneri corespunzătoare de modificare a prezentei decizii-cadru.

Articolul 28

Legătura cu actele anterioare adoptate de Uniune

Atunci când în actele adoptate în temeiul titlului VI din Tratatul privind Uniunea Europeană înaintea datei intrării în vigoare a prezentei decizii-cadru și care reglementează schimbul de date cu caracter personal între statele membre sau accesul autorităților desemnate ale statelor membre la sistemele informatice instituite în temeiul Tratatului de instituire a Comunității Europene au fost introduse condiții specifice privind utilizarea acestor date de către statul membru destinatar, aceste condiții prevalează în fața dispozițiilor din prezenta decizie-cadru referitoare la utilizarea datelor primite sau puse la dispoziție de către un alt stat membru.

Articolul 29

Punerea în aplicare

(1) Statele membre iau măsurile necesare pentru a se conforma dispozițiilor prezentei decizii-cadru până la 27 noiembrie 2010.

(2) Statele membre comunică, până la aceeași dată, Secretariatului General al Consiliului și Comisiei textul dispozițiilor care transpun în legislațiile lor naționale obligațiile impuse prin prezenta decizie-cadru, precum și informații privind desemnarea autorităților de supraveghere prevăzute la articolul 25. Pe baza unui raport întocmit de Comisie în temeiul acestor informații, Consiliul evaluează până la 27 noiembrie 2011 modul în care statele membre au luat măsurile necesare pentru a se conforma prezentei decizii-cadru.

Articolul 30

Intrarea în vigoare

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

Adoptată la Bruxelles, 27 noiembrie 2008.

Pentru Consiliu

Președintele

M. ALLIOT-MARIE