REGULAMENT nr. 679 din 27 aprilie 2016

privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor) (Text cu relevanţă pentru SEE)

PARLAMENTUL EUROPEAN ŞI CONSILIUL UNIUNII EUROPENE, având în vedere **Tratatul privind funcţionarea Uniunii Europene**, în special articolul 16, având în vedere propunerea Comisiei Europene, după transmiterea proiectului de act legislativ către parlamentele naţionale, având în vedere avizul Comitetului Economic şi Social European (1) , (1) JO C 229, 31.7.2012, p. 90. având în vedere avizul Comitetului Regiunilor (2) , (2) JO C 391, 18.12.2012, p. 127. hotărând în conformitate cu procedura legislativă ordinară (3) , (3) Poziţia Parlamentului European din 12 martie 2014 (nepublicată încă în Jurnalul Oficial) şi Poziţia în primă lectură a Consiliului din 8 aprilie 2016 (nepublicată încă în Jurnalul Oficial) . Poziţia Parlamentului European din 14 aprilie 2016.

întrucât:

(1) Protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din **Carta drepturilor fundamentale a Uniunii Europene** ("carta") şi articolul 16 alineatul (1) din **Tratatul privind funcţionarea Uniunii Europene** (TFUE) prevăd dreptul oricărei persoane la protecţia datelor cu caracter personal care o privesc.

(2) Principiile şi normele referitoare la protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor lor cu caracter personal ar trebui, indiferent de cetăţenia sau de locul de reşedinţă al persoanelor fizice, să respecte drepturile şi libertăţile fundamentale ale acestora, în special dreptul la protecţia datelor cu caracter personal. Prezentul regulament urmăreşte să contribuie la realizarea unui spaţiu de libertate, securitate şi justiţie şi a unei uniuni economice, la progresul economic şi social, la consolidarea şi convergenţa economiilor în cadrul pieţei interne şi la bunăstarea persoanelor fizice.

(3) Directiva **95/46/CE** a Parlamentului European şi a Consiliului (4) vizează armonizarea nivelului de protecţie a drepturilor şi libertăţilor fundamentale ale persoanelor fizice în ceea ce priveşte activităţile de prelucrare şi asigurarea liberei circulaţii a datelor cu caracter personal între statele membre.

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

(4) Prelucrarea datelor cu caracter personal ar trebui să fie în serviciul cetăţenilor. Dreptul la protecţia datelor cu caracter personal nu este un drept absolut; acesta trebuie luat în considerare în raport cu funcţia pe care o îndeplineşte în societate şi echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporţionalităţii. Prezentul regulament respectă toate drepturile fundamentale şi libertăţile şi principiile recunoscute în **cartă** astfel cum sunt consacrate în tratate, în special respectarea vieţii private şi de familie, a reşedinţei şi a comunicaţiilor, a protecţiei datelor cu caracter personal, a libertăţii de gândire, de conştiinţă şi de religie, a libertăţii de exprimare şi de informare, a libertăţii de a desfăşura o activitate comercială, dreptul la o cale de atac eficientă şi la un proces echitabil, precum şi diversitatea culturală, religioasă şi lingvistică.

(5) Integrarea economică şi socială care rezultă din funcţionarea pieţei interne a condus la o creştere substanţială a fluxurilor transfrontaliere de date cu caracter personal. Schimbul de date cu caracter personal între actori publici şi privaţi, inclusiv persoane fizice, asociaţii şi întreprinderi, s-a intensificat în întreaga Uniune. Conform dreptului Uniunii, autorităţile naţionale din statele membre sunt chemate să coopereze şi să facă schimb de date cu caracter personal pentru a putea să îşi îndeplinească atribuţiile sau să execute sarcini în numele unei autorităţi dintr-un alt stat membru.

(6) Evoluţiile tehnologice rapide şi globalizarea au generat noi provocări pentru protecţia datelor cu caracter personal. Amploarea colectării şi a schimbului de date cu caracter personal a crescut în mod semnificativ. Tehnologia permite atât societăţilor private, cât şi autorităţilor publice să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităţilor lor. Din ce în ce mai mult, persoanele fizice fac publice la nivel mondial informaţii cu caracter personal. Tehnologia a transformat deopotrivă economia şi viaţa socială şi ar trebui să faciliteze în continuare libera circulaţie a datelor cu caracter personal în cadrul Uniunii şi transferul către ţări terţe şi organizaţii internaţionale, asigurând, totodată, un nivel ridicat de protecţie a datelor cu caracter personal.

(7) Aceste evoluţii impun un cadru solid şi mai coerent în materie de protecţie a datelor în Uniune, însoţit de o aplicare riguroasă a normelor, luând în considerare importanţa creării unui climat de încredere care va permite economiei digitale să se dezvolte pe piaţa internă. Persoanele fizice ar trebui să aibă control asupra propriilor date cu caracter personal, iar securitatea juridică şi practică pentru persoane fizice, operatori economici şi autorităţi publice ar trebui să fie consolidată.

(8) În cazul în care prezentul regulament prevede specificări sau restricţionări ale normelor sale de către dreptul intern, statele membre pot, în măsura în care acest lucru este necesar pentru coerenţă şi pentru a asigura înţelegerea dispoziţiilor naţionale de către persoanele cărora li se aplică acestea, să încorporeze elemente din prezentul regulament în dreptul lor intern.

(9) Obiectivele şi principiile Directivei **95/46/CE** rămân solide, dar aceasta nu a prevenit fragmentarea modului în care protecţia datelor este pusă în aplicare în Uniune, insecuritatea juridică sau percepţia publică larg răspândită conform căreia există riscuri semnificative pentru protecţia persoanelor fizice, în special în legătură cu activitatea online. Diferenţele dintre nivelurile de protecţie a drepturilor şi libertăţilor persoanelor fizice, în special a dreptului la protecţia datelor cu caracter personal, în ceea ce priveşte prelucrarea datelor cu caracter personal din statele membre pot împiedica libera circulaţie a datelor cu caracter personal în întreaga Uniune. Aceste diferenţe pot constitui, prin urmare, un obstacol în desfăşurarea de activităţi economice la nivelul Uniunii, pot denatura concurenţa şi pot împiedica autorităţile să îndeplinească responsabilităţile care le revin în temeiul dreptului Uniunii. Această diferenţă între nivelurile de protecţie este cauzată de existenţa unor deosebiri în ceea ce priveşte transpunerea şi aplicarea Directivei **95/46/CE**.

(10) Pentru a se asigura un nivel consecvent şi ridicat de protecţie a persoanelor fizice şi pentru a se îndepărta obstacolele din calea circulaţiei datelor cu caracter personal în cadrul Uniunii, nivelul protecţiei drepturilor şi libertăţilor persoanelor fizice în ceea ce priveşte prelucrarea unor astfel de date ar trebui să fie echivalent în toate statele membre. Aplicarea consecventă şi omogenă a normelor în materie de protecţie a drepturilor şi libertăţilor fundamentale ale persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal ar trebui să fie asigurată în întreaga Uniune. În ceea ce priveşte prelucrarea datelor cu caracter personal în vederea respectării unei obligaţii legale, a îndeplinirii unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul, statelor membre ar trebui să li se permită să menţină sau să introducă dispoziţii de drept intern care să clarifice într-o mai mare măsură aplicarea normelor prezentului regulament. În coroborare cu legislaţia generală şi orizontală privind protecţia datelor, prin care este pusă în aplicare Directiva **95/46/CE**, statele membre au mai multe legi sectoriale specifice în domenii care necesită dispoziţii mai precise. Prezentul regulament oferă, de asemenea, statelor membre o marjă de manevră în specificarea normelor sale, inclusiv în ceea ce priveşte prelucrarea categoriilor speciale de date cu caracter personal ("date sensibile") . În acest sens, prezentul regulament nu exclude dreptul statelor membre care stabileşte circumstanţele aferente unor situaţii de prelucrare specifice, inclusiv stabilirea cu o mai mare precizie a condiţiilor în care prelucrarea datelor cu caracter personal este legală.

(11) Protecţia efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea şi stabilirea în detaliu a drepturilor persoanelor vizate şi a obligaţiilor celor care prelucrează şi decid prelucrarea datelor cu caracter personal, ci şi competenţe echivalente pentru monitorizarea şi asigurarea conformităţii cu normele de protecţie a datelor cu caracter personal şi sancţiuni echivalente pentru infracţiuni în statele membre.

(12) Articolul 16 alineatul (2) din **TFUE** mandatează Parlamentul European şi Consiliul să stabilească normele privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal, precum şi normele privind libera circulaţie a acestor date.

(13) În vederea asigurării unui nivel uniform de protecţie pentru persoanele fizice în întreaga Uniune şi a preîntâmpinării discrepanţelor care împiedică libera circulaţie a datelor în cadrul pieţei interne, este necesar un regulament în scopul de a furniza securitate juridică şi transparenţă pentru operatorii economici, inclusiv microîntreprinderi şi întreprinderi mici şi mijlocii, precum şi de a oferi persoanelor fizice în toate statele membre acelaşi nivel de drepturi, obligaţii şi responsabilităţi opozabile din punct de vedere juridic pentru operatori şi persoanele împuternicite de aceştia, pentru a se asigura o monitorizare coerentă a prelucrării datelor cu caracter personal, sancţiuni echivalente în toate statele membre, precum şi cooperarea eficace a autorităţilor de supraveghere ale diferitelor state membre. Pentru buna funcţionare a pieţei interne este necesar ca libera circulaţie a datelor cu caracter personal în cadrul Uniunii să nu fie restricţionată sau interzisă din motive legate de protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal. Pentru a se lua în considerare situaţia specifică a microîntreprinderilor şi a întreprinderilor mici şi mijlocii, prezentul regulament include o derogare pentru organizaţiile cu mai puţin de 250 de angajaţi în ceea ce priveşte păstrarea evidenţelor. În plus, instituţiile şi organele Uniunii şi statele membre şi autorităţile lor de supraveghere sunt încurajate să ia în considerare necesităţile specifice ale microîntreprinderilor şi ale întreprinderilor mici şi mijlocii în aplicarea prezentului regulament. Noţiunea de microîntreprinderi şi de întreprinderi mici şi mijlocii ar trebui să se bazeze pe articolul 2 din anexa la Recomandarea 2003/361/CE a Comisiei (1) .

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

(14) Protecţia conferită de prezentul regulament ar trebui să vizeze persoanele fizice, indiferent de cetăţenia sau de locul de reşedinţă al acestora, în ceea ce priveşte prelucrarea datelor cu caracter personal ale acestora. Prezentul regulament nu se aplică prelucrării datelor cu caracter personal care privesc persoane juridice şi, în special, întreprinderi cu personalitate juridică, inclusiv numele şi tipul de persoană juridică şi datele de contact ale persoanei juridice.

(15) Pentru a preveni apariţia unui risc major de eludare, protecţia persoanelor fizice ar trebui să fie neutră din punct de vedere tehnologic şi să nu depindă de tehnologiile utilizate. Protecţia persoanelor fizice ar trebui să se aplice prelucrării datelor cu caracter personal prin mijloace automatizate, precum şi prelucrării manuale, în cazul în care datele cu caracter personal sunt cuprinse sau destinate să fie cuprinse într-un sistem de evidenţă. Dosarele sau seturile de dosare, precum şi coperţile acestora, care nu sunt structurate în conformitate cu criterii specifice nu ar trebui să intre în domeniul de aplicare al prezentului regulament.

(16) Prezentul regulament nu se aplică chestiunilor de protecţie a drepturilor şi libertăţilor fundamentale sau la libera circulaţie a datelor cu caracter personal referitoare la activităţi care nu intră în domeniul de aplicare al dreptului Uniunii, de exemplu activităţile privind securitatea naţională. Prezentul regulament nu se aplică prelucrării datelor cu caracter personal de către statele membre atunci când acestea desfăşoară activităţi legate de politica externă şi de securitatea comună a Uniunii.

(17) Regulamentul (CE) nr. **45/2001** al Parlamentului European şi al Consiliului (2) se aplică prelucrării de date cu caracter personal de către instituţiile, organele, oficiile şi agenţiile Uniunii. Regulamentul (CE) nr. **45/2001** şi alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal ar trebui adaptate la principiile şi normele stabilite în prezentul regulament şi aplicate în conformitate cu prezentul regulament. În vederea asigurării unui cadru solid şi coerent în materie de protecţie a datelor în Uniune, ar trebui ca după adoptarea prezentului regulament să se aducă Regulamentului (CE) nr. **45/2001** adaptările necesare, astfel încât acestea să poată fi aplicate odată cu prezentul regulament.

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

(18) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal de către o persoană fizică în cadrul unei activităţi exclusiv personale sau domestice şi care, prin urmare, nu are legătură cu o activitate profesională sau comercială. Activităţile personale sau domestice ar putea include corespondenţa şi repertoriul de adrese sau activităţile din cadrul reţelelor sociale şi activităţile online desfăşurate în contextul respectivelor activităţi. Cu toate acestea, prezentul regulament se aplică operatorilor sau persoanelor împuternicite de operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activităţi personale sau domestice.

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

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

În ceea ce priveşte prelucrarea datelor cu caracter personal de către aceste autorităţi competente în scopuri care intră în domeniul de aplicare al prezentului regulament, statele membre ar trebui să poată menţine sau introduce dispoziţii mai detaliate pentru a adapta aplicarea normelor din prezentul regulament. Aceste dispoziţii pot stabili mai precis cerinţe specifice pentru prelucrarea datelor cu caracter

personal de către respectivele autorităţi competente în aceste alte scopuri, ţinând seama de structura constituţională, organizatorică şi administrativă a statului membru în cauză. Atunci când prelucrarea de date cu caracter personal de către organisme private face obiectul prezentului regulament, prezentul regulament ar trebui să prevadă posibilitatea ca statele membre, în anumite condiţii, să impună prin lege restricţii asupra anumitor obligaţii şi drepturi, în cazul în care asemenea restricţii constituie o măsură necesară şi proporţională într-o societate democratică în scopul garantării unor interese specifice importante, printre care se numără siguranţa publică şi prevenirea, investigarea, depistarea şi urmărirea penală a infracţiunilor sau executarea pedepselor, inclusiv protejarea împotriva ameninţărilor la adresa siguranţei publice şi prevenirea acestora. Acest lucru este relevant, de exemplu, în cadrul combaterii spălării de bani sau al activităţilor laboratoarelor criminalistice.

(20) Deşi prezentul regulament se aplică, inter alia, activităţilor instanţelor şi ale altor autorităţi judiciare, dreptul Uniunii sau al statelor membre ar putea să precizeze operaţiunile şi procedurile de prelucrare în ceea ce priveşte prelucrarea datelor cu caracter personal de către instanţe şi alte autorităţi judiciare. Prelucrarea datelor cu caracter personal nu ar trebui să fie de competenţa autorităţilor de supraveghere în cazul în care instanţele îşi exercită atribuţiile judiciare, în scopul garantării independenţei sistemului judiciar în îndeplinirea sarcinilor sale judiciare, inclusiv în luarea deciziilor. Supravegherea unor astfel de operaţiuni de prelucrare a datelor ar trebui să poată fi încredinţată unor organisme specifice din cadrul sistemului judiciar al statului membru, care ar trebui să asigure în special respectarea normelor prevăzute de prezentul regulament, să sensibilizeze membrii sistemului judiciar cu privire la obligaţiile care le revin în temeiul prezentului regulament şi să trateze plângerile în legătură cu astfel de operaţiuni de prelucrare a datelor.

(21) Prezentul regulament nu aduce atingere aplicării Directivei **2000/31/CE** a Parlamentului European şi a Consiliului (2) , în special normelor privind răspunderea furnizorilor intermediari de servicii prevăzute la articolele 12-15 din directiva menţionată. Respectiva directivă îşi propune să contribuie la buna funcţionare a pieţei interne, prin asigurarea liberei circulaţii a serviciilor societăţii informaţionale între statele membre.

(2) Directiva **2000/31/CE** a Parlamentului European şi a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societăţii informaţionale, în special ale comerţului electronic, pe piaţa internă (directiva privind comerţul electronic) (JO L 178, 17.7.2000, p. 1) .

(22) Orice prelucrare a datelor cu caracter personal în cadrul activităţilor unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune ar trebui efectuată în conformitate cu prezentul regulament, indiferent dacă procesul de prelucrare în sine are loc sau nu în cadrul Uniunii. Sediul implică exercitarea efectivă şi reală a unei activităţi în cadrul unor înţelegeri stabile. Forma juridică a unor astfel de înţelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privinţă.

(23) Pentru a se asigura că persoanele fizice nu sunt lipsite de protecţia la care au dreptul în temeiul prezentului regulament, prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Uniunii de către un operator sau o persoană împuternicită de acesta care nu îşi are sediul în Uniune ar trebui să facă obiectul prezentului regulament în cazul în care activităţile de prelucrare au legătură cu oferirea de bunuri sau servicii unor astfel de persoane vizate, indiferent dacă acestea sunt sau nu legate de o plată. Pentru a determina dacă un astfel de operator sau o astfel de persoană împuternicită de operator oferă bunuri sau servicii unor persoane vizate care se află pe teritoriul Uniunii, ar trebui să se stabilească dacă reiese că operatorul sau persoana împuternicită de operator intenţionează să furnizeze servicii persoanelor vizate din unul sau mai multe state membre din Uniune. Întrucât simplul fapt că există acces la un site al operatorului, al persoanei împuternicite de operator sau al unui intermediar în Uniune, că este disponibilă o adresă de e-mail şi alte date de contact sau că este utilizată o limbă folosită în general în ţara terţă în care operatorul îşi are sediul este insuficient pentru a confirma o astfel de intenţie, factori precum utilizarea unei limbi sau a unei monede utilizate în general în unul sau mai multe state membre cu posibilitatea de a comanda bunuri şi servicii în respectiva limbă sau menţionarea unor clienţi sau utilizatori care se află pe teritoriul Uniunii pot conduce la concluzia că operatorul intenţionează să ofere bunuri sau servicii unor persoane vizate în Uniune.

(24) Prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Uniunii de către un operator sau o persoană împuternicită de acesta care nu îşi are sediul în Uniune ar trebui, de asemenea, să facă obiectul prezentului regulament în cazul în care este legată de monitorizarea comportamentului unor astfel de persoane vizate, în măsura în care acest comportament se manifestă pe teritoriul Uniunii. Pentru a se determina dacă o activitate de prelucrare poate fi considerată ca

"monitorizare a comportamentului" persoanelor vizate, ar trebui să se stabilească dacă persoanele fizice sunt urmărite pe internet, inclusiv posibila utilizare ulterioară a unor tehnici de prelucrare a datelor cu caracter personal care constau în crearea unui profil al unei persoane fizice, în special în scopul de a lua decizii cu privire la aceasta sau de a analiza sau de a face previziuni referitoare la preferinţele personale, comportamentele şi atitudinile acesteia.

(25) În cazul în care dreptul unui stat membru se aplică în temeiul dreptului internaţional public, prezentul regulament ar trebui să se aplice, de asemenea, unui operator care nu este stabilit în Uniune, ci, de exemplu, într-o misiune diplomatică sau într-un oficiu consular al unui stat membru.

(26) Principiile protecţiei datelor ar trebui să se aplice oricărei informaţii referitoare la o persoană fizică identificată sau identificabilă. Datele cu caracter personal care au fost supuse pseudonimizării, care ar putea fi atribuite unei persoane fizice prin utilizarea de informaţii suplimentare, ar trebui considerate informaţii referitoare la o persoană fizică identificabilă. Pentru a se determina dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană, în scopul identificării, în mod direct sau indirect, a persoanei fizice respective. Pentru a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace pentru identificarea persoanei fizice, ar trebui luaţi în considerare toţi factorii obiectivi, precum costurile şi intervalul de timp necesare pentru identificare, ţinându-se seama atât de tehnologia disponibilă la momentul prelucrării, cât şi de dezvoltarea tehnologică. Principiile protecţiei datelor ar trebui, prin urmare, să nu se aplice informaţiilor anonime, adică informaţiilor care nu sunt legate de o persoană fizică identificată sau identificabilă sau datelor cu caracter personal care sunt anonimizate astfel încât persoana vizată nu este sau nu mai este identificabilă. Prin urmare, prezentul regulament nu se aplică prelucrării unor astfel de informaţii anonime, inclusiv în cazul în care acestea sunt utilizate în scopuri statistice sau de cercetare.

(27) Prezentul regulament nu se aplică datelor cu caracter personal referitoare la persoane decedate. Statele membre pot să prevadă norme privind prelucrarea datelor cu caracter personal referitoare la persoane decedate.

(28) Aplicarea pseudonimizării datelor cu caracter personal poate reduce riscurile pentru persoanele vizate şi poate ajuta operatorii şi persoanele împuternicite de aceştia să îşi îndeplinească obligaţiile de protecţie a datelor. Introducerea explicită a conceptului de "pseudonimizare" în prezentul regulament nu este destinată să împiedice alte eventuale măsuri de protecţie a datelor.

(29) Pentru a crea stimulente pentru aplicarea pseudonimizării atunci când sunt prelucrate date cu caracter personal, ar trebui să fie posibile măsuri de pseudonimizare, permiţând în acelaşi timp analiza generală, în cadrul aceluiaşi operator atunci când operatorul a luat măsurile tehnice şi organizatorice necesare pentru a se asigura că prezentul regulament este pus în aplicare în ceea ce priveşte respectiva prelucrare a datelor şi că informaţiile suplimentare pentru atribuirea datelor cu caracter personal unei anumite persoane vizate sunt păstrate separat. Operatorul care prelucrează datele cu caracter personal ar trebui să indice persoanele autorizate din cadrul aceluiaşi operator.

(30) Persoanele fizice pot fi asociate cu identificatorii online furnizaţi de dispozitivele, aplicaţiile, instrumentele şi protocoalele lor, cum ar fi adresele IP, identificatorii cookie sau alţi identificatori precum etichetele de identificare prin frecvenţe radio. Aceştia pot lăsa urme care, în special atunci când sunt combinate cu identificatori unici şi alte informaţii primite de servere, pot fi utilizate pentru crearea de profiluri ale persoanelor fizice şi pentru identificarea lor.

(31) Autorităţile publice cărora le sunt divulgate date cu caracter personal în conformitate cu o obligaţie legală în vederea exercitării funcţiei lor oficiale, cum ar fi autorităţile fiscale şi vamale, unităţile de investigare financiară, autorităţile administrative independente sau autorităţile pieţelor financiare responsabile de reglementarea şi supravegherea pieţelor titlurilor de valoare, nu ar trebui să fie considerate destinatari în cazul în care primesc date cu caracter personal care sunt necesare pentru efectuarea unei anumite anchete de interes general, în conformitate cu dreptul Uniunii sau cel al statelor membre. Cererile de divulgare trimise de autorităţile publice ar trebui să fie întotdeauna prezentate în scris, motivate şi ocazionale şi nu ar trebui să se refere la un sistem de evidenţă în totalitate sau să conducă la interconectarea sistemelor de evidenţă. Prelucrarea datelor cu caracter personal de către autorităţile publice respective ar trebui să respecte normele aplicabile în materie de protecţie a datelor în conformitate cu scopurile prelucrării.

(32) Consimţământul ar trebui acordat printr-o acţiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoştinţă de cauză şi clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declaraţie făcută în scris, inclusiv în format electronic,

sau verbal. Acesta ar putea include bifarea unei căsuţe atunci când persoana vizitează un site, alegerea parametrilor tehnici pentru serviciile societăţii informaţionale sau orice altă declaraţie sau acţiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absenţa unui răspuns, căsuţele bifate în prealabil sau absenţa unei acţiuni nu ar trebui să constituie un consimţământ. Consimţământul ar trebui să vizeze toate activităţile de prelucrare efectuate în acelaşi scop sau în aceleaşi scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimţământul ar trebui dat pentru toate scopurile prelucrării. În cazul în care consimţământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară şi concisă şi să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimţământul.

(33) Adesea nu este posibil, în momentul colectării datelor cu caracter personal, să se identifice pe deplin scopul prelucrării datelor în scopuri de cercetare ştiinţifică. Din acest motiv, persoanelor vizate ar trebui să li se permită să îşi exprime consimţământul pentru anumite domenii ale cercetării ştiinţifice atunci când sunt respectate standardele etice recunoscute pentru cercetarea ştiinţifică. Persoanele vizate ar trebui să aibă posibilitatea de a-şi exprima consimţământul doar pentru anumite domenii de cercetare sau părţi ale proiectelor de cercetare în măsura permisă de scopul preconizat.

(34) Datele genetice ar trebui definite drept date cu caracter personal referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care rezultă în urma unei analize a unei mostre de material biologic al persoanei fizice în cauză, în special a unei analize cromozomiale, a unei analize a acidului dezoxiribonucleic (ADN) sau a acidului ribonucleic (ARN) sau a unei analize a oricărui alt element ce permite obţinerea unor informaţii echivalente.

(35) Datele cu caracter personal privind sănătatea ar trebui să includă toate datele având legătură cu starea de sănătate a persoanei vizate care dezvăluie informaţii despre starea de sănătate fizică sau mentală trecută, prezentă sau viitoare a persoanei vizate. Acestea includ informaţii despre persoana fizică colectate în cadrul înscrierii acesteia la serviciile de asistenţă medicală sau în cadrul acordării serviciilor respective persoanei fizice în cauză, astfel cum sunt menţionate în Directiva **2011/24/UE** a Parlamentului European şi a Consiliului (1) ; un număr, un simbol sau un semn distinctiv atribuit unei persoane fizice pentru identificarea singulară a acesteia în scopuri medicale; informaţii rezultate din testarea sau examinarea unei părţi a corpului sau a unei substanţe corporale, inclusiv din date genetice şi eşantioane de material biologic; precum şi orice informaţii 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.

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

(36) Sediul principal al unui operator în Uniune ar trebui să fie locul în care se află administraţia centrală a acestuia în Uniune, cu excepţia cazului în care deciziile privind scopurile şi mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului în Uniune. În acest caz, acesta din urmă ar trebui considerat drept sediul principal. Sediul principal al unui operator în Uniune ar trebui să fie determinat conform unor criterii obiective şi ar trebui să implice exercitarea efectivă şi reală a unor activităţi de gestionare care să determine principalele decizii cu privire la scopurile şi mijloacele de prelucrare în cadrul unor înţelegeri stabile. Acest criteriu nu ar trebui să depindă de realizarea prelucrării datelor cu caracter personal în locul respectiv. Prezenţa şi utilizarea mijloacelor tehnice şi a tehnologiilor de prelucrare a datelor cu caracter personal sau activităţile de prelucrare nu constituie un sediu principal şi, prin urmare, nu sunt criteriul determinant în acest sens. Sediul principal al persoanei împuternicite de operator ar trebui să fie locul în care se află administraţia centrală a acestuia în Uniune sau, în cazul în care nu are o administraţie centrală în Uniune, locul în care se desfăşoară principalele activităţi de prelucrare în Uniune. În cazurile care implică atât operatorul, cât şi persoana împuternicită de operator, autoritatea de supraveghere principală competentă ar trebui să rămână autoritatea de supraveghere a statului membru în care operatorul îşi are sediul principal, dar autoritatea de supraveghere a persoanei împuternicite de operator ar trebui considerată ca fiind o autoritate de supraveghere vizată şi acea autoritate de supraveghere ar trebui să participe la procedura de cooperare prevăzută de prezentul regulament. În orice caz, autorităţile de supraveghere ale statului membru sau ale statelor membre în care persoana împuternicită de operator are unul sau mai multe sedii nu ar trebui considerate ca fiind autorităţi de supraveghere vizate în cazul în care proiectul de decizie nu se referă decât la operator. În cazul în care prelucrarea este efectuată de un grup de întreprinderi, sediul principal al întreprinderii care exercită

controlul ar trebui considerat drept sediul principal al grupului de întreprinderi, cu excepţia cazului în care scopurile şi mijloacele aferente prelucrării sunt stabilite de o altă întreprindere.

(37) Un grup de întreprinderi ar trebui să cuprindă o întreprindere care exercită controlul şi întreprinderile controlate de aceasta, în cadrul căruia întreprinderea care exercită controlul ar trebui să fie întreprinderea care poate exercita o influenţă dominantă asupra celorlalte întreprinderi, de exemplu în temeiul proprietăţii, al participării financiare sau al regulilor care o reglementează sau al competenţei de a pune în aplicare norme în materie de protecţie a datelor cu caracter personal. O întreprindere care controlează prelucrarea datelor cu caracter personal în întreprinderile sale afiliate ar trebui considerată, împreună cu acestea din urmă, drept "grup de întreprinderi".

(38) Copiii au nevoie de o protecţie specifică a datelor lor cu caracter personal, întrucât pot fi mai puţin conştienţi de riscurile, consecinţele, garanţiile în cauză şi drepturile lor în ceea ce priveşte prelucrarea datelor cu caracter personal. Această protecţie specifică ar trebui să se aplice în special utilizării datelor cu caracter personal ale copiilor în scopuri de marketing sau pentru crearea de profiluri de personalitate sau de utilizator şi la colectarea datelor cu caracter personal privind copiii în momentul utilizării serviciilor oferite direct copiilor. Consimţământul titularului răspunderii părinteşti nu ar trebui să fie necesar în contextul serviciilor de prevenire sau consiliere oferite direct copiilor.

(39) Orice prelucrare de date cu caracter personal ar trebui să fie legală şi echitabilă. Ar trebui să fie transparent pentru persoanele fizice că sunt colectate, utilizate, consultate sau prelucrate în alt mod datele cu caracter personal care le privesc şi în ce măsură datele cu caracter personal sunt sau vor fi prelucrate. Principiul transparenţei prevede că orice informaţii şi comunicări referitoare la prelucrarea respectivelor date cu caracter personal sunt uşor accesibile şi uşor de înţeles şi că se utilizează un limbaj simplu şi clar. Acest principiu se referă în special la informarea persoanelor vizate privind identitatea operatorului şi scopurile prelucrării, precum şi la oferirea de informaţii suplimentare, pentru a asigura o prelucrare echitabilă şi transparentă în ceea ce priveşte persoanele fizice vizate şi dreptul acestora de a li se confirma şi comunica datele cu caracter personal care le privesc care sunt prelucrate. Persoanele fizice ar trebui informate cu privire la riscurile, normele, garanţiile şi drepturile în materie de prelucrare a datelor cu caracter personal şi cu privire la modul în care să îşi exercite drepturile în legătură cu prelucrarea. În special, scopurile specifice în care datele cu caracter personal sunt prelucrate ar trebui să fie explicite şi legitime şi să fie determinate la momentul colectării datelor respective. Datele cu caracter personal ar trebui să fie adecvate, relevante şi limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Aceasta necesită, în special, asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum. Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace. În vederea asigurării faptului că datele cu caracter personal nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ştergere sau revizuirea periodică. Ar trebui să fie luate toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau şterse. Datele cu caracter personal ar trebui prelucrate într-un mod care să asigure în mod adecvat securitatea şi confidenţialitatea acestora, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizată a datelor cu caracter personal şi a echipamentului utilizat pentru prelucrare.

(40) Pentru ca prelucrarea datelor cu caracter personal să fie legală, aceasta ar trebui efectuată pe baza consimţământului persoanei vizate sau în temeiul unui alt motiv legitim, prevăzut de lege, fie în prezentul regulament, fie în alt act din dreptul Uniunii sau din dreptul intern, după cum se prevede în prezentul regulament, inclusiv necesitatea respectării obligaţiilor legale la care este supus operatorul sau necesitatea de a executa un contract la care persoana vizată este parte sau pentru a parcurge etapele premergătoare încheierii unui contract, la solicitarea persoanei vizate.

(41) Ori de câte ori prezentul regulament face trimitere la un temei juridic sau la o măsură legislativă, aceasta nu necesită neapărat un act legislativ adoptat de către un parlament, fără a aduce atingere cerinţelor care decurg din ordinea constituţională a statului membru în cauză. Cu toate acestea, un astfel de temei juridic sau o astfel de măsură legislativă ar trebui să fie clară şi precisă, iar aplicarea acesteia ar trebui să fie previzibilă pentru persoanele vizate de aceasta, în conformitate cu jurisprudenţa Curţii de Justiţie a Uniunii Europene ("Curtea de Justiţie") şi a Curţii Europene a Drepturilor Omului.

(42) În cazul în care prelucrarea se bazează pe consimţământul persoanei vizate, operatorul ar trebui să fie în măsură să demonstreze faptul că persoana vizată şi-a dat consimţământul pentru operaţiunea de prelucrare. În special, în contextul unei declaraţii scrise cu privire la un alt aspect, garanţiile ar trebui să asigure că persoana vizată este conştientă de faptul că şi-a dat consimţământul şi în ce măsură a făcut acest lucru. În conformitate cu Directiva **93/13/CEE** a Consiliului (1) , ar trebui furnizată o declaraţie de

consimţământ formulată în prealabil de către operator, într-o formă inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, iar această declaraţie nu ar trebui să conţină clauze abuzive. Pentru ca acordarea consimţământului să fie în cunoştinţă de cauză, persoana vizată ar trebui să fie la curent cel puţin cu identitatea operatorului şi cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal. Consimţământul nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să îşi retragă consimţământul fără a fi prejudiciată.

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

(43) Pentru a garanta faptul că a fost acordat în mod liber, consimţământul nu ar trebui să constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal în cazul particular în care există un dezechilibru evident între persoana vizată şi operator, în special în cazul în care operatorul este o autoritate publică, iar acest lucru face improbabilă acordarea consimţământului în mod liber în toate circumstanţele aferente respectivei situaţii particulare. Consimţământul este considerat a nu fi acordat în mod liber în cazul în care aceasta nu permite să se acorde consimţământul separat pentru diferitele operaţiuni de prelucrare a datelor cu caracter personal, deşi acest lucru este adecvat în cazul particular, sau dacă executarea unui contract, inclusiv furnizarea unui serviciu, este condiţionată de consimţământ, în ciuda faptului că consimţământul în cauză nu este necesar pentru executarea contractului.

(44) Prelucrarea ar trebui să fie considerată legală în cazul în care este necesară în cadrul unui contract sau în vederea încheierii unui contract.

(45) În cazul în care prelucrarea este efectuată în conformitate cu o obligaţie legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care face parte din exercitarea autorităţii publice, prelucrarea ar trebui să aibă un temei în dreptul Uniunii sau în dreptul intern. Prezentul regulament nu impune existenţa unei legi specifice pentru fiecare prelucrare în parte. Poate fi suficientă o singură lege drept temei pentru mai multe operaţiuni de prelucrare efectuate în conformitate cu o obligaţie legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care face parte din exercitarea autorităţii publice. De asemenea, ar trebui ca scopul prelucrării să fie stabilit în dreptul Uniunii sau în dreptul intern. Mai mult decât atât, dreptul respectiv ar putea să specifice condiţiile generale ale prezentului regulament care reglementează legalitatea prelucrării datelor cu caracter personal, să determine specificaţiile pentru stabilirea operatorului, a tipului de date cu caracter personal care fac obiectul prelucrării, a persoanelor vizate, a entităţilor cărora le pot fi divulgate datele cu caracter personal, a limitărilor în funcţie de scop, a perioadei de stocare şi a altor măsuri pentru a garanta o prelucrare legală şi echitabilă. De asemenea, ar trebui să se stabilească în dreptul Uniunii sau în dreptul intern dacă operatorul care îndeplineşte o sarcină care serveşte unui interes public sau care face parte din exercitarea autorităţii publice ar trebui să fie o autoritate publică sau o altă persoană fizică sau juridică guvernată de dreptul public sau, atunci când motive de interes public justifică acest lucru, inclusiv în scopuri medicale, precum sănătatea publică şi protecţia socială, precum şi gestionarea serviciilor de asistenţă medicală, de dreptul privat, cum ar fi o asociaţie profesională.

(46) Prelucrarea datelor cu caracter personal ar trebui, de asemenea, să fie considerată legală în cazul în care este necesară în scopul asigurării protecţiei unui interes care este esenţial pentru viaţa persoanei vizate sau pentru viaţa unei alte persoane fizice. Prelucrarea datelor cu caracter personal care are drept temei interesele vitale ale unei alte persoane fizice ar trebui efectuată numai în cazul în care prelucrarea nu se poate baza în mod evident pe un alt temei juridic. Unele tipuri de prelucrare pot servi atât unor motive importante de interes public, cât şi intereselor vitale ale persoanei vizate, de exemplu în cazul în care prelucrarea este necesară în scopuri umanitare, inclusiv în vederea monitorizării unei epidemii şi a răspândirii acesteia sau în situaţii de urgenţe umanitare, în special în situaţii de dezastre naturale sau provocate de om.

(47) Interesele legitime ale unui operator, inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terţe părţi, pot constitui un temei juridic pentru prelucrare, cu condiţia să nu prevaleze interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate, luând în considerare aşteptările rezonabile ale persoanelor vizate bazate pe relaţia acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relaţie relevantă şi adecvată între persoana vizată şi operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia. În orice caz, existenţa unui interes legitim ar necesita o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată poate preconiza în mod rezonabil, în momentul şi în contextul

colectării datelor cu caracter personal, posibilitatea prelucrării în acest scop. Interesele şi drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date atunci când datele cu caracter personal sunt prelucrate în circumstanţe în care persoanele vizate nu preconizează în mod rezonabil o prelucrare ulterioară. Întrucât legiuitorul trebuie să furnizeze temeiul juridic pentru prelucrarea datelor cu caracter personal de către autorităţile publice, temeiul juridic respectiv nu ar trebui să se aplice prelucrării de către autorităţile publice în îndeplinirea sarcinilor care le revin. Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor constituie, de asemenea, un interes legitim al operatorului de date în cauză. Prelucrarea de date cu caracter personal care are drept scop marketingul direct poate fi considerată ca fiind desfăşurată pentru un interes legitim.

(48) Operatorii care fac parte dintr-un grup de întreprinderi sau instituţii afiliate unui organism central pot avea un interes legitim de a transmite date cu caracter personal în cadrul grupului de întreprinderi în scopuri administrative interne, inclusiv în scopul prelucrării datelor cu caracter personal ale clienţilor sau angajaţilor. Principiile generale ale transferului de date cu caracter personal, în cadrul unui grup de întreprinderi, către o întreprindere situată într-o ţară terţă rămân neschimbate.

(49) Prelucrarea datelor cu caracter personal în măsura strict necesară şi proporţională în scopul asigurării securităţii reţelelor şi a informaţiilor, şi anume capacitatea unei reţele sau a unui sistem de informaţii de a face faţă, la un anumit nivel de încredere, evenimentelor accidentale sau acţiunilor ilegale sau rău intenţionate care compromit disponibilitatea, autenticitatea, integritatea şi confidenţialitatea datelor cu caracter personal stocate sau transmise, precum şi securitatea serviciilor conexe oferite de aceste reţele şi sisteme, sau accesibile prin intermediul acestora, de către autorităţile publice, echipele de intervenţie în caz de urgenţă informatică, echipele de intervenţie în cazul producerii unor incidente care afectează securitatea informatică, furnizorii de reţele şi servicii de comunicaţii electronice, precum şi de către furnizorii de servicii şi tehnologii de securitate, constituie un interes legitim al operatorului de date în cauză. Acesta ar putea include, de exemplu, prevenirea accesului neautorizat la reţelele de comunicaţii electronice şi a difuzării de coduri dăunătoare şi oprirea atacurilor de "blocare a serviciului", precum şi prevenirea daunelor aduse calculatoarelor şi sistemelor de comunicaţii electronice.

(50) Prelucrarea datelor cu caracter personal în alte scopuri decât scopurile pentru care datele cu caracter personal au fost iniţial colectate ar trebui să fie permisă doar atunci când prelucrarea este compatibilă cu scopurile respective pentru care datele cu caracter personal au fost iniţial colectate. În acest caz nu este necesar un temei juridic separat de cel pe baza căruia a fost permisă colectarea datelor cu caracter personal. În cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul, dreptul Uniunii sau dreptul intern poate stabili şi specifica sarcinile şi scopurile pentru care prelucrarea ulterioară ar trebui considerată a fi compatibilă şi legală. Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice ar trebui considerată ca reprezentând operaţiuni de prelucrare legale compatibile. Temeiul juridic prevăzut în dreptul Uniunii sau în dreptul intern pentru prelucrarea datelor cu caracter personal poate constitui, de asemenea, un temei juridic pentru prelucrarea ulterioară. Pentru a stabili dacă scopul prelucrării ulterioare este compatibil cu scopul pentru care au fost colectate iniţial datele cu caracter personal, operatorul, după ce a îndeplinit toate cerinţele privind legalitatea prelucrării iniţiale, ar trebui să ţină seama, printre altele, de orice legătură între respectivele scopuri şi scopurile prelucrării ulterioare preconizate, de contextul în care au fost colectate datele cu caracter personal, în special de aşteptările rezonabile ale persoanelor vizate, bazate pe relaţia lor cu operatorul, în ceea ce priveşte utilizarea ulterioară a datelor, de natura datelor cu caracter personal, de consecinţele prelucrării ulterioare preconizate asupra persoanelor vizate, precum şi de existenţa garanţiilor corespunzătoare atât în cadrul operaţiunilor de prelucrare iniţiale, cât şi în cadrul operaţiunilor de prelucrare ulterioare preconizate. În cazul în care persoana vizată şi-a dat consimţământul sau prelucrarea se bazează pe dreptul Uniunii sau pe dreptul intern, care constituie o măsură necesară şi proporţională într-o societate democratică pentru a proteja, în special, obiective importante de interes public general, operatorul ar trebui să aibă posibilitatea de a prelucra în continuare datele cu caracter personal, indiferent de compatibilitatea scopurilor. În orice caz, aplicarea principiilor stabilite de prezentul regulament şi, în special, informarea persoanei vizate cu privire la aceste alte scopuri şi la drepturile sale, inclusiv dreptul la opoziţie, ar trebui să fie garantate. Indicarea unor posibile infracţiuni sau ameninţări la adresa siguranţei publice de către operator şi transmiterea către o autoritate competentă a datelor cu caracter personal relevante în cazuri individuale sau în mai multe cazuri legate de aceeaşi infracţiune sau de aceleaşi ameninţări la adresa siguranţei publice ar trebui considerată ca fiind în interesul legitim urmărit de operator. Cu toate acestea, o astfel de transmitere în interesul legitim al

operatorului sau prelucrarea ulterioară a datelor cu caracter personal ar trebui interzisă în cazul în care prelucrarea nu este compatibilă cu o obligaţie legală, profesională sau cu o altă obligaţie de păstrare a confidenţialităţii.

(51) Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce priveşte drepturile şi libertăţile fundamentale necesită o protecţie specifică, deoarece contextul prelucrării acestora ar putea genera riscuri considerabile la adresa drepturilor şi libertăţilor fundamentale. Aceste date cu caracter personal ar trebui să includă datele cu caracter personal care dezvăluie originea rasială sau etnică, utilizarea termenului "origine rasială" în prezentul regulament neimplicând o acceptare de către Uniune a teoriilor care urmăresc să stabilească existenţa unor rase umane separate. Prelucrarea fotografiilor nu ar trebui să fie considerată în mod sistematic ca fiind o prelucrare de categorii speciale de date cu caracter personal, întrucât fotografiile intră sub incidenţa definiţiei datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice. Asemenea date cu caracter personal nu ar trebui prelucrate, cu excepţia cazului în care prelucrarea este permisă în cazuri specifice prevăzute de prezentul regulament, ţinând seama de faptul că dreptul statelor membre poate prevedea dispoziţii specifice cu privire la protecţia datelor în scopul adaptării aplicării normelor din prezentul regulament în vederea respectării unei obligaţii legale sau a îndeplinirii unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul. Pe lângă cerinţele specifice pentru o astfel de prelucrare, ar trebui să se aplice principiile generale şi alte norme prevăzute de prezentul regulament, în special în ceea ce priveşte condiţiile pentru prelucrarea legală. Ar trebui prevăzute în mod explicit derogări de la interdicţia generală de prelucrare a acestor categorii speciale de date cu caracter personal, printre altele atunci când persoana vizată îşi dă consimţământul explicit sau în ceea ce priveşte nevoile specifice în special atunci când prelucrarea este efectuată în cadrul unor activităţi legitime de către anumite asociaţii sau fundaţii al căror scop este de a permite exercitarea libertăţilor fundamentale.

(52) Derogarea de la interdicţia privind prelucrarea categoriilor speciale de date cu caracter personal ar trebui să fie permisă, de asemenea, în cazul în care dreptul Uniunii sau dreptul intern prevede acest lucru şi ar trebui să facă obiectul unor garanţii adecvate, astfel încât să fie protejate datele cu caracter personal şi alte drepturi fundamentale, atunci când acest lucru se justifică din motive de interes public, în special în cazul prelucrării datelor cu caracter personal în domeniul legislaţiei privind ocuparea forţei de muncă, protecţia socială, inclusiv pensiile, precum şi în scopuri de securitate, supraveghere şi alertă în materie de sănătate, pentru prevenirea sau controlul bolilor transmisibile şi a altor ameninţări grave la adresa sănătăţii. Această derogare poate fi acordată în scopuri medicale, inclusiv sănătatea publică şi gestionarea serviciilor de asistenţă medicală, în special în vederea asigurării calităţii şi eficienţei din punctul de vedere al costurilor ale procedurilor utilizate pentru soluţionarea cererilor de prestaţii şi servicii în cadrul sistemului de asigurări de sănătate, sau în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice. De asemenea, prelucrarea unor asemenea date cu caracter personal ar trebui permisă, printro derogare, atunci când este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiţie, indiferent dacă are loc în cadrul unei proceduri în faţa unei instanţe sau în cadrul unei proceduri administrative sau a unei proceduri extrajudiciare.

(53) Categoriile speciale de date cu caracter personal care necesită un nivel mai ridicat de protecţie ar trebui prelucrate doar în scopuri legate de sănătate atunci când este necesar pentru realizarea acestor scopuri în beneficiul persoanelor fizice şi al societăţii în general, în special în contextul gestionării serviciilor şi sistemelor de sănătate sau de asistenţă socială, inclusiv prelucrarea acestor date de către autorităţile de management şi de către autorităţile centrale naţionale din domeniul sănătăţii în scopul controlului calităţii, furnizării de informaţii de gestiune şi al supravegherii generale a sistemului de sănătate sau de asistenţă socială la nivel naţional şi local, precum şi în contextul asigurării continuităţii asistenţei medicale sau sociale şi a asistenţei medicale transfrontaliere ori în scopuri de securitate, supraveghere şi alertă în materie de sănătate ori în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice în temeiul dreptului Uniunii sau al dreptului intern, care trebuie să urmărească un obiectiv de interes public, precum şi în cazul studiilor realizate în interes public în domeniul sănătăţii publice. Prin urmare, prezentul regulament ar trebui să prevadă condiţii armonizate pentru prelucrarea categoriilor speciale de date cu caracter personal privind sănătatea, în ceea ce priveşte nevoile specifice, în special atunci când prelucrarea acestor date este efectuată în anumite scopuri legate de sănătate de către persoane care fac obiectul unei obligaţii legale de a păstra secretul profesional. Dreptul Uniunii sau dreptul intern ar trebui să prevadă măsuri specifice şi adecvate pentru a proteja drepturile fundamentale şi datele cu caracter personal ale persoanelor fizice. Statele membre ar

trebui să aibă posibilitatea de a menţine sau de a introduce condiţii suplimentare, inclusiv restricţii, în ceea ce priveşte prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea. Totuşi, acest lucru nu ar trebui să împiedice libera circulaţie a datelor cu caracter personal în cadrul Uniunii atunci când aceste condiţii se aplică prelucrării transfrontaliere a unor astfel de date.

(54) Prelucrarea categoriilor speciale de date cu caracter personal poate fi necesară din motive de interes public în domeniile sănătăţii publice, fără consimţământul persoanei vizate. O astfel de prelucrare ar trebui condiţionată de măsuri adecvate şi specifice destinate să protejeze drepturile şi libertăţile persoanelor fizice. În acest context, conceptul de "sănătate publică" ar trebui interpretat astfel cum este definit în Regulamentul (CE) nr. **1338/2008** al Parlamentului European şi al Consiliului (1) , şi anume toate elementele referitoare la sănătate şi anume starea de sănătate, inclusiv morbiditatea sau handicapul, factorii determinanţi care au efect asupra stării de sănătate, necesităţile în domeniul asistenţei medicale, resursele alocate asistenţei medicale, furnizarea asistenţei medicale şi asigurarea accesului universal la aceasta, precum şi cheltuielile şi sursele de finanţare în domeniul sănătăţii şi cauzele mortalităţii. Această prelucrare a datelor privind sănătatea din motive de interes public nu ar trebui să ducă la prelucrarea acestor date în alte scopuri de către părţi terţe, cum ar fi angajatorii sau societăţile de asigurări şi băncile.

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

(55) În plus, prelucrarea datelor cu caracter personal de către autorităţile publice în vederea realizării obiectivelor prevăzute de dreptul constituţional sau de dreptul internaţional public, ale asociaţiilor religioase recunoscute oficial se efectuează din motive de interes public.

(56) În cazul în care, în cadrul activităţilor electorale, funcţionarea sistemului democratic necesită, într-un stat membru, ca partidele politice să colecteze date cu caracter personal privind opiniile politice ale persoanelor, prelucrarea unor astfel de date poate fi permisă din motive de interes public, cu condiţia să se prevadă garanţiile corespunzătoare.

(57) Dacă datele cu caracter personal prelucrate de un operator nu îi permit acestuia să identifice o persoană fizică, operatorul de date nu ar trebui să aibă obligaţia de a obţine informaţii suplimentare în vederea identificării persoanei vizate, cu unicul scop de a respecta oricare dintre dispoziţiile prezentului regulament. Cu toate acestea, operatorul nu ar trebui să refuze să preia informaţiile suplimentare furnizate de persoana vizată cu scopul de a sprijini exercitarea drepturilor acesteia. Identificarea ar trebui să includă identificarea digitală a unei persoane vizate, de exemplu prin mecanisme de autentificare precum aceleaşi acreditări utilizate de către persoana vizată pentru a accesa serviciile online oferite de operatorul de date.

(58) Principiul transparenţei prevede că orice informaţii care se adresează publicului sau persoanei vizate să fie concise, uşor accesibile şi uşor de înţeles şi să se utilizeze un limbaj simplu şi clar, precum şi vizualizare acolo unde este cazul. Aceste informaţii ar putea fi furnizate în format electronic, de exemplu atunci când sunt adresate publicului, prin intermediul unui site. Acest lucru este important în special în situaţii în care datorită multitudinii actorilor şi a complexităţii, din punct de vedere tehnologic, a practicii, este dificil ca persoana vizată să ştie şi să înţeleagă dacă datele cu caracter personal care o privesc sunt colectate, de către cine şi în ce scop, cum este cazul publicităţii online. Întrucât copii necesită o protecţie specifică, orice informaţii şi orice comunicare, în cazul în care prelucrarea vizează un copil, ar trebui să fie exprimate într-un limbaj simplu şi clar, astfel încât copilul să îl poată înţelege cu uşurinţă.

(59) Ar trebui să fie prevăzute modalităţi de facilitare a exercitării de către persoana vizată a drepturilor care îi sunt conferite prin prezentul regulament, inclusiv mecanismele prin care aceasta poate solicita şi, dacă este cazul, obţine, în mod gratuit, în special, acces la datele cu caracter personal, precum şi rectificarea sau ştergerea acestora, şi exercitarea dreptului la opoziţie. Operatorul ar trebui să ofere, de asemenea, modalităţi de introducere a cererilor pe cale electronică, mai ales în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice. Operatorul ar trebui să aibă obligaţia de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate şi cel târziu în termen de o lună şi, în cazul în care nu intenţionează să se conformeze respectivele cereri, să motiveze acest refuz.

(60) Conform principiilor prelucrării echitabile şi transparente, persoana vizată este informată cu privire la existenţa unei operaţiuni de prelucrare şi la scopurile acesteia. Operatorul ar trebui să furnizeze persoanei vizate orice informaţii suplimentare necesare pentru a asigura o prelucrare echitabilă şi transparentă, ţinând seama de circumstanţele specifice şi de contextul în care sunt prelucrate datele cu caracter personal. În plus, persoana vizată ar trebui informată cu privire la crearea de profiluri, precum şi la consecinţele acesteia. Atunci când datele cu caracter personal sunt colectate de la persoana vizată, aceasta ar trebui informată, de asemenea, dacă are obligaţia de a furniza datele cu caracter personal şi care

sunt consecinţele în cazul unui refuz. Aceste informaţii pot fi furnizate în combinaţie cu pictograme standardizate pentru a oferi într-un mod uşor vizibil, inteligibil şi clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea ar trebui să poată fi citite automat.

(61) Informaţiile în legătură cu prelucrarea datelor cu caracter personal referitoare la persoana vizată ar trebui furnizate acesteia la momentul colectării de la persoana vizată sau, în cazul în care datele cu caracter personal sunt obţinute din altă sursă, într-o perioadă rezonabilă, în funcţie de circumstanţele cazului. În cazul în care datele cu caracter personal pot fi divulgate în mod legitim unui alt destinatar, persoana vizată ar trebui informată atunci când datele cu caracter personal sunt divulgate pentru prima dată destinatarului. În cazul în care operatorul intenţionează să prelucreze datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul ar trebui să furnizeze persoanei vizate, înainte de această prelucrare ulterioară, informaţii privind scopul secundar respectiv şi alte informaţii necesare. În cazul în care originea datelor cu caracter personal nu a putut fi comunicată persoanei vizate din cauză că au fost utilizate surse diverse, informaţiile generale ar trebui furnizate.

(62) Cu toate acestea, nu este necesară impunerea obligaţiei de a furniza informaţii în cazul în care persoana vizată deţine deja informaţiile, în cazul în care înregistrarea sau divulgarea datelor cu caracter personal este prevăzută în mod expres de lege sau în cazul în care informarea persoanei vizate se dovedeşte imposibilă sau ar implica eforturi disproporţionate. Acesta din urmă ar putea fi cazul în special atunci când prelucrarea se efectuează în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice. În această privinţă, ar trebui luate în considerare numărul persoanelor vizate, vechimea datelor şi orice garanţii adecvate adoptate.

(63) O persoană vizată ar trebui să aibă drept de acces la datele cu caracter personal colectate care o privesc şi ar trebui să îşi exercite acest drept cu uşurinţă şi la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare şi pentru a verifica legalitatea acesteia. Acest lucru include dreptul persoanelor vizate de a avea acces la datele lor privind sănătatea, de exemplu datele din registrele lor medicale conţinând informaţii precum diagnostice, rezultate ale examinărilor, evaluări ale medicilor curanţi şi orice tratament sau intervenţie efectuată. Orice persoană vizată ar trebui, prin urmare, să aibă dreptul de a cunoaşte şi de a i se comunica în special scopurile în care sunt prelucrate datele, dacă este posibil perioada pentru care se prelucrează datele cu caracter personal, destinatarii datelor cu caracter personal, logica de prelucrare automată a datelor cu caracter personal şi, cel puţin în cazul în care se bazează pe crearea de profiluri, consecinţele unei astfel de prelucrări. Dacă acest lucru este posibil, operatorul de date ar trebui să poată furniza acces de la distanţă la un sistem sigur, care să ofere persoanei vizate acces direct la datele sale cu caracter personal. Acest drept nu ar trebui să aducă atingere drepturilor sau libertăţilor altora, inclusiv secretului comercial sau proprietăţii intelectuale şi, în special, drepturilor de autor care asigură protecţia programelor software. Cu toate acestea, consideraţiile de mai sus nu ar trebui să aibă drept rezultat refuzul de a furniza toate informaţiile persoanei vizate. Atunci când operatorul prelucrează un volum mare de informaţii privind persoana vizată, operatorul ar trebui să poată solicita ca, înainte de a îi fi furnizate informaţiile, persoana vizată să precizeze informaţiile sau activităţile de prelucrare la care se referă cererea sa.

(64) Operatorul ar trebui să ia toate măsurile rezonabile pentru a verifica identitatea unei persoane vizate care solicită acces la date, în special în contextul serviciilor online şi al identificatorilor online. Un operator nu ar trebui să reţină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacţioneze la cereri potenţiale.

(65) O persoană vizată ar trebui să aibă dreptul la rectificarea datelor cu caracter personal care o privesc şi "dreptul de a fi uitată", în cazul în care păstrarea acestor date încalcă prezentul regulament sau dreptul Uniunii sau dreptul intern sub incidenţa căruia intră operatorul. În special, persoanele vizate ar trebui să aibă dreptul ca datele lor cu caracter personal să fie şterse şi să nu mai fie prelucrate, în cazul în care datele cu caracter personal nu mai sunt necesare pentru scopurile în care sunt colectate sau sunt prelucrate, în cazul în care persoanele vizate şi-au retras consimţământul pentru prelucrare sau în cazul în care acestea se opun prelucrării datelor cu caracter personal care le privesc sau în cazul în care prelucrarea datelor cu caracter personal ale acestora nu este conformă cu prezentul regulament. Acest drept este relevant în special în cazul în care persoana vizată şi-a dat consimţământul când era copil şi nu cunoştea pe deplin riscurile pe care le implică prelucrarea, iar ulterior doreşte să elimine astfel de date cu caracter personal, în special de pe internet. Persoana vizată ar trebui să aibă posibilitatea de a-şi exercita acest drept în pofida faptului că nu mai este copil. Cu toate acestea, păstrarea în continuare a datelor cu caracter personal ar trebui să fie legală în cazul în care este necesară pentru exercitarea dreptului la libertatea de

exprimare şi de informare, pentru respectarea unei obligaţii legale, pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul, din motive de interes public în domeniul sănătăţii publice, în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice sau pentru constatarea, exercitarea sau apărarea unui drept în instanţă.

(66) Pentru a se consolida "dreptul de a fi uitat" în mediul online, dreptul de ştergere ar trebui să fie extins astfel încât un operator care a făcut publice date cu caracter personal ar trebui să aibă obligaţia de a informa operatorii care prelucrează respectivele date cu caracter personal să şteargă orice linkuri către datele respective sau copii sau reproduceri ale acestora. În acest scop, operatorul în cauză ar trebui să ia măsuri rezonabile, ţinând seama de tehnologia disponibilă şi de mijloacele aflate la dispoziţia lui, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal în ceea ce priveşte cererea persoanei vizate.

(67) Metodele de restricţionare a prelucrării de date cu caracter personal ar putea include, printre altele, mutarea temporară a datelor cu caracter personal selectate într-un alt sistem de prelucrare, sau anularea accesului utilizatorilor la datele selectate sau înlăturarea temporară a datelor publicate de pe un site. În ceea ce priveşte sistemele automatizate de evidenţă a datelor, restricţionarea prelucrării ar trebui, în principiu, asigurată prin mijloace tehnice în aşa fel încât datele cu caracter personal să nu facă obiectul unor operaţiuni de prelucrare ulterioară şi să nu mai poată fi schimbate. Faptul că prelucrarea datelor cu caracter personal este restricţionată ar trebui indicat în mod clar în sistem.

(68) Pentru a spori suplimentar controlul asupra propriilor date, persoana vizată ar trebui, în cazul în care datele cu caracter personal sunt prelucrate prin mijloace automate, să poată primi datele cu caracter personal care o privesc şi pe care le-a furnizat unui operator, într-un format structurat, utilizat în mod curent, prelucrabil automat şi interoperabil şi să le poată transmite unui alt operator. Operatorii de date ar trebui să fie încurajaţi să dezvolte formate interoperabile care să permită portabilitatea datelor. Acest drept ar trebui să se aplice în cazul în care persoana vizată a furnizat datele cu caracter personal pe baza propriului consimţământ sau în cazul în care prelucrarea datelor este necesară pentru executarea unui contract. Acest drept nu ar trebui să se aplice în cazul în care prelucrarea se bazează pe un alt temei juridic decât consimţământul sau contractul. Prin însăşi natura sa, acest drept nu ar trebui exercitat împotriva operatorilor care prelucrează date cu caracter personal în cadrul exercitării funcţiilor lor publice. Acesta nu ar trebui să se aplice în special în cazul în care prelucrarea de date cu caracter personal este necesară în vederea respectării unei obligaţii legale căreia îi este supus operatorul sau în cazul îndeplinirii unei sarcini care serveşte unui interes public sau care rezultă din exercitarea unei autorităţi publice cu care este învestit operatorul. Dreptul persoanei vizate de a transmite sau de a primi date cu caracter personal care o privesc nu ar trebui să creeze pentru operatori obligaţia de a adopta sau de a menţine sisteme de prelucrare care să fie compatibile din punct de vedere tehnic. În cazul în care, într-un anumit set de date cu caracter personal, sunt implicate mai multe persoane vizate, dreptul de a primi datele cu caracter personal nu ar trebui să aducă atingere drepturilor şi libertăţilor altor persoane vizate, în conformitate cu prezentul regulament. De asemenea, acest drept nu ar trebui să aducă atingere dreptului persoanei vizate de a obţine ştergerea datelor cu caracter personal şi limitărilor dreptului respectiv, astfel cum sunt prevăzute în prezentul regulament, şi nu ar trebui, în special, să implice ştergerea acelor date cu caracter personal referitoare la persoana vizată care au fost furnizate de către aceasta în vederea executării unui contract, în măsura în care şi atât timp cât datele respective sunt necesare pentru executarea contractului. Persoana vizată ar trebui să aibă dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul, dacă acest lucru este fezabil din punct de vedere tehnic.

(69) În cazurile în care datele cu caracter personal ar putea fi prelucrate în mod legal deoarece prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul sau pe baza intereselor legitime ale unui operator sau ale unei părţi terţe, o persoană vizată ar trebui să aibă totuşi dreptul de a se opune prelucrării oricăror date cu caracter personal care se referă la situaţia sa particulară. Ar trebui să revină operatorului sarcina de a demonstra că interesele sale legitime şi imperioase prevalează asupra intereselor sau a drepturilor şi libertăţilor fundamentale ale persoanei vizate.

(70) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de marketing direct, persoana vizată ar trebui să aibă dreptul de a se opune unei astfel de prelucrări, inclusiv creării de profiluri în măsura în care aceasta are legătură cu marketingul direct, indiferent dacă prelucrarea în cauză este cea iniţială sau una ulterioară, în orice moment şi în mod gratuit. Acest drept ar trebui adus în mod explicit în atenţia persoanei vizate şi prezentat în mod clar şi separat de orice alte informaţii.

(71) Persoana vizată ar trebui să aibă dreptul de a nu face obiectul unei decizii, care poate include o măsură, care evaluează aspecte personale referitoare la persoana vizată, care se bazează exclusiv pe prelucrarea automată şi care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă, cum ar fi refuzul automat al unei cereri de credit online sau practicile de recrutare pe cale electronică, fără intervenţie umană. O astfel de prelucrare include "crearea de profiluri", care constă în orice formă de prelucrare automată a datelor cu caracter personal prin evaluarea aspectelor personale referitoare la o persoană fizică, în special în vederea analizării sau preconizării anumitor aspecte privind randamentul la locul de muncă al persoanei vizate, situaţia economică, starea de sănătate, preferinţele sau interesele personale, fiabilitatea sau comportamentul, locaţia sau deplasările, atunci când aceasta produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă. Cu toate acestea, luarea de decizii pe baza unei astfel de prelucrări, inclusiv crearea de profiluri, ar trebui permisă în cazul în care este autorizată în mod expres în dreptul Uniunii sau în dreptul intern care se aplică operatorului, inclusiv în scopul monitorizării şi prevenirii fraudei şi a evaziunii fiscale, desfăşurate în conformitate cu reglementările, standardele şi recomandările instituţiilor Uniunii sau ale organismelor naţionale de supraveghere, şi în scopul asigurării securităţii şi fiabilităţii unui serviciu oferit de operator sau în cazul în care este necesară pentru încheierea sau executarea unui contract între persoana vizată şi un operator sau în cazul în care persoana vizată şi-a dat în mod explicit consimţământul. În orice caz, o astfel de prelucrare ar trebui să facă obiectul unor garanţii corespunzătoare, care ar trebui să includă o informare specifică a persoanei vizate şi dreptul acesteia de a obţine intervenţie umană, de aşi exprima punctul de vedere, de a primi o explicaţie privind decizia luată în urma unei astfel de evaluări, precum şi dreptul de a contesta decizia. O astfel de măsură nu ar trebui să se refere la un copil. Pentru a asigura o prelucrare echitabilă şi transparentă în ceea ce priveşte persoana vizată, având în vedere circumstanţele specifice şi contextul în care sunt prelucrate datele cu caracter personal, operatorul ar trebui să utilizeze proceduri matematice sau statistice adecvate pentru crearea de profiluri, să implementeze măsuri tehnice şi organizatorice adecvate pentru a asigura în special faptul că factorii care duc la inexactităţi ale datelor cu caracter personal sunt corectaţi şi că riscul de erori este redus la minimum, precum şi să securizeze datele cu caracter personal într-un mod care să ţină seama de pericolele potenţiale la adresa intereselor şi drepturilor persoanei vizate şi care să prevină, printre altele, efectele discriminatorii împotriva persoanelor pe motiv de rasă sau origine etnică, opinii politice, religie sau convingeri, apartenenţă sindicală, caracteristici genetice, stare de sănătate sau orientare sexuală sau care să ducă la măsuri care să aibă astfel de efecte. Procesul decizional automatizat şi crearea de profiluri pe baza unor categorii speciale de date cu caracter personal ar trebui permise numai în condiţii specifice.

(72) Crearea de profiluri este supusă normelor prezentului regulament care reglementează prelucrarea datelor cu caracter personal, precum temeiurile juridice ale prelucrării sau principiile de protecţie a datelor. Comitetul european pentru protecţia datelor instituit prin prezentul regulament ("comitetul") ar trebui să poată emite orientări în acest context.

(73) Dreptul Uniunii sau dreptul intern poate impune restricţii în privinţa unor principii specifice, în privinţa dreptului de informare, a dreptului de acces la datele cu caracter personal şi de rectificare sau ştergere a acestora, în privinţa dreptului la portabilitatea datelor, a dreptului la opoziţie, a deciziilor bazate pe crearea de profiluri, precum şi în privinţa comunicării unei încălcări a securităţii datelor cu caracter personal persoanei vizate şi a anumitor obligaţii conexe ale operatorilor, în măsura în care acest lucru este necesar şi proporţional într-o societate democratică pentru a se garanta siguranţa publică, inclusiv protecţia vieţii oamenilor, în special ca răspuns la dezastre naturale sau provocate de om, prevenirea, investigarea şi urmărirea penală a infracţiunilor sau executarea pedepselor, inclusiv protejarea împotriva ameninţărilor la adresa siguranţei publice sau împotriva încălcării eticii în cazul profesiilor reglementate şi prevenirea acestora, alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, menţinerea de registre publice din motive de interes public general, prelucrarea ulterioară a datelor cu caracter personal arhivate pentru a transmite informaţii specifice legate de comportamentul politic în perioada regimurilor fostelor state totalitare, protecţia persoanei vizate sau a drepturilor şi libertăţilor unor terţi, inclusiv protecţia socială, sănătatea publică şi scopurile umanitare. Aceste restricţii ar trebui să fie conforme cu cerinţele prevăzute de **cartă** şi de **Convenţia europeană pentru apărarea drepturilor omului şi a libertăţilor fundamentale**.

(74) Ar trebui să se stabilească responsabilitatea şi răspunderea operatorului pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său. În special, operatorul ar trebui să fie obligat să implementeze măsuri adecvate şi eficace şi să fie în măsură să demonstreze conformitatea

activităţilor de prelucrare cu prezentul regulament, inclusiv eficacitatea măsurilor. Aceste măsuri ar trebui să ţină seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscul pentru drepturile şi libertăţile persoanelor fizice.

(75) Riscul pentru drepturile şi libertăţile persoanelor fizice, prezentând grade diferite de probabilitate de materializare şi de gravitate, poate fi rezultatul unei prelucrări a datelor cu caracter personal care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care: prelucrarea poate conduce la discriminare, furt sau fraudă a identităţii, pierdere financiară, compromiterea reputaţiei, pierderea confidenţialităţii datelor cu caracter personal protejate prin secret profesional, inversarea neautorizată a pseudonimizării sau la orice alt dezavantaj semnificativ de natură economică sau socială; persoanele vizate ar putea fi private de drepturile şi libertăţile lor sau împiedicate să-şi exercite controlul asupra datelor lor cu caracter personal; datele cu caracter personal prelucrate sunt date care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenenţa sindicală; sunt prelucrate date genetice, date privind sănătatea sau date privind viaţa sexuală sau privind condamnările penale şi infracţiunile sau măsurile de securitate conexe; sunt evaluate aspecte de natură personală, în special analizarea sau previzionarea unor aspecte privind randamentul la locul de muncă, situaţia economică, starea de sănătate, preferinţele sau interesele personale, fiabilitatea sau comportamentul, locaţia sau deplasările, în scopul de a se crea sau de a se utiliza profiluri personale; sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale unor copii; sau prelucrarea implică un volum mare de date cu caracter personal şi afectează un număr larg de persoane vizate.

(76) Probabilitatea de a se materializa şi gravitatea riscului pentru drepturile şi libertăţile persoanei vizate ar trebui să fie determinate în funcţie de natura, domeniul de aplicare, contextul şi scopurile prelucrării datelor cu caracter personal. Riscul ar trebui apreciat pe baza unei evaluări obiective prin care se stabileşte dacă operaţiunile de prelucrare a datelor prezintă un risc sau un risc ridicat.

(77) Orientări pentru implementarea unor măsuri adecvate şi pentru demonstrarea conformităţii de către operator sau persoana împuternicită de operator, mai ales în ceea ce priveşte identificarea riscului legat de prelucrare, evaluarea acestuia din punctul de vedere al originii, naturii, probabilităţii de a se materializa şi al gravităţii, precum şi identificarea bunelor practici pentru atenuarea riscului ar putea fi oferite în special prin coduri de conduită aprobate, certificări aprobate, orientări ale comitetului sau prin indicaţii furnizate de un responsabil cu protecţia datelor. Comitetul poate, de asemenea, să emită orientări cu privire la operaţiunile de prelucrare care sunt considerate puţin susceptibile de a genera un risc ridicat pentru drepturile şi libertăţile persoanelor fizice şi să indice măsurile care se pot dovedi suficiente în asemenea cazuri pentru a aborda un astfel de risc.

(78) Protecţia drepturilor şi libertăţilor persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice şi organizatorice corespunzătoare pentru a se asigura îndeplinirea cerinţelor din prezentul regulament. Pentru a fi în măsură să demonstreze conformitatea cu prezentul regulament, operatorul ar trebui să adopte politici interne şi să pună în aplicare măsuri care să respecte în special principiul protecţiei datelor începând cu momentul conceperii şi cel al protecţiei implicite a datelor. Astfel de măsuri ar putea consta, printre altele, în reducerea la minimum a prelucrării datelor cu caracter personal, pseudonimizarea acestor date cât mai curând posibil, transparenţa în ceea ce priveşte funcţiile şi prelucrarea datelor cu caracter personal, abilitarea persoanei vizate să monitorizeze prelucrarea datelor, abilitarea operatorului să creeze elemente de siguranţă şi să le îmbunătăţească. Atunci când elaborează, proiectează, selectează şi utilizează aplicaţii, servicii şi produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează date cu caracter personal pentru a-şi îndeplini rolul, producătorii acestor produse şi furnizorii acestor servicii şi aplicaţii ar trebui să fie încurajaţi să aibă în vedere dreptul la protecţia datelor la momentul elaborării şi proiectării unor astfel de produse, servicii şi aplicaţii şi, ţinând cont de stadiul actual al dezvoltării, să se asigure că operatorii şi persoanele împuternicite de operatori sunt în măsură să îşi îndeplinească obligaţiile referitoare la protecţia datelor. Principiul protecţiei datelor începând cu momentul conceperii şi cel al protecţiei implicite a datelor ar trebui să fie luate în considerare şi în contextul licitaţiilor publice.

(79) Protecţia drepturilor şi libertăţilor persoanelor vizate, precum şi responsabilitatea şi răspunderea operatorilor şi a persoanelor împuternicite de operator, inclusiv în ceea ce priveşte monitorizarea de către autorităţile de supraveghere şi măsurile adoptate de acestea, necesită o atribuire clară a responsabilităţilor în temeiul prezentului regulament, inclusiv în cazul în care un operator stabileşte scopurile şi mijloacele prelucrării împreună cu alţi operatori sau în cazul în care o operaţiune de prelucrare este efectuată în numele unui operator.

(80) Atunci când un operator sau o persoană împuternicită de operator care nu este stabilită în Uniune prelucrează date cu caracter personal ale unor persoane vizate care se află pe teritoriul Uniunii, iar activităţile sale de prelucrare au legătură cu oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăţi de către persoana vizată, sau cu monitorizarea comportamentului unor persoane vizate dacă acesta se manifestă în cadrul Uniunii, operatorul sau persoana împuternicită de operator ar trebui să desemneze un reprezentant, cu excepţia cazului în care prelucrarea are caracter ocazional, nu include prelucrarea pe scară largă a unor categorii speciale de date cu caracter personal şi nici prelucrarea de date referitoare la condamnări penale şi la infracţiuni, şi este puţin susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice, având în vedere natura, contextul, domeniul de aplicare şi scopurile prelucrării, precum şi a cazului în care operatorul este o autoritate publică sau un organism public. Reprezentantul ar trebui să acţioneze în numele operatorului sau al persoanei împuternicite de operator, putând fi contactat de orice autoritate de supraveghere. Reprezentantul ar trebui desemnat în mod explicit, printr-un mandat scris al operatorului sau al persoanei împuternicite de operator, să acţioneze în numele acestuia (acesteia) în ceea ce priveşte obligaţiile lor în temeiul prezentului regulament. Desemnarea unui astfel de reprezentant nu aduce atingere responsabilităţii sau răspunderii operatorului sau a persoanei împuternicite de operator în temeiul prezentului regulament. Un astfel de reprezentant ar trebui să îşi îndeplinească sarcinile în conformitate cu mandatul primit de la operator sau de la persoana împuternicită de operator, inclusiv să coopereze cu autorităţile de supraveghere competente în ceea ce priveşte orice acţiune întreprinsă pentru a asigura respectarea prezentului regulament. Reprezentantul desemnat ar trebui să fie supus unor proceduri de asigurare a respectării legii în cazul nerespectării prezentului regulament de către operator sau de către persoana împuternicită de operator.

(81) Pentru a asigura respectarea cerinţelor impuse de prezentul regulament în ceea ce priveşte prelucrarea care trebuie efectuată în numele operatorului de către persoana împuternicită de operator, atunci când atribuie activităţi de prelucrare unei persoane împuternicite de operator, acesta din urmă ar trebui să utilizeze numai persoane împuternicite care oferă garanţii suficiente, în special în ceea ce priveşte cunoştinţele de specialitate, fiabilitatea şi resursele, pentru a implementa măsuri tehnice şi organizatorice care îndeplinesc cerinţele impuse de prezentul regulament, inclusiv pentru securitatea prelucrării. Aderarea de către persoana împuternicită de operator la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate fi utilizată drept element care să demonstreze respectarea obligaţiilor de către operator. Efectuarea prelucrării de către o persoană împuternicită de un operator ar trebui să fie reglementată printr-un contract sau un alt tip de act juridic, în temeiul dreptului Uniunii sau al dreptului intern, care creează obligaţii pentru persoana împuternicită de operator în raport cu operatorul şi care stabileşte obiectul şi durata prelucrării, natura şi scopurile prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate, şi ar trebui să ţină seama de sarcinile şi responsabilităţile specifice ale persoanei împuternicite de operator în contextul prelucrării care trebuie efectuată, precum şi de riscul pentru drepturile şi libertăţile persoanei vizate. Operatorul şi persoana împuternicită de operator pot alege să utilizeze un contract individual sau clauze contractuale standard care sunt adoptate fie direct de Comisie, fie de o autoritate de supraveghere în conformitate cu mecanismul de asigurare a coerenţei şi apoi adoptate de Comisie. După finalizarea prelucrării în numele operatorului, persoana împuternicită de operator ar trebui să returneze sau să şteargă, în funcţie de opţiunea operatorului, datele cu caracter personal, cu excepţia cazului în care există o cerinţă de stocare a datelor cu caracter personal în temeiul dreptului Uniunii sau al dreptului intern care instituie obligaţii pentru persoana împuternicită de operator.

(82) În vederea demonstrării conformităţii cu prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să păstreze evidenţe ale activităţilor de prelucrare aflate în responsabilitatea sa. Fiecare operator şi fiecare persoană împuternicită de operator ar trebui să aibă obligaţia de a coopera cu autoritatea de supraveghere şi de a pune la dispoziţia acesteia, la cerere, aceste evidenţe, pentru a putea fi utilizate în scopul monitorizării operaţiunilor de prelucrare respective.

(83) În vederea menţinerii securităţii şi a prevenirii prelucrărilor care încalcă prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să evalueze riscurile inerente prelucrării şi să implementeze măsuri pentru atenuarea acestor riscuri, cum ar fi criptarea. Măsurile respective ar trebui să asigure un nivel corespunzător de securitate, inclusiv confidenţialitatea, luând în considerare stadiul actual al dezvoltării şi costurile implementării în raport cu riscurile şi cu natura datelor cu caracter personal a căror protecţie trebuie asigurată. La evaluarea riscului pentru securitatea datelor cu caracter personal, ar trebui să se acorde atenţie riscurilor pe care le prezintă prelucrarea datelor, cum ar fi distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter

personal transmise, stocate sau prelucrate în alt mod, în mod accidental sau ilegal, care pot duce în special la prejudicii fizice, materiale sau morale.

(84) Pentru a favoriza respectarea dispoziţiilor prezentului regulament în cazurile în care operaţiunile de prelucrare sunt susceptibile să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul ar trebui să fie responsabil de efectuarea unei evaluări a impactului asupra protecţiei datelor, care să estimeze, în special, originea, natura, specificitatea şi gravitatea acestui risc. Rezultatul evaluării ar trebui luat în considerare la stabilirea măsurilor adecvate care trebuie luate pentru a demonstra că prelucrarea datelor cu caracter personal respectă prezentul regulament. În cazul în care o evaluare a impactului asupra protecţiei datelor arată că operaţiunile de prelucrare implică un risc ridicat, pe care operatorul nu îl poate atenua prin măsuri adecvate sub aspectul tehnologiei disponibile şi al costurilor implementării, ar trebui să aibă loc o consultare a autorităţii de supraveghere înainte de prelucrare.

(85) Dacă nu este soluţionată la timp şi într-un mod adecvat, o încălcare a securităţii datelor cu caracter personal poate conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputaţiei, pierderea confidenţialităţii datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză. Prin urmare, de îndată ce a luat cunoştinţă de producerea unei încălcări a securităţii datelor cu caracter personal, operatorul ar trebui să notifice această încălcare autorităţii de supraveghere, fără întârziere nejustificată şi, dacă este posibil, în cel mult 72 de ore după ce a luat la cunoştinţă de existenţa acesteia, cu excepţia cazului în care operatorul este în măsură să demonstreze, în conformitate cu principiul responsabilităţii, că încălcarea securităţii datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice. Atunci când notificarea nu se poate realiza în termen de 72 de ore, aceasta ar trebui să cuprindă motivele întârzierii, iar informaţiile pot fi furnizate treptat, fără altă întârziere.

(86) Operatorul ar trebui să comunice persoanei vizate o încălcare a securităţii datelor cu caracter personal, fără întârzieri nejustificate, atunci când încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanei fizice, pentru a-i permite să ia măsurile de precauţie necesare. Comunicarea ar trebui să descrie natura încălcării securităţii datelor cu caracter personal şi să cuprindă recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative. Comunicările către persoanele vizate ar trebui efectuate în cel mai scurt timp posibil în mod rezonabil şi în strânsă cooperare cu autoritatea de supraveghere, respectându-se orientările furnizate de aceasta sau de alte autorităţi competente, cum ar fi autorităţile de aplicare a legii. De exemplu, necesitatea de a atenua un

risc imediat de producere a unui prejudiciu ar presupune comunicarea cu promptitudine către persoanele vizate, în timp ce necesitatea de a implementa măsuri corespunzătoare împotriva încălcării în continuare a securităţii datelor cu caracter personal sau împotriva unor încălcări similare ale securităţii datelor cu caracter personal ar putea justifica un termen mai îndelungat pentru comunicare.

(87) Ar trebui să se stabilească dacă au fost implementate toate măsurile tehnologice de protecţie şi organizatorice corespunzătoare în scopul de a se stabili imediat dacă s-a produs o încălcare a securităţii datelor cu caracter personal şi de a se informa cu promptitudine autoritatea de supraveghere şi persoana vizată. Faptul că notificarea a fost efectuată fără întârziere nejustificată ar trebui stabilit luându-se în considerare, în special, natura şi gravitatea încălcării securităţii datelor cu caracter personal, precum şi consecinţele şi efectele negative ale acesteia asupra persoanei vizate. Această notificare poate conduce la o intervenţie a autorităţii de supraveghere, în conformitate cu sarcinile şi competenţele specificate în prezentul regulament.

(88) La stabilirea de norme detaliate privind formatul şi procedurile aplicabile notificării referitoare la încălcările securităţii datelor cu caracter personal, ar trebui să se acorde atenţia cuvenită circumstanţelor în care a avut loc încălcarea, stabilindu-se inclusiv dacă protecţia datelor cu caracter personal a fost sau nu a fost asigurată prin măsuri tehnice de protecţie corespunzătoare, care să limiteze efectiv probabilitatea fraudării identităţii sau a altor forme de utilizare abuzivă. În plus, astfel de norme şi proceduri ar trebui să ţină cont de interesele legitime ale autorităţilor de aplicare a legii în cazurile în care divulgarea timpurie ar putea îngreuna în mod inutil investigarea circumstanţelor în care a avut loc o încălcare a datelor cu caracter personal.

(89) Directiva **95/46/CE** a prevăzut o obligaţie generală de a notifica prelucrarea datelor cu caracter personal autorităţilor de supraveghere. Cu toate că obligaţia respectivă generează sarcini administrative şi

financiare, aceasta nu a contribuit întotdeauna la îmbunătăţirea protecţiei datelor cu caracter personal. Prin urmare, astfel de obligaţii de notificare generală nediferenţiată ar trebui să fie abrogate şi înlocuite cu proceduri şi mecanisme eficace care să pună accentul, în schimb, pe acele tipuri de operaţiuni de prelucrare susceptibile să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice prin însăşi natura lor, prin domeniul lor de aplicare, prin contextul şi prin scopurile lor. Astfel de tipuri de operaţiuni de prelucrare pot fi cele care presupun, în special, utilizarea unor noi tehnologii sau care reprezintă un nou tip de operaţiuni, pentru care nicio evaluare a impactului asupra protecţiei datelor nu a fost efectuată anterior de către operator ori care devin necesare dată fiind perioada de timp care s-a scurs de la prelucrarea iniţială.

(90) În astfel de cazuri, operatorul ar trebui să efectueze, înainte de prelucrare, o evaluare a impactului asupra protecţiei datelor, în scopul evaluării gradului specific de probabilitate a materializării riscului ridicat şi gravitatea acestuia, având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi sursele riscului. Respectiva evaluare a impactului ar trebui să includă, în special, măsurile, garanţiile şi mecanismele avute în vedere pentru atenuarea riscului respectiv, pentru asigurarea protecţiei datelor cu caracter personal şi pentru demonstrarea conformităţii cu prezentul regulament.

(91) Aceasta ar trebui să se aplice, în special, operaţiunilor de prelucrare la scară largă, care au drept obiectiv prelucrarea unui volum considerabil de date cu caracter personal la nivel regional, naţional sau supranaţional, care ar putea afecta un număr mare de persoane vizate şi care sunt susceptibile de a genera un risc ridicat, de exemplu, din cauza sensibilităţii lor, în cazul în care, în conformitate cu nivelul atins al cunoştinţelor tehnologice, se foloseşte la scară largă o tehnologie nouă, precum şi altor operaţiuni de prelucrare care generează un risc ridicat pentru drepturile şi libertăţile persoanelor vizate, în special în cazul în care operaţiunile respective limitează capacitatea persoanelor vizate de a-şi exercita drepturile. Ar trebui efectuată o evaluare a impactului asupra protecţiei datelor şi în situaţiile în care datele cu caracter personal sunt prelucrate în scopul luării de decizii care vizează anumite persoane fizice în urma unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, pe baza creării de profiluri pentru datele respective, sau în urma prelucrării unor categorii speciale de date cu caracter personal, a unor date biometrice sau a unor date privind condamnările penale şi infracţiunile sau măsurile de securitate conexe. Este la fel de necesară o evaluare a impactului asupra protecţiei datelor pentru monitorizarea la scară largă a zonelor accesibile publicului, mai ales în cazul utilizării dispozitivelor optoelectronice sau pentru orice alte operaţiuni în cazul în care autoritatea de supraveghere competentă consideră că prelucrarea este susceptibilă de a genera un risc ridicat pentru drepturile şi libertăţile persoanelor vizate, în special deoarece acestea împiedică persoanele vizate să exercite un drept sau să utilizeze un serviciu ori un contract, sau deoarece acestea sunt efectuate în mod sistematic la scară largă. Prelucrarea datelor cu caracter personal nu ar trebui considerată a fi la scară largă în cazul în care prelucrarea se referă la date cu caracter personal de la pacienţi sau clienţi de către un anumit medic, un alt profesionist în domeniul sănătăţii sau un avocat. În aceste cazuri, o evaluare a impactului asupra protecţiei datelor nu ar trebui să fie obligatorie.

(92) În unele circumstanţe ar putea fi rezonabil şi util din punct de vedere economic ca o evaluare a impactului asupra protecţiei datelor să aibă o perspectivă mai extinsă decât cea a unui singur proiect, de exemplu în cazul în care autorităţi sau organisme publice intenţionează să instituie o aplicaţie sau o platformă de prelucrare comună sau în cazul în care mai mulţi operatori preconizează să introducă o aplicaţie comună sau un mediu de prelucrare comun în cadrul unui sector sau segment industrial sau pentru o activitate orizontală utilizată la scară largă.

(93) În contextul adoptării legislaţiei naţionale pe care se bazează îndeplinirea sarcinilor autorităţii publice sau ale organismului public şi care reglementează operaţiunea sau seria de operaţiuni de prelucrare în cauză, statele membre pot considera că este necesară efectuarea unei astfel de evaluări înaintea desfăşurării activităţilor de prelucrare.

(94) În cazul în care o evaluare a impactului asupra protecţiei datelor arată că prelucrarea ar genera, în absenţa garanţiilor, măsurilor de securitate şi mecanismelor de atenuare a riscului, un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile şi al costurilor implementării, autoritatea de supraveghere ar trebui să fie consultată înainte de începerea activităţilor de prelucrare. Un astfel de risc ridicat este susceptibil să fie generat de anumite tipuri de prelucrare, precum şi de amploarea şi frecvenţa prelucrării, care pot duce şi la producerea unor prejudicii sau pot atinge drepturile şi libertăţile persoanelor fizice. Autoritatea de supraveghere ar trebui să răspundă cererii de consultare într-un anumit termen. Cu toate acestea, lipsa unei reacţii din partea autorităţii de supraveghere în termenul respectiv ar

trebui să nu aducă atingere niciunei intervenţii a autorităţii de supraveghere în conformitate cu sarcinile şi competenţele sale prevăzute în prezentul regulament, inclusiv competenţa de a interzice operaţiuni de prelucrare. Ca parte a acestui proces de consultare, rezultatul unei evaluări a impactului asupra protecţiei datelor efectuate cu privire la prelucrarea în cauză poate fi transmis autorităţii de supraveghere, în special măsurile avute în vedere pentru a atenua riscul pentru drepturile şi libertăţile persoanelor fizice.

(95) Persoana împuternicită de operator ar trebui să acorde asistenţă operatorului, dacă este necesar şi la cerere, la asigurarea respectării obligaţiilor care decurg din realizarea de evaluări ale impactului asupra protecţiei datelor şi din consultarea prealabilă a autorităţii de supraveghere.

(96) În timpul elaborării unei măsuri legislative sau de reglementare care prevede prelucrarea unor date cu caracter personal ar trebui, de asemenea, să aibă loc o consultare a autorităţii de supraveghere, pentru a garanta conformitatea prelucrării avute în vedere cu prezentul regulament şi, în special, pentru a atenua riscul la care este expusă persoana vizată.

(97) În cazul în care prelucrarea este efectuată de o autoritate publică, cu excepţia instanţelor sau a autorităţilor judiciare independente atunci când acţionează în calitatea lor judiciară, în cazul în care, în sectorul privat, prelucrarea este efectuată de un operator a cărui activitate principală constă în operaţiuni de prelucrare care necesită o monitorizare regulată şi sistematică a persoanelor vizate pe scară largă, sau în cazul în care activitatea principală a operatorului sau a persoanei împuternicite de operator constă în prelucrarea pe scară largă de categorii speciale de date cu caracter personal şi de date privind condamnările penale şi infracţiunile, o persoană care deţine cunoştinţe de specialitate în materie de legislaţie şi practici privind protecţia datelor ar trebui să acorde asistenţă operatorului sau persoanei împuternicite de operator pentru monitorizarea conformităţii, la nivel intern, cu prezentul regulament. În sectorul privat, activităţile principale ale unui operator se referă la activităţile sale de bază, şi nu la prelucrarea datelor cu caracter personal drept activităţi auxiliare. Nivelul necesar al cunoştinţelor de specialitate ar trebui să fie stabilit în special în funcţie de operaţiunile de prelucrare a datelor efectuate şi de nivelul de protecţie impus pentru datele cu caracter personal prelucrate de operator sau de persoana împuternicită de operator. Aceşti responsabili cu protecţia datelor, indiferent dacă sunt sau nu angajaţi ai operatorului, ar trebui să fie în măsură să îşi îndeplinească atribuţiile şi sarcinile în mod independent.

(98) Asociaţiile sau alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori ar trebui încurajate să elaboreze coduri de conduită, în limitele prezentului regulament, astfel încât să se faciliteze aplicarea efectivă a prezentului regulament, luându-se în considerare caracteristicile specifice ale prelucrării efectuate în anumite sectoare şi necesităţile specifice ale microîntreprinderilor şi ale întreprinderilor mici şi mijlocii. În special, astfel de coduri de conduită ar putea să ajusteze obligaţiile operatorilor şi ale persoanelor împuternicite de operatori, ţinând seama de riscul aferent prelucrării care este susceptibil de a fi generat pentru drepturile şi libertăţile persoanelor fizice.

(99) Atunci când elaborează un cod de conduită sau când modifică sau extind un astfel de cod, asociaţiile şi alte organisme care reprezintă categorii de operatori sau persoane împuternicite de operatori ar trebui să consulte părţile implicate relevante, inclusiv persoanele vizate, dacă este fezabil, şi să ia în considerare contribuţiile transmise şi opiniile exprimate în cadrul unor astfel de consultări.

(100) Pentru a se îmbunătăţi transparenţa şi conformitatea cu prezentul regulament, ar trebui să se încurajeze instituirea de mecanisme de certificare, precum şi de sigilii şi mărci în materie de protecţie a datelor, care să permită persoanelor vizate să evalueze rapid nivelul de protecţie a datelor aferent produselor şi serviciilor relevante.

(101) Fluxurile de date cu caracter personal către şi dinspre ţări situate în afara Uniunii şi organizaţii internaţionale sunt necesare pentru dezvoltarea comerţului internaţional şi a cooperării internaţionale. Creşterea acestor fluxuri a generat noi provocări şi preocupări cu privire la protecţia datelor cu caracter personal. Cu toate acestea, în cazul în care se transferă date cu caracter personal din Uniune către operatori, persoane împuternicite de operatori sau alţi destinatari din ţări terţe sau organizaţii internaţionale, nivelul de protecţie a persoanelor fizice asigurat în Uniune prin prezentul regulament nu ar trebui să fie diminuat, inclusiv în cazurile de transferuri ulterioare de date cu caracter personal dinspre ţara terţă sau organizaţia internaţională către operatori, persoane împuternicite de operatori din aceeaşi sau dintr-o altă ţară terţă sau organizaţie internaţională. În orice caz, transferurile către ţări terţe şi organizaţii internaţionale pot fi desfăşurate numai în conformitate deplină cu prezentul regulament. Un transfer ar putea avea loc numai dacă, sub rezerva respectării celorlalte dispoziţii ale prezentului regulament, operatorul sau persoana împuternicită de operator îndeplineşte condiţiile prevăzute de

dispoziţiile prezentului regulament privind transferul de date cu caracter personal către ţări terţe sau organizaţii internaţionale.

(102) Prezentul regulament nu aduce atingere acordurilor internaţionale încheiate între Uniune şi ţări terţe în vederea reglementării transferului de date cu caracter personal, inclusiv garanţii adecvate pentru persoanele vizate. Statele membre pot încheia acorduri internaţionale care implică transferul de date cu caracter personal către ţări terţe sau organizaţii internaţionale, în măsura în care astfel de acorduri nu afectează prezentul regulament şi nici alte dispoziţii din dreptul Uniunii şi includ un nivel corespunzător de protecţie a drepturilor fundamentale ale persoanelor vizate.

(103) Comisia poate decide, cu efect în întreaga Uniune, că o ţară terţă, un teritoriu sau un anumit sector dintr-o ţară terţă sau o organizaţie internaţională oferă un nivel adecvat de protecţie a datelor, asigurând astfel securitate juridică şi uniformitate în Uniune în ceea ce priveşte ţara terţă sau organizaţia internaţională care este considerată a furniza un astfel de nivel de protecţie. În aceste cazuri, transferurile de date cu caracter personal către ţara terţă sau organizaţia internaţională respectivă pot avea loc fără a fi necesar să se obţină autorizări suplimentare. De asemenea, Comisia poate să decidă, după trimiterea unei notificări şi a unei justificări complete ţării terţe sau organizaţiei internaţionale, să anuleze o astfel de decizie.

(104) În conformitate cu valorile fundamentale pe care se întemeiază Uniunea, în special protecţia drepturilor omului, Comisia ar trebui, în evaluarea sa referitoare la ţara terţă sau la un teritoriu sau la un sector specificat dintr-o ţară terţă, să ia în considerare modul în care aceasta respectă statul de drept, accesul la justiţie, precum şi normele şi standardele internaţionale în materie de drepturi ale omului şi legislaţia sa generală şi sectorială, inclusiv legislaţia privind securitatea publică, apărarea şi securitatea naţională, precum şi ordinea publică şi dreptul penal. Adoptarea unei decizii privind caracterul adecvat al nivelului de protecţie pentru un teritoriu sau un sector specificat dintr-o ţară terţă ar trebui să ţină seama de criterii clare şi obiective, cum ar fi activităţile specifice de prelucrare şi domeniul de aplicare al standardelor legale aplicabile şi legislaţia în vigoare în ţara terţă respectivă. Ţara terţă ar trebui să ofere garanţii care să asigure un nivel adecvat de protecţie, echivalent în esenţă cu cel asigurat în cadrul Uniunii, în special atunci când datele cu caracter personal sunt prelucrate în unul sau mai multe sectoare specifice. În special, ţara terţă ar trebui să asigure o supraveghere efectivă independentă în materie de protecţie a datelor şi să prevadă mecanisme de cooperare cu autorităţile statelor membre de protecţie a datelor, iar persoanele vizate ar trebui să beneficieze de drepturi efective şi opozabile şi de reparaţii efective pe cale administrativă şi judiciară.

(105) Pe lângă angajamentele internaţionale asumate de ţara terţă sau de organizaţia internaţională, Comisia ar trebui să ţină seama de obligaţiile care decurg din participarea ţării terţe sau a organizaţiei internaţionale la sistemele multilaterale sau regionale, în special în ceea ce priveşte protecţia datelor cu caracter personal, precum şi de punerea în aplicare a unor astfel de obligaţii. În special, ar trebui să fie luată în considerare aderarea ţării terţe la **Convenţia Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter** personal şi **protocolul adiţional** la aceasta. Comisia ar trebui să consulte comitetul atunci când evaluează nivelul de protecţie din ţările terţe sau din organizaţiile internaţionale.

(106) Comisia ar trebui să monitorizeze funcţionarea deciziilor privind nivelul de protecţie dintr-o ţară terţă sau un teritoriu sau un anumit sector dintr-o ţară terţă sau dintr-o organizaţie internaţională şi să monitorizeze funcţionarea deciziilor adoptate în temeiul articolului 25 alineatul (6) sau al articolului 26 alineatul (4) din Directiva **95/46/CE**. În deciziile sale privind caracterul adecvat al nivelului de protecţie, Comisia ar trebui să prevadă un mecanism de revizuire periodică a modului lor de funcţionare. Această revizuire periodică ar trebui să fie efectuată în consultare cu ţara terţă sau organizaţia internaţională în cauză şi ar trebui să ia în considerare toate evoluţiile relevante din ţara terţă sau organizaţia internaţională. În scopul monitorizării şi al efectuării revizuirilor periodice, Comisia ar trebui să ia în considerare opiniile şi constatările Parlamentului European şi ale Consiliului, precum şi ale altor organisme şi surse relevante. Comisia ar trebui să evalueze, într-un termen rezonabil, funcţionarea deciziilor din urmă şi să raporteze toate constatările relevante comitetului, în sensul Regulamentului (UE) nr. **182/2011** al Parlamentului European şi al Consiliului (1) , după cum s-a stabilit în temeiul prezentului regulament, Parlamentului European şi Consiliului.

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

(107) Comisia poate să recunoască faptul că o ţară terţă,un teritoriu sau un sector specificat dintr-o ţară terţă sau o organizaţie internaţională nu mai asigură un nivel adecvat de protecţie a datelor. În consecinţă, transferul de date cu caracter personal către ţara terţă sau organizaţia internaţională respectivă ar trebui să fie interzis, cu excepţia cazului în care sunt îndeplinite cerinţele prevăzute în prezentul regulament privind transferurile în baza unor garanţii adecvate, inclusiv regulile corporatiste obligatorii şi derogările de la situaţiile specifice. În acest caz, ar trebui să se prevadă dispoziţii pentru consultări între Comisie şi astfel de ţări terţe sau organizaţii internaţionale. Comisia ar trebui ca, în timp util, să informeze ţara terţă sau organizaţia internaţională cu privire la aceste motive şi să iniţieze consultări cu aceasta pentru remedierea situaţiei.

(108) În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie, operatorul sau persoana împuternicită de operator ar trebui să adopte măsuri pentru a compensa lipsa protecţiei datelor într-o ţară terţă prin intermediul unor garanţii adecvate pentru persoana vizată. Astfel de garanţii adecvate pot consta în utilizarea regulilor corporatiste obligatorii, a clauzelor standard de protecţie a datelor adoptate de Comisie, a clauzelor standard de protecţie a datelor adoptate de o autoritate de supraveghere sau a clauzelor contractuale autorizate de o autoritate de supraveghere. Respectivele garanţii ar trebui să asigure respectarea cerinţelor în materie de protecţie a datelor şi drepturi ale persoanelor vizate corespunzătoare prelucrării în interiorul Uniunii, inclusiv disponibilitatea unor drepturi opozabile ale persoanelor vizate şi a unor căi de atac eficiente, printre care dreptul de acces la reparaţii efective pe cale administrativă sau judiciară şi dreptul de a solicita despăgubiri, în Uniune sau într-o ţară terţă. Acestea ar trebui să se refere în special la respectarea principiilor generale privind prelucrarea datelor cu caracter personal: principiul protecţiei datelor începând cu momentul conceperii şi principiul protecţiei implicite a datelor. Transferurile pot fi efectuate şi de către autorităţile sau organismele publice cu autorităţi sau organisme publice în ţări terţe sau cu organizaţii internaţionale cu atribuţii şi funcţii corespunzătoare, inclusiv pe baza dispoziţiilor care prevăd drepturi opozabile şi efective pentru persoanele vizate, care trebuie introduse în acordurile administrative, cum ar fi un memorandum de înţelegere. Autorizaţia din partea autorităţii de supraveghere competente ar trebui obţinută atunci când garanţiile sunt oferite în cadrul unor acorduri administrative fără caracter juridic obligatoriu.

(109) Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecţie a datelor, adoptate de Comisie sau de o autoritate de supraveghere, nu ar trebui să împiedice operatorii sau persoanele împuternicite de aceştia să includă clauzele standard în materie de protecţie a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator şi o altă persoană împuternicită de operator, şi nici să adauge alte clauze sau garanţii suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de o autoritate de supraveghere sau nu prejudiciază drepturile sau libertăţile fundamentale ale persoanelor vizate. Operatorii şi persoanele împuternicite de operatori ar trebui să fie încurajaţi să ofere garanţii suplimentare prin intermediul unor angajamente contractuale care să completeze clauzele standard în materie de protecţie.

(110) Un grup de întreprinderi sau un grup de întreprinderi implicat într-o activitate economică comună ar trebui să poată utiliza regulile corporatiste obligatorii aprobate pentru transferurile sale internaţionale dinspre Uniune către organizaţii din cadrul aceluiaşi grup de întreprinderi sau grup de întreprinderi implicate într-o activitate economică comună, cu condiţia ca astfel de reguli corporatiste să includă toate principiile esenţiale şi drepturile opozabile în scopul asigurării unor garanţii adecvate pentru transferurile sau categoriile de transferuri de date cu caracter personal.

(111) Ar trebui să se prevadă posibilitatea de a se efectua transferuri în anumite circumstanţe în care persoana vizată şi-a dat consimţământul explicit, în care transferul este ocazional şi necesar în legătură cu un contract sau cu o acţiune în justiţie, indiferent dacă este în contextul unei proceduri judiciare sau în contextul unei proceduri administrative sau extrajudiciare, inclusiv în cadrul procedurilor înaintate organismelor de reglementare. De asemenea, ar trebui să se prevadă posibilitatea de a se efectua transferuri în cazul în care motive importante de interes public stabilite de dreptul Uniunii sau de dreptul intern impun acest lucru sau în cazul în care transferul se efectuează dintr-un registru instituit prin lege şi destinat să fie consultat de către public sau de către persoane care au un interes legitim. În acest ultim caz, un astfel de transfer nu ar trebui să implice totalitatea datelor cu caracter personal sau ansamblul categoriilor de date conţinute în registru, iar atunci când registrul este destinat să fie consultat de persoane care au un interes legitim, transferul ar trebui să fie efectuat doar la cererea persoanelor respective sau dacă acestea sunt destinatarii, luând pe deplin în considerare interesele şi drepturile fundamentale ale persoanei vizate.

(112) Aceste derogări ar trebui să se aplice, în special, transferurilor de date solicitate şi necesare din considerente importante de interes public, de exemplu în cazul schimbului internaţional de date între autorităţile din domeniul concurenţei, administraţiile fiscale sau vamale, între autorităţile de supraveghere financiară, între serviciile competente în materie de securitate socială sau de sănătate publică, de exemplu în cazul depistării punctelor de contact pentru bolile contagioase sau pentru reducerea şi/sau eliminarea dopajului în sport. Un transfer de date cu caracter personal ar trebui, de asemenea, să fie considerat legal în cazul în care este necesar în scopul protejării unui interes care este esenţial în interesele vitale ale persoanei vizate sau ale unei alte persoane, inclusiv pentru integritatea fizică sau pentru viaţa acesteia, în cazul în care persona vizată nu are capacitatea să îşi dea consimţământul. În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie, dreptul Uniunii sau dreptul intern poate, din considerente importante de interes public, stabili în mod expres limite asupra transferului unor categorii specifice de date către o ţară terţă sau o organizaţie internaţională. Statele membre ar trebui să notifice Comisiei aceste dispoziţii. Orice transfer către o organizaţie umanitară internaţională al datelor cu caracter personal ale unei persoane vizate care se află în incapacitate fizică sau juridică de a îşi da consimţământul, în vederea îndeplinirii unei sarcini care decurge din Convenţiile de la Geneva sau în vederea conformării cu dreptul internaţional umanitar aplicabil în conflictele armate, ar putea fi considerat necesar pentru un motiv important de interes public sau pentru că este în interesul vital al persoanei vizate.

(113) Transferurile care pot fi considerate ca nefiind repetitive şi care se referă doar la un număr limitat de persoane vizate, ar putea, de asemenea, să fie efectuate în scopul realizării intereselor legitime urmărite de operator, atunci când asupra respectivelor interese nu prevalează interesele sau drepturile şi libertăţile persoanei vizate şi atunci când operatorul a evaluat toate circumstanţele aferente transferului de date. Operatorul ar trebui să acorde o atenţie deosebită naturii datelor cu caracter personal, scopului şi duratei operaţiunii sau operaţiunilor propuse de prelucrare, precum şi situaţiei din ţara de origine, din ţara terţă şi din ţara de destinaţie finală şi ar trebui să ofere garanţii adecvate pentru protecţia drepturilor şi libertăţilor fundamentale ale persoanelor fizice în ceea ce priveşte prelucrarea datelor lor cu caracter personal. Astfel de transferuri ar trebui să fie posibile numai în cazurile reziduale în care nu se poate aplica niciunul dintre celelalte motive de transfer. În ceea ce priveşte scopurile de cercetare ştiinţifică sau istorică sau scopurile statistice, ar trebui să se ia în considerare aşteptările legitime ale societăţii cu privire la creşterea nivelului de cunoştinţe. Operatorul ar trebui să informeze autoritatea de supraveghere şi persoana vizată cu privire la transfer.

(114) În orice caz, atunci când Comisia nu a luat o decizie cu privire la nivelul adecvat de protecţie a datelor dintr-o ţară terţă, operatorul sau persoana împuternicită de operator ar trebui să utilizeze soluţii care să ofere persoanelor vizate drepturi opozabile şi efective în ceea ce priveşte prelucrarea datelor lor în Uniune odată ce aceste date au fost transferate, astfel încât persoanele vizate să beneficieze în continuare de drepturi fundamentale şi garanţii.

(115) Unele ţări terţe au adoptat legi, reglementări şi alte acte juridice care au drept obiectiv să reglementeze în mod direct activităţile de prelucrare a datelor ale persoanelor fizice şi juridice aflate sub jurisdicţia statelor membre. Aceasta poate include hotărâri ale instanţelor judecătoreşti sau decizii ale autorităţilor administrative din ţări terţe care solicită unui operator sau unei persoane împuternicite de operator să transfere sau să divulge date cu caracter personal şi care nu se bazează pe un acord internaţional, cum ar fi un tratat de asistenţă juridică reciprocă, în vigoare între ţara terţă solicitantă şi Uniune sau un stat membru. Aplicarea extrateritorială a acestor legi, reglementări şi alte acte juridice poate încălca dreptul internaţional şi poate împiedica asigurarea protecţiei persoanelor fizice asigurată în Uniune prin prezentul regulament. Transferurile ar trebui să fie permise numai în cazul îndeplinirii condiţiilor prevăzute de prezentul regulament pentru un transfer către ţări terţe. Acesta ar putea fi cazul, inter alia, atunci când divulgarea este necesară dintr-un motiv important de interes public recunoscut în dreptul Uniunii sau în dreptul intern care se aplică operatorului.

(116) Fluxul transfrontalier de date cu caracter personal în afara Uniunii poate expune unui risc sporit capacitatea persoanelor fizice de a-şi exercita drepturile în materie de protecţie a datelor, în special pentru a-şi asigura protecţia împotriva utilizării sau a divulgării ilegale a acestor informaţii. În acelaşi timp, autorităţile de supraveghere pot constata că se află în imposibilitatea de a trata plângeri sau de a efectua investigaţii referitoare la activităţile desfăşurate în afara frontierelor lor. Eforturile acestora de a conlucra în context transfrontalier pot fi, de asemenea, îngreunate de insuficienţa competenţelor de prevenire sau remediere, de caracterul eterogen al regimurilor juridice şi de existenţa unor obstacole de ordin practic, cum ar fi constrângerile în materie de resurse. Prin urmare, este necesar să se promoveze o cooperare mai strânsă între autorităţile de supraveghere a protecţiei datelor pentru a putea face schimb de

informaţii şi a desfăşura investigaţii împreună cu omologii lor internaţionali. În scopul elaborării de mecanisme de cooperare internaţională pentru a facilita şi a oferi asistenţă internaţională reciprocă în asigurarea aplicării legislaţiei din domeniul protecţiei datelor cu caracter personal, Comisia şi autorităţile de supraveghere ar trebui să facă schimb de informaţii şi să coopereze în cadrul activităţilor legate de exercitarea competenţelor lor cu autorităţile competente din ţări terţe, pe bază de reciprocitate şi în conformitate cu prezentul regulament.

(117) Instituirea în statele membre a unor autorităţi de supraveghere, împuternicite să îşi îndeplinească sarcinile şi să îşi exercite competenţele în deplină independenţă, este un element esenţial al protecţiei persoanelor fizice în ceea ce priveşte prelucrarea datelor lor cu caracter personal. Statele membre ar trebui să poată institui mai multe autorităţi de supraveghere, pentru a reflecta structura lor constituţională, organizatorică şi administrativă.

(118) Independenţa autorităţilor de supraveghere nu ar trebui să însemne că autorităţile de supraveghere nu pot face obiectul unor mecanisme de control sau de monitorizare în ceea cepriveşte cheltuielile acestora sau unui control jurisdicţional.

(119) În cazul în care un stat membru instituie mai multe autorităţi de supraveghere, acesta ar trebui să stabilească prin lege mecanisme care să asigure participarea efectivă a autorităţilor de supraveghere respective la mecanismul pentru asigurarea coerenţei. Statul membru respectiv ar trebui, în special, să desemneze autoritatea de supraveghere care îndeplineşte funcţia de punct unic de contact pentru participarea efectivă a acestor autorităţi la mecanism, în scopul asigurării unei cooperări rapide şi armonioase cu alte autorităţi de supraveghere, cu comitetul şi cu Comisia.

(120) Fiecare autoritate de supraveghere ar trebui să beneficieze de resurse financiare şi umane, de spaţiile şi de infrastructura necesare pentru îndeplinirea cu eficacitate a sarcinilor lor, inclusiv a celor legate de asistenţa reciprocă şi cooperarea cu alte autorităţi de supraveghere în întreaga Uniune. Fiecare autoritate de supraveghere ar trebui să aibă un buget public anual separat, care poate face parte din bugetul general de stat sau naţional.

(121) Condiţiile generale pentru membrul sau membrii autorităţii de supraveghere ar trebui stabilite de lege în fiecare stat membru şi ar trebui, în special, să prevadă că respectivii membri sunt numiţi printr-o procedură transparentă fie de parlamentul, de guvernul ori şeful de stat al statului membru pe baza unei propuneri din partea guvernului, a unui membru al guvernului, a parlamentului sau a unei camere a parlamentului, fie de către un organism independent împuternicit prin dreptul intern. În vederea asigurării independenţei autorităţii de supraveghere, membrul sau membrii acesteia ar trebui să acţioneze cu integritate, să nu întreprindă acţiuni incompatibile cu îndatoririle lor, iar, pe durata mandatului, ar trebui să nu desfăşoare activităţi incompatibile, remunerate sau nu. Autoritatea de supraveghere ar trebui să aibă personal propriu, ales de autoritatea de supraveghere sau de un organism independent înfiinţat în temeiul dreptului intern, care ar trebui să fie subordonat exclusiv membrului sau membrilor autorităţii de supraveghere.

(122) Fiecare autoritate de supraveghere ar trebui să aibă, pe teritoriul statului membru de care aparţine, atribuţia de a exercita competenţele şi de a îndeplini sarcinile cu care este învestită în conformitate cu prezentul regulament. Aceasta ar trebui să includă în special prelucrarea în contextul activităţilor unui sediu al operatorului sau al persoanei împuternicite de operator pe teritoriul propriului stat membru, prelucrarea datelor cu caracter personal efectuată de autorităţile publice sau de organisme private care acţionează în interes public, prelucrarea care afectează persoanele vizate de pe teritoriul său sau prelucrarea efectuată de către un operator sau o persoană împuternicită de operator care nu îşi are sediul în Uniune în cazul în care aceasta priveşte persoane vizate care îşi au reşedinţa pe teritoriul său. Aceasta ar trebui să includă tratarea plângerilor depuse de o persoană vizată, efectuarea de investigaţii privind aplicarea prezentului regulament şi promovarea informării publicului cu privire la riscurile, normele, garanţiile şi drepturile în materie de prelucrare a datelor cu caracter personal.

(123) Autorităţile de supraveghere ar trebui să monitorizeze aplicarea dispoziţiilor prevăzute de prezentul regulament şi să contribuie la aplicarea coerentă a acestuia în întreaga Uniune, în scopul asigurării protecţiei persoanelor fizice în ceea ce priveşte prelucrarea datelor lor cu caracter personal şi al facilitării liberei circulaţii a datelor cu caracter personal în interiorul pieţei interne. În acest sens, autorităţile de supraveghere ar trebui să coopereze reciproc, precum şi cu Comisia, fără să fie necesar niciun acord între statele membre cu privire la acordarea de asistenţă reciprocă sau cu privire la respectiva cooperare.

(124) În cazul în care prelucrarea datelor cu caracter personal se desfăşoară în cadrul activităţilor unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune, iar operatorul sau

persoana împuternicită de operator are sedii în mai multe state membre, sau în cazul în care prelucrarea care se desfăşoară în contextul activităţilor unui singur sediu al unui operator sau al unei persoane împuternicite de operator din Uniune afectează sau este susceptibilă să afecteze semnificativ persoane vizate din mai multe state membre, autoritatea de supraveghere a sediului principal al operatorului sau al persoanei împuternicite de operator ori a sediului unic al operatorului sau al persoanei împuternicite de operator ar trebui să acţioneze în calitate de autoritate principală. Aceasta ar trebui să coopereze cu celelalte autorităţi vizate, pentru că operatorul sau persoana împuternicită de operator are un sediu pe teritoriul statului lor membru, pentru că persoanele vizate care îşi au reşedinţa pe teritoriul lor sunt afectate în mod semnificativ sau pentru că le-a fost înaintată o plângere. De asemenea, în cazul în care o persoană vizată care nu îşi are reşedinţa în statul membru respectiv a depus o plângere, autoritatea de supraveghere la care a fost depusă plângerea ar trebui, de asemenea, să fie o autoritate de supraveghere vizată. În cadrul sarcinilor sale de a emite orientări cu privire la orice chestiune referitoare la punerea în aplicare a prezentului regulament, comitetul ar trebui să poată emite orientări privind, în special, criteriile care trebuie luate în considerare pentru a se stabili dacă prelucrarea în cauză afectează în mod semnificativ persoane vizate din mai multe state membre şi privind conţinutul unei obiecţii relevante şi motivate.

(125) Autoritatea principală ar trebui să aibă competenţa de a adopta decizii obligatorii privind măsurile de aplicare a competenţelor care îi sunt conferite în conformitate cu prezentul regulament. În calitatea sa de autoritate principală, autoritatea de supraveghere ar trebui să implice îndeaproape şi să coordoneze activităţile autorităţilor de supraveghere vizate în procesul decizional. În cazurile în care decizia este de respingere parţială sau totală a plângerii din partea persoanei vizate, o asemenea decizie ar trebui adoptată de către autoritatea de supraveghere la care s-a depus plângerea.

(126) Decizia ar trebui convenită în comun de autoritatea de supraveghere principală şi de autorităţile de supraveghere vizate şi ar trebui să vizeze sediul principal sau sediul unic al operatorului sau al persoanei împuternicite de operator şi să fie obligatorie pentru operator şi pentru persoana împuternicită de operator. Operatorul sau persoana împuternicită de operator ar trebui să ia măsurile necesare pentru a asigura conformitatea cu prezentul regulament şi punerea în aplicare a deciziei notificate de autoritatea de supraveghere principală sediului principal al operatorului sau al persoanei împuternicite de operator în ceea ce priveşte activităţile de prelucrare în Uniune.

(127) Fiecare autoritate de supraveghere care nu acţionează ca autoritate de supraveghere principală ar trebui să aibă competenţa de a trata cazuri locale, în care operatorul sau persoana împuternicită de operator are sedii în mai multe state membre, dar obiectul respectivei prelucrări priveşte doar prelucrarea efectuată într-un singur stat membru şi implicând doar persoane vizate din acel unic stat membru, de exemplu în cazul în care obiectul îl constituie prelucrarea datelor cu caracter personal ale angajaţilor în contextul specific legat de forţa de muncă dintr-un stat membru. În astfel de cazuri, autoritatea de supraveghere ar trebui să informeze fără întârziere autoritatea de supraveghere principală cu privire la această chestiune. După ce a fost informată, autoritatea de supraveghere principală ar trebui să decidă dacă va trata ea însăşi cazul în temeiul dispoziţiei privind cooperarea între autoritatea de supraveghere principală şi alte autorităţi de supraveghere vizate ("mecanismul ghişeului unic") , sau dacă autoritatea de supraveghere care a informat-o ar trebui să se ocupe de caz la nivel local. Atunci când decide dacă va trata cazul, autoritatea de supraveghere principală ar trebui să ia în considerare dacă există un sediu al operatorului sau al persoanei împuternicite de operator în statul membru al autorităţii de supraveghere care a informat-o, în vederea garantării respectării efective a unei decizii în ceea ce priveşte operatorul sau persoana împuternicită de operator. În cazul în care autoritatea de supraveghere principală decide să trateze cazul, autoritatea de supraveghere care a informat-o ar trebui să beneficieze de posibilitatea de a prezenta un proiect de decizie, de care autoritatea de supraveghere principală ar trebui să ţină seama în cea mai mare măsură atunci când pregăteşte proiectul său de decizie în cadrul respectivului mecanism al ghişeului unic.

(128) Normele privind autoritatea de supraveghere principală şi mecanismul ghişeului unic nu ar trebui să se aplice în cazul în care prelucrarea este efectuată de autorităţi publice sau organisme private în interes public. În asemenea cazuri, singura autoritate de supraveghere competentă să îşi exercite competenţele care i-au fost atribuite în conformitate cu prezentul regulament ar trebui să fie autoritatea de supraveghere a statului membru în care autoritatea publică sau organismul privat îşi are sediul.

(129) Pentru a se asigura consecvenţa monitorizării şi a aplicării prezentului regulament în întreaga Uniune, autorităţile de supraveghere ar trebui să aibă în fiecare stat membru aceleaşi sarcini şi competenţe efective, inclusiv competenţe de investigare, competenţe corective şi sancţiuni, precum şi competenţe de

autorizare şi de consiliere, în special în cazul plângerilor depuse de persoane fizice, precum şi, fără a aduce atingere competenţelor autorităţilor de urmărire penală în temeiul dreptului intern, de a aduce în atenţia autorităţilor judiciare cazurile de încălcare a prezentului regulament şi de a se implica în proceduri judiciare. Aceste competenţe ar trebui să includă şi competenţa de a impune o limitare temporară sau definitivă, inclusiv o interdicţie, asupra prelucrării. Statele membre pot stabili alte sarcini legate de protecţia datelor cu caracter personal în temeiul prezentului regulament. Competenţele autorităţilor de supraveghere ar trebui exercitate în conformitate cu garanţii procedurale adecvate prevăzute în dreptul Uniunii şi în dreptul intern, în mod imparţial, echitabil şi într-un termen rezonabil. În special, fiecare măsură ar trebui să fie adecvată, necesară şi proporţională în scopul de a asigura conformitatea cu dispoziţiile prezentului regulament, luând în considerare circumstanţele fiecărui caz în parte, să respecte dreptul oricărei persoane de a fi ascultată înainte de luarea oricărei măsuri individuale care ar putea să îi aducă atingere şi să evite costurile inutile şi inconvenientele excesive pentru persoanele în cauză. Competenţele de investigare în ceea ce priveşte accesul în incinte ar trebui exercitate în conformitate cu cerinţele specifice din dreptul procedural naţional, cum ar fi obligaţia de a obţine în prealabil o autorizare judiciară. Fiecare măsură obligatorie din punct de vedere juridic luată de autoritatea de supraveghere ar trebui să fie prezentată în scris, să fie clară şi lipsită de ambiguitate, să indice autoritatea de supraveghere care a emis măsura, data emiterii măsurii, să poarte semnătura şefului sau a unui membru al autorităţii de supraveghere autorizat de acesta, să furnizeze motivele pentru care s-a luat măsura şi să facă trimitere la dreptul la o cale de atac eficientă. Acest lucru nu ar trebui să excludă cerinţe suplimentare în conformitate cu dreptul procedural naţional. Adoptarea unor astfel de decizii obligatorii din punct de vedere juridic implică faptul că se poate da naştere unui control jurisdicţional în statul membru al autorităţii de supraveghere care a adoptat decizia.

(130) În cazul în care autoritatea de supraveghere la care s-a depus plângerea nu este autoritatea de supraveghere principală, autoritatea de supraveghere principală ar trebui să coopereze îndeaproape cu autoritatea de supraveghere la care s-a depus plângerea, în conformitate cu dispoziţiile privind cooperarea şi consecvenţa prevăzute în prezentul regulament. În astfel de cazuri, autoritatea de supraveghere principală ar trebui, atunci când ia măsuri destinate să producă efecte juridice, inclusiv impunerea de amenzi administrative, să ţină seama cât mai mult posibil de opinia autorităţii de supraveghere la care a fost depusă plângerea şi care ar trebui să îşi menţină competenţa de a desfăşura orice investigaţie pe teritoriul propriului stat membru, în colaborare cu autoritatea de supraveghere principală.

(131) În cazurile în care o altă autoritate de supraveghere ar trebui să acţioneze în calitate de autoritate de supraveghere principală pentru activităţile de prelucrare ale operatorului sau alepersoanei împuternicite de operator, dar obiectul concret al unei plângeri sau posibila încălcare vizează numai activităţile de prelucrare ale operatorului sau ale persoanei împuternicite de operator în statul membru în care a fost depusă plângerea sau a fost depistată posibila încălcare, iar chestiunea nu afectează în mod substanţial sau nu este susceptibilă să afecteze în mod substanţial persoane vizate din alte state membre, autoritatea de supraveghere care a primit o plângere sau a depistat ori a fost informată în alt mod asupra unor situaţii de posibile încălcări ale prezentului regulament ar trebui să încerce o soluţionare pe cale amiabilă cu operatorul şi, în cazul în care aceasta eşuează, să îşi exercite plenitudinea competenţelor. Aceasta ar trebui să includă activităţi specifice de prelucrare efectuate pe teritoriul statului membru al autorităţii de supraveghere ori cu privire la persoane vizate de pe teritoriul acelui stat membru, activităţi de prelucrare care au loc în contextul unei oferte de bunuri sau servicii destinate în mod special persoanelor vizate pe teritoriul statului membru al autorităţii de supraveghere sau activităţi de prelucrare care trebuie evaluate ţinând seama de obligaţiile juridice relevante în temeiul dreptului intern.

(132) Activităţile de creştere a gradului de conştientizare organizate pentru public de autorităţile de supraveghere ar trebui să includă măsuri specifice care să vizeze operatorii şi persoanele împuternicite de operatori, inclusiv microîntreprinderile şi întreprinderile mici şi mijlocii, precum şi persoanele fizice, în special în context educaţional.

(133) Autorităţile de supraveghere ar trebui să îşi acorde reciproc asistenţă în îndeplinirea sarcinilor care le revin, pentru a se asigura coerenţa aplicării prezentului regulament pe piaţa internă. O autoritate de supraveghere care solicită asistenţă reciprocă poate adopta o măsură provizorie în cazul în care nu primeşte un răspuns la o solicitare de asistenţă reciprocă în termen de o lună de la primirea solicitării de către cealaltă autoritate de supraveghere.

(134) Fiecare autoritate de supraveghere ar trebui să participe, după caz, la operaţiuni comune între autorităţile de supraveghere. Autoritatea de supraveghere căreia i s-a adresat solicitarea ar trebui să aibă obligaţia de a răspunde cererii într-un anumit termen.

(135) Pentru a se asigura aplicarea coerentă a prezentului regulament în întreaga Uniune, ar trebui să se instituie un mecanism pentru asigurarea coerenţei în cadrul căruia autorităţile de supraveghere să coopereze. Acest mecanism ar trebui să se aplice, în special, în cazul în care o autoritate de supraveghere intenţionează să adopte o măsură prevăzută a produce efecte juridice în ceea ce priveşte operaţiunile de prelucrare care afectează în mod substanţial un număr semnificativ de persoane vizate din mai multe state membre. Mecanismul ar trebui să se aplice, de asemenea, în cazul în care o autoritate de supraveghere vizată sau Comisia solicită ca aspectul respectiv să fie tratat în cadrul mecanismului pentru asigurarea coerenţei. Acest mecanism nu ar trebui să aducă atingere măsurilor pe care Comisia le poate adopta în exercitarea competenţelor care îi revin în temeiul tratatelor.

(136) În aplicarea mecanismului pentru asigurarea coerenţei, comitetul ar trebui, într-un anumit termen, să emită un aviz în cazul în care o majoritate a membrilor săi decide astfel sau în cazul în care orice autoritate de supraveghere vizată sau Comisia solicită acest lucru. Comitetul ar trebui, de asemenea, să fie împuternicit să adopte decizii obligatorii din punct de vedere juridic în cazul unor litigii între autorităţile de supraveghere. În acest scop, acesta ar trebui să emită, în principiu cu o majoritate de două treimi din membrii săi, decizii obligatorii din punct de vedere juridic, în cazuri bine definite, în cazul în care există opinii divergente între autorităţile de supraveghere, în special în cadrul mecanismului de cooperare între autoritatea de supraveghere principală şi autorităţile de supraveghere vizate privind fondul cauzei, în special existenţa sau nu a unei încălcări a prezentului regulament.

(137) Este posibil să existe o necesitate urgentă de a se acţiona pentru asigurarea protecţiei drepturilor şi libertăţilor persoanelor vizate, în special în cazul în care există pericolul ca exercitarea unui drept al unei persoane vizate să fie împiedicată în mod considerabil. Prin urmare, o autoritate de supraveghere ar trebui să poată adopta măsuri provizorii pe teritoriul său, justificate în mod corespunzător, având o perioadă de valabilitate determinată care nu ar trebui să depăşească trei luni.

(138) Aplicarea unui astfel de mecanism ar trebui să constituie o condiţie pentru legalitatea unei măsuri destinate să producă efecte juridice, luate de o autoritate de supraveghere, în cazurile în care aplicarea acesteia este obligatorie. În alte cazuri cu relevanţă transfrontalieră, ar trebui pus în aplicare mecanismul de cooperare între autoritatea de supraveghere principală şi autorităţile de supraveghere vizate, iar între autorităţile de supraveghere vizate s-ar putea acorda asistenţă reciprocă şi s-ar putea desfăşura operaţiuni comune pe bază bilaterală sau multilaterală, fără declanşarea mecanismului pentru asigurarea coerenţei.

(139) Cu scopul de a promova aplicarea coerentă a prezentului regulament, comitetul ar trebui instituit ca organ independent al Uniunii. Pentru a-şi îndeplini obiectivele, comitetul ar trebui să aibă personalitate juridică. Comitetul ar trebui să fie reprezentat de preşedintele său. Acesta ar trebui să înlocuiască Grupul de lucru pentru protecţia persoanelor în ceea ce priveşte prelucrarea datelor cu caracter personal, instituit prin Directiva **95/46/CE**. Acesta ar trebui să fie alcătuit din şefii autorităţilor de supraveghere din fiecare stat membru şi din Autoritatea Europeană pentru Protecţia Datelor sau reprezentanţii acestora. Comisia ar trebui să participe la activităţile comitetului fără a avea drept de vot, iar Autoritatea Europeană pentru Protecţia Datelor ar trebui să aibă drepturi de vot speciale. Comitetul ar trebui să contribuie la aplicarea coerentă a prezentului regulament în întreaga Uniune, inclusiv prin oferirea de consiliere Comisiei, în special cu privire la nivelul de protecţie în ţările terţe şi în cadrul organizaţiilor internaţionale, şi prin promovarea cooperării autorităţilor desupraveghere în întreaga Uniune. Comitetul ar trebui să acţioneze în mod independent în îndeplinirea sarcinilor sale.

(140) Comitetul ar trebui să fie asistat de un secretariat asigurat de Autoritatea Europeană pentru Protecţia Datelor. Personalul Autorităţii Europene pentru Protecţia Datelor implicat în îndeplinirea sarcinilor conferite comitetului în temeiul prezentului regulament ar trebui să îşi îndeplinească sarcinile exclusiv conform instrucţiunilor preşedintelui comitetului şi să raporteze acestuia.

(141) Orice persoană vizată ar trebui să aibă dreptul de a depune o plângere la o singură autoritate de supraveghere, în special în statul membru în care îşi are reşedinţa obişnuită, precum şi dreptul la o cale de atac eficientă în conformitate cu articolul 47 din **cartă**, în cazul în care persoana vizată consideră că drepturile sale în temeiul prezentului regulament sunt încălcate sau în cazul în care autoritatea de supraveghere nu reacţionează la o plângere, respinge sau refuză parţial sau total o plângere sau nu acţionează atunci când o astfel de acţiune este necesară pentru asigurarea protecţiei drepturilor persoanei vizate. Investigaţia în urma unei plângeri ar trebui să fie efectuată, sub control judiciar, în măsura în care este necesar, în funcţie de caz. Autoritatea de supraveghere ar trebui să informeze persoana vizată cu privire la evoluţia şi soluţionarea 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 informaţii intermediare persoanei vizate. În vederea facilitării depunerii plângerilor, fiecare autoritate de supraveghere ar trebui să ia măsuri precum punerea la dispoziţie a unui formular de depunere a plângerii, care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.

(142) În cazul în care persoana vizată consideră că drepturile sale în temeiul prezentului regulament sunt încălcate, aceasta ar trebui să aibă dreptul de a mandata un organism, o organizaţie sau o asociaţie fără scop lucrativ care este înfiinţat(ă) în conformitate cu dreptul intern, ale cărui (cărei) obiective statutare sunt în interesul public şi care îşi desfăşoară activitatea în domeniul asigurării protecţiei datelor cu caracter personal, să depună o plângere în numele său la o autoritate de supraveghere, să exercite dreptul la o cale de atac în numele persoanelor vizate sau, în cazul în care se prevede în dreptul intern, să exercite dreptul de a primi despăgubiri în numele persoanelor vizate. Un stat membru poate prevedea ca un astfel de organism, organizaţie sau asociaţie să aibă dreptul de a depune o plângere în statul membru respectiv, independent de mandatul acordat de o persoană vizată, şi să aibă dreptul la o cale de atac eficientă în cazul în care are motive să considere că drepturile unei persoane vizate au fost încălcate ca rezultat al unei prelucrări a datelor cu caracter personal care încalcă prezentul regulament. Organismul, organizaţia sau asociaţia în cauza nu poate pretinde despăgubiri în numele unei persoane vizate, independent de mandatul acordat de persoana vizată.

(143) Orice persoană fizică sau juridică are dreptul de a introduce o acţiune în anulare împotriva deciziilor comitetului în faţa Curţii de Justiţie, în conformitate cu condiţiile prevăzute la articolul 263 din **TFUE**. În calitate de destinatare ale acestor decizii, autorităţile de supraveghere vizate care doresc să le conteste trebuie să introducă o acţiune împotriva deciziilor respective în termen de două luni de la data la care le-au fost notificate, în conformitate cu articolul 263 din **TFUE**. În cazul în care deciziile comitetului vizează în mod direct şi individual un operator, o persoană împuternicită de operator sau reclamantul, aceştia din urmă pot introduce o acţiune în anularea respectivelor decizii în termen de două luni de la publicarea acestora pe site-ul comitetului, în conformitate cu articolul 263 din **TFUE**. Fără a aduce atingere acestui drept în temeiul articolului 263 din **TFUE**, orice persoană fizică sau juridică ar trebui să aibă dreptul la o cale de atac judiciară eficientă în faţa instanţei naţionale competente împotriva unei decizii a unei autorităţi de supraveghere care produce efecte juridice privind respectiva persoană. O astfel de decizie se referă în special la exercitarea competenţelor de investigare, corective şi de autorizare de către autoritatea de supraveghere sau la refuzul sau respingerea plângerilor. Cu toate acestea, dreptul la o cale de atac judiciară eficientă nu include măsuri ale autorităţilor de supraveghere care nu sunt obligatorii din punct de vedere juridic, cum ar fi avizele emise de autoritatea de supraveghere sau consiliere furnizată de aceasta. Acţiunile împotriva unei autorităţi de supraveghere ar trebui să fie aduse în faţa instanţelor statului membru în care este stabilită autoritatea de supraveghere şi ar trebui să se desfăşoare în conformitate cu dreptul procesual al statului membru respectiv. Respectivele instanţe ar trebui să îşi exercite competenţa judiciară deplină, care ar trebui să includă competenţa de a examina toate aspectele de fapt sau de drept care au relevanţă pentru litigiul cu care acestea sunt sesizate. În cazul în care o plângere a fost respinsă sau refuzată de o autoritate de supraveghere, reclamantul poate introduce o acţiune la instanţele din acelaşi stat membru. În contextul căilor de atac judiciare privind aplicarea prezentului regulament, instanţele naţionale care consideră necesară o decizie privind chestiunea respectivă pentru a le permite să ia o hotărâre pot sau, în cazul prevăzut la articolul 267 din **TFUE**, trebuie să solicite Curţii de Justiţie să pronunţe o decizie preliminară privind interpretarea dreptului Uniunii, inclusiv a prezentului regulament. În plus, în cazul în care o decizie a unei autorităţi de supraveghere care pune în aplicare o decizie a comitetului este contestată în faţa unei instanţe naţionale şi este în discuţie validitatea deciziei comitetului, respectiva instanţă naţională nu are competenţa de a declara nulă decizia comitetului, ci trebuie să aducă chestiunea validităţii în faţa Curţii de Justiţie, în conformitate cu articolul 267 din **TFUE**, astfel cum a fost interpretat de Curtea de Justiţie, ori de câte ori instanţa naţională consideră decizia nulă. Cu toate acestea, o instanţă naţională nu poate să transmită o chestiune cu privire la validitatea deciziei comitetului la cererea unei persoane fizice sau juridice care a avut posibilitatea de a introduce o acţiune în anulare împotriva respectivei decizii, în special dacă aceasta era vizată în mod direct şi individual de decizia în cauză, dar nu a făcut acest lucru în termenul prevăzut la articolul 263 din **TFUE**.

(144) Atunci când o instanţă sesizată cu o procedură împotriva unei decizii a unei autorităţi de supraveghere are motive să creadă că în faţa unei instanţe competente dintr-un alt stat membru au fost introduse proceduri cu privire la aceeaşi prelucrare, cum ar fi acelaşi obiect al prelucrării, de către acelaşi operator sau aceleaşi persoană împuternicită de operator, sau aceeaşi cauză, instanţa respectivă ar trebui

să contacteze cea de a doua instanţă pentru a confirma existenţa unor astfel de proceduri conexe. În cazul în care aceste proceduri conexe se află pe rolul unei instanţe dintr-un alt stat membru, orice instanţă, cu excepţia celei sesizate iniţial, poate să îşi suspende procedurile sau, la cererea uneia dintre părţi, îşi poate declina competenţa în favoarea instanţei sesizate iniţial, cu condiţia ca aceasta din urmă să aibă competenţa de a soluţiona procedurile în cauză şi ca dreptul care i se aplică să îi permită consolidarea acestor proceduri conexe. Procedurile sunt considerate conexe atunci când sunt atât de strâns legate între ele încât este oportună instrumentarea şi judecarea lor în acelaşi timp pentru a se evita riscul pronunţării unor hotărâri ireconciliabile în cazul judecării lor în mod separat.

(145) În ceea ce priveşte acţiunile iniţiate împotriva unui operator sau unei persoane împuternicite de operator, reclamantul ar trebui să aibă posibilitatea de a introduce acţiunea în faţa instanţelor din statele membre în care operatorul sau persoana împuternicită de operator are un sediu sau în care persoana vizată îşi are reşedinţa, cu excepţia cazului în care operatorul este o autoritate publică dintr-un stat membru ce acţionează în exercitarea competenţelor sale publice.

(146) Operatorul sau persoana împuternicită de operator ar trebui să plătească despăgubiri pentru orice prejudiciu pe care o persoană îl poate suferi ca urmare a unei prelucrări care încalcă prezentul regulament. Operatorul sau persoana împuternicită de operator ar trebui să fie exoneraţi de răspundere dacă dovedesc că nu sunt în niciun fel răspunzători pentru prejudiciu. Conceptul de prejudiciu ar trebui interpretat în sens larg, din perspectiva jurisprudenţei Curţii de Justiţie, într-un mod care să reflecte pe deplin obiectivele prezentului regulament. Această dispoziţie nu aduce atingere niciunei cereri de despăgubire care rezultă din încălcarea altor norme din dreptul Uniunii sau din dreptul intern. O prelucrare care încalcă prezentul regulament include şi prelucrarea care încalcă actele delegate şi de punere în aplicare adoptate în conformitate cu prezentul regulament şi cu dreptul intern care specifică norme din prezentul regulament. Persoanele vizate ar trebui să primească despăgubiri integrale şi eficace pentru prejudiciul pe care le-au suferit. În cazul în care operatorii sau persoanele împuternicite de operatori sunt implicate în aceeaşi prelucrare, fiecare operator sau fiecare persoană împuternicită de operator ar trebui să fie considerată răspunzătoare pentru întregul prejudiciu. Cu toate acestea, atunci când procedurile juridice care le vizează sunt conexate, în conformitate cu dreptul intern, despăgubirile pot fi împărţite în funcţie de răspunderea fiecărui operator sau a fiecărei persoane împuternicite de operator, cu condiţia să se asigure despăgubirea integrală şi efectivă a persoanei vizate care a suferit prejudiciul. Orice operator sau persoană împuternicită de operator care a plătit despăgubiri integrale poate formula ulterior o acţiune în regres împotriva altor operatori sau persoane împuternicite de operatori implicate în aceeaşi prelucrare.

(147) În cazul în care prezentul regulament cuprinde norme specifice privind competenţa judiciară, în special în ceea ce priveşte căile de atac judiciare, inclusiv acţiunile în despăgubiri, împotriva unui operator sau a unei persoane împuternicite de operator, normele generale privind competenţa judiciară precum cele din Regulamentul (UE) nr. **1215/2012** al Parlamentului European şi al Consiliului (1) nu ar trebui să aducă atingere aplicării unor astfel de norme specifice.

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

(148) Pentru a consolida respectarea aplicării normelor prevăzute în prezentul regulament, ar trebui impuse sancţiuni, inclusiv amenzi administrative, pentru orice încălcare a prezentului regulament, pe lângă sau în locul măsurilor adecvate impuse de autoritatea de supraveghere în temeiul prezentului regulament. În cazul unei încălcări minore sau în cazul în care amenda susceptibilă de a fi impusă ar constitui o sarcină disproporţionată pentru o persoană fizică, poate fi emis un avertisment în locul unei amenzi. Cu toate acestea, ar trebui să se ia în considerare în mod corespunzător natura, gravitatea şi durata încălcării, caracterul deliberat al încălcării, acţiunile întreprinse pentru a reduce prejudiciul cauzat, gradul de răspundere sau orice încălcări anterioare relevante, modul în care încălcarea a fost adusă la cunoştinţa autorităţii de supraveghere, conformitatea cu măsurile adoptate împotriva operatorului sau a persoanei împuternicite de operator, aderarea la un cod de conduită şi orice alt factor agravant sau atenuant. Impunerea de sancţiuni, inclusiv de amenzi administrative, ar trebui să facă obiectul unor garanţii procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii şi cu **carta**, inclusiv o protecţie judiciară eficientă şi un proces echitabil.

(149) Statele membre ar trebui să poată stabili normele privind sancţiunile penale pentru încălcările prezentului regulament, inclusiv pentru încălcarea normelor de drept intern adoptate în temeiul şi în limitele prezentului regulament. Respectivele sancţiuni penale pot, de asemenea, permite privarea de profiturile obţinute prin încălcarea prezentului regulament. Cu toate acestea, impunerea de sancţiuni

penale pentru încălcări ale unor asemenea norme de drept intern şi de sancţiuni administrative nu ar trebui să ducă la încălcarea principiului ne bis in idem, astfel cum a fost interpretat de Curtea de Justiţie.

(150) Pentru consolidarea şi armonizarea sancţiunilor administrative în cazul încălcării prezentului regulament, fiecare autoritate de supraveghere ar trebui să aibă competenţa de a impune amenzi administrative. Prezentul regulament ar trebui să indice încălcările, şi limita maximă şi criteriile pentru stabilirea amenzilor administrative aferente, care ar trebui să fie stabilite de autoritatea de supraveghere competentă în fiecare caz în parte, ţinând seama de toate circumstanţele relevante ale situaţiei specifice, luându-se în considerare în mod corespunzător, în special, natura, gravitatea şi durata încălcării, precum şi consecinţele acesteia şi măsurile luate pentru a se asigura respectarea obligaţiilor în temeiul prezentului regulament şi pentru a se preveni sau atenua consecinţele încălcării. În cazul în care amenzile administrative sunt impuse unei întreprinderi, o întreprindere ar trebui înţeleasă ca fiind o întreprindere în conformitate cu articolele 101 şi 102 din **TFUE** în aceste scopuri. În cazul în care se impun amenzi administrative unor persoane care nu sunt întreprinderi, autoritatea de supraveghere ar trebui să ţină seama de nivelul general al veniturilor din statul membru respectiv, precum şi de situaţia economică a persoanei atunci când estimează cuantumul adecvat al amenzii. Mecanismul pentru asigurarea coerenţei poate fi, de asemenea, utilizat pentru a promova aplicarea consecventă a amenzilor administrative. Competenţa de a stabili dacă şi în ce măsură autorităţile publice ar trebui să facă obiectul unor amenzi administrative ar trebui să revină statelor membre. Impunerea unei amenzi administrative sau transmiterea unei avertizări nu afectează aplicarea altor competenţe ale autorităţilor de supraveghere sau a altor sancţiuni în temeiul prezentului regulament.

(151) Sistemele juridice ale Danemarcei şi Estoniei nu permit amenzi administrative astfel cum sunt prevăzute în prezentul regulament. Normele privind amenzile administrative pot fi aplicate astfel încât, în Danemarca, amenda să fie impusă de instanţele naţionale competente ca sancţiune penală, iar în Estonia amenda să fie impusă de autoritatea de supraveghere în cadrul unei proceduri privind delictele, cu condiţia ca o astfel de aplicare a normelor în statele membre respective să aibă un efect echivalent cu cel al amenzilor administrative impuse de autorităţile de supraveghere. Prin urmare, instanţele naţionale competente ar trebui să ţină seama de recomandarea autorităţii de supraveghere care a iniţiat amenda. În orice caz, amenzile impuse ar trebui să fie eficace, proporţionale şi disuasive.

(152) În cazul în care prezentul regulament nu armonizează sancţiunile administrative sau în alte cazuri, acolo unde este necesar, de exemplu în cazul unor încălcări grave ale prezentului regulament, statele membre ar trebui să pună în aplicare un sistem care să prevadă sancţiuni eficace, proporţionale şi disuasive. Natura unor astfel de sancţiuni, penale sau administrative, ar trebui stabilită în dreptul intern.

(153) Dreptul statelor membre ar trebui să stabilească un echilibru între normele care reglementează libertatea de exprimare şi de informare, inclusiv exprimarea jurnalistică, academică, artistică şi/sau literară, şi dreptul la protecţia datelor cu caracter personal în temeiul prezentului regulament. Prelucrarea datelor cu caracter personal exclusiv în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare ar trebui să facă obiectul unor derogări sau al unor excepţii de la anumite dispoziţii ale prezentului regulament în cazul în care este necesară stabilirea unui echilibru între dreptul la protecţia datelor cu caracter personal şi dreptul la libertatea de exprimare şi de informare, astfel cum este prevăzut în articolul 11 din **cartă**. Acest lucru ar trebui să se aplice în special prelucrării datelor cu caracter personal în domeniul audiovizualului, precum şi în arhivele de ştiri şi în bibliotecile ziarelor. Prin urmare, statele membre ar trebui să adopte măsuri legislative care să prevadă excepţiile şi derogările necesare în vederea asigurării echilibrului între aceste drepturi fundamentale. Statele membre ar trebui să adopte astfel de excepţii şi derogări în ceea ce priveşte principiile generale, drepturile persoanelor vizate, operatorul şi persoana împuternicită de operator, transferul de date cu caracter personal către ţări terţe sau organizaţii internaţionale, autorităţile de supraveghere independente, cooperarea şi coerenţa, precum şi în ceea ce priveşte situaţii specifice de prelucrare a datelor. În cazul în care aceste excepţii sau derogări diferă de la un stat membru la altul, ar trebui să se aplice dreptul statului membru sub incidenţa căruia intră operatorul. Pentru a ţine seama de importanţa dreptului la libertatea de exprimare în fiecare societate democratică, este necesar ca noţiunile legate de această libertate, cum ar fi jurnalismul, să fie interpretate în sens larg.

(154) Prezentul regulament permite luarea în considerare a principiului accesului public la documente oficiale în aplicarea prezentului regulament. Accesul public la documente oficiale poate fi considerat a fi în interes public. Datele cu caracter personal din documentele deţinute de o autoritate publică sau de un organism public ar trebui să poată fi divulgate de autoritatea respectivă sau de organismul respectiv în cazul în care dreptul Uniunii sau dreptul intern sub incidenţa căruia intră

autoritatea publică sau organismul public prevede acest lucru. Dreptul Uniunii şi dreptul intern ar trebui să asigure un echilibru între accesul public la documentele oficiale şi reutilizarea informaţiilor din sectorul public, pe de o parte, şi dreptul la protecţia datelor cu caracter personal, pe de altă parte, şi ar putea prin urmare să prevadă echilibrul necesar cu dreptul la protecţia datelor cu caracter personal în temeiul prezentului regulament. Trimiterea la autorităţile şi organismele publice ar trebui, în acest context, să includă toate autorităţile sau alte organisme reglementate de dreptul intern privind accesul public la documente. Directiva **2003/98/CE** a Parlamentului European şi a Consiliului (1) lasă intact şi nu aduce atingere în niciun fel nivelului de protecţie a persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal în conformitate cu dreptul Uniunii şi cu cel intern şi, în special, nu modifică drepturile şi obligaţiile prevăzute de prezentul regulament. În special, directiva sus-menţionată nu se aplică documentelor la care accesul este exclus sau restrâns în temeiul regimurilor de acces din motive legate de protecţia datelor cu caracter personal şi nici părţilor din documente accesibile în temeiul respectivelor regimuri care conţin date cu caracter personal a căror reutilizare a fost stabilită prin lege ca fiind incompatibilă cu dreptul privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal.

(1) Directiva **2003/98/CE** a Parlamentului European şi a Consiliului din 17 noiembrie 2003 privind reutilizarea informaţiilor din sectorul public (JO L 345, 31.12.2003, p. 90) . **(155)** Dreptul intern sau acordurile colective, inclusiv "acordurile de muncă", pot prevedea norme specifice care să reglementeze prelucrarea datelor cu caracter personal ale angajaţilor în contextul ocupării unui loc de muncă, în special condiţiile în care datele cu caracter personal în contextul ocupării unui loc de muncă pot fi prelucrate pe baza consimţământului angajatului, în scopul recrutării, al respectării clauzelor contractului de muncă, inclusiv descărcarea de obligaţiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării şi organizării muncii, al egalităţii şi diversităţii la locul de muncă, al asigurării sănătăţii şi securităţii la locul de muncă, precum şi în scopul exercitării şi beneficierii, în mod individual sau colectiv, de drepturile şi beneficiile legate de ocuparea unui loc de muncă, precum şi în scopul încetării raporturilor de muncă.

(156) Prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice ar trebui să facă obiectul unor garanţii adecvate pentru drepturile şi libertăţile persoanei vizate în temeiul prezentului regulament. Respectivele garanţii ar trebui să asigure faptul că au fost instituite măsuri tehnice şi organizatorice necesare pentru a se asigura, în special, principiul reducerii la minimum a datelor. Prelucrarea ulterioară a datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice se efectuează atunci când operatorul a evaluat fezabilitatea pentru îndeplinirea acestor obiective prin prelucrarea unor date cu caracter personal care nu permit sau nu mai permit identificarea persoanelor vizate, cu condiţia să existe garanţii adecvate (cum ar fi pseudonimizarea datelor cu caracter personal) . Statele membre ar trebui să prevadă garanţii adecvate pentru prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice. Statele membre ar trebui să fie autorizate să ofere, în anumite condiţii şi sub rezerva unor garanţii adecvate pentru persoanele vizate, precizări şi derogări în ceea ce priveşte cererile de informaţii şi dreptul la rectificare, dreptul la ştergere, dreptul de a fi uitat, dreptul la restricţionarea prelucrării,dreptul la portabilitatea datelor, precum şi dreptul la opoziţie în cazul prelucrării datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice. Condiţiile şi garanţiile în cauză pot genera proceduri specifice astfel încât persoanele vizate să îşi exercite respectivele drepturi dacă acest lucru este adecvat în contextul scopurilor vizate de prelucrarea specifică, precum şi măsuri tehnice şi organizaţionale vizând reducerea la minimum a prelucrării datelor cu caracter personal, în conformitate cu principiile proporţionalităţii şi necesităţii. Prelucrarea datelor cu caracter personal în scopuri ştiinţifice ar trebui să fie, de asemenea, conformă cu alte acte legislative relevante, cum ar fi cele privind studiile clinice.

(157) Prin combinarea informaţiilor din registre, cercetătorii pot obţine noi cunoştinţe de mare valoare în ceea ce priveşte bolile cu largă răspândire, cum ar fi bolile cardiovasculare, cancerul şi depresia. Pe baza registrelor, rezultatele cercetărilor pot fi întărite, întrucât acestea se bazează pe o populaţie mai mare. În domeniul ştiinţelor sociale, cercetarea pe baza registrelor le permite cercetătorilor să obţină informaţii esenţiale despre corelarea pe termen lung a unei serii de condiţii sociale, precum şomajul sau educaţia, cu alte condiţii de viaţă. Rezultatele cercetărilor obţinute pe baza registrelor furnizează cunoştinţe solide, de înaltă calitate, care pot constitui baza pentru elaborarea şi punerea în aplicare a unor politici bazate pe cunoaştere şi care pot îmbunătăţi calitatea vieţii pentru un număr de persoane, eficienţa serviciilor sociale. Pentru a facilita cercetarea ştiinţifică, datele cu caracter personal pot fi prelucrate în scopuri de cercetare ştiinţifică, sub rezerva condiţiilor şi a garanţiilor corespunzătoare stabilite în dreptul Uniunii sau în dreptul intern.

(158) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare, prezentul regulament ar trebui să se aplice şi prelucrării respective, ţinând seama de faptul că prezentul regulament nu ar trebui să se aplice persoanelor decedate. Autorităţile publice sau organismele publice sau private care deţin evidenţe de interes public ar trebui, în temeiul dreptului Uniunii sau al dreptului naţional, să aibă o obligaţie legală de a dobândi, a păstra, a evalua, a pregăti, a descrie, a comunica, a promova, a disemina şi a asigura accesul la evidenţe de valoare durabilă de interes public general. Statele membre ar trebui, de asemenea, să poată să prevadă prelucrarea ulterioară a datelor cu caracter personal în scopuri de arhivare, de exemplu cu scopul de a furniza informaţii specifice referitoare la comportamentul politic în perioada fostelor regimuri de stat totalitare, la genociduri, la crime împotriva umanităţii, în special holocaustul, sau la crime de război.

(159) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare ştiinţifică, prezentul regulament ar trebui să se aplice şi prelucrării respective. În sensul prezentului regulament, prelucrarea datelor cu caracter personal în scopuri de cercetare ştiinţifică ar trebui să fie interpretată în sens larg, incluzând de exemplu dezvoltarea tehnologică şi activităţile demonstrative, cercetarea fundamentală, cercetarea aplicată şi cercetarea finanţată din surse private. Ar trebui, în plus, luat în considerare obiectivul Uniunii de creare a unui Spaţiu european de cercetare, astfel cum este menţionat la articolul 179 alineatul (1) din **TFUE**. Scopurile de cercetare ştiinţifică ar trebui să includă, de asemenea, studii efectuate în interes public în domeniul sănătăţii publice. Pentru a îndeplini caracteristicile specifice ale prelucrării datelor cu caracter personal în scopuri de cercetare ştiinţifică, ar trebui să se aplice condiţii specifice, în special în ceea ce priveşte publicarea sau divulgarea într-un alt mod a datelor cu caracter personal în contextul scopurilor de cercetare ştiinţifică. În cazul în care rezultatul cercetării ştiinţifice, în special în contextul sănătăţii, constituie un motiv pentru măsuri suplimentare în interesul persoanei vizate, normele generale ale prezentului regulament ar trebui să se aplice având în vedere aceste măsuri.

(160) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare istorică, prezentul regulament ar trebui să se aplice şi prelucrării respective. Acest lucru ar trebui să includă, de asemenea, cercetarea istorică şi cercetarea în scopuri genealogice, ţinând seama de faptul că prezentul regulament nu ar trebui să se aplice persoanelor decedate.

(161) În scopul acordării consimţământului de a participa la activităţi de cercetare ştiinţifică în cadrul testelor clinice, ar trebui să se aplice dispoziţiile relevante ale Regulamentului (UE) nr. **536/2014** al Parlamentului European şi al Consiliului (1) .

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

(162) În cazul în care datele cu caracter personal sunt prelucrate în scopuri statistice, prezentul regulament ar trebui să se aplice prelucrării respective. Dreptul Uniunii sau dreptul intern ar trebui, în limitele prezentului regulament, să determine conţinutul statistic, controlul accesului, specificaţiile pentru prelucrarea datelor cu caracter personal în scopuri statistice şi măsurile adecvate pentru a proteja drepturile şi libertăţile persoanelor vizate şi pentru a asigura confidenţialitatea datelor statistice. Aceste rezultate statistice pot fi utilizate ulterior în diferite scopuri, inclusiv în scopuri de cercetare ştiinţifică. Scopuri statistice înseamnă orice operaţiune de colectare şi prelucrare de date cu caracter personal necesară pentru anchetele statistice sau pentru producerea de rezultate statistice. Scopurile statistice presupun că rezultatul prelucrării în scopuri statistice nu constituie date cu caracter personal, ci date agregate şi că acest rezultat sau datele cu caracter personal nu sunt utilizate în sprijinul unor măsuri sau decizii privind o anumită persoană fizică.

(163) Informaţiile confidenţiale pe care autorităţile statistice de la nivelul Uniunii şi de la nivel naţional le colectează în vederea elaborării de statistici europene şi naţionale oficiale ar trebui să fie protejate. Statisticile europene ar trebui concepute, elaborate şi difuzate în conformitate cu principiile statistice prevăzute la articolul 338 alineatul (2) din **TFUE**, în timp ce statisticile naţionale ar trebui, de asemenea, să fie în conformitate cu dreptul intern. Regulamentul (CE) nr. **223/2009** al Parlamentului European şi al Consiliului (2) prevede specificaţii suplimentare privind confidenţialitatea datelor statistice pentru statisticile europene.

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

(164) În ceea ce priveşte competenţele autorităţilor de supraveghere de a obţine de la operator sau de la persoana împuternicită de operator accesul la datele cu caracter personal şi accesul în clădirile lor,

statele membre pot adopta, pe cale legislativă şi în limitele stabilite de prezentul regulament, norme specifice pentru protejarea secretului profesional sau a altor obligaţii echivalente, în măsura în care acest lucru este necesar pentru a asigura un echilibru între dreptul la protecţia datelor cu caracter personal şi obligaţia de păstrare a secretului profesional. Aceasta nu aduce atingere obligaţiilor existente ale statelor membre de a adopta norme privind secretul profesional în situaţiile cerute de dreptul Uniunii.

(165) Prezentul regulament respectă şi nu aduce atingere statutului de care beneficiază, în temeiul dreptului constituţional existent, bisericile şi asociaţiile sau comunităţile religioase din statele membre, astfel cum este recunoscut în articolul 17 din **TFUE**.

(166) În vederea îndeplinirii obiectivelor prezentului regulament, şi anume protejarea drepturilor şi libertăţilor fundamentale ale persoanelor fizice şi, în special, a dreptului acestora la protecţia datelor cu caracter personal, şi pentru a se garanta libera circulaţie a datelor cu caracter personal pe teritoriul Uniunii, competenţa de a adopta acte în conformitate cu articolul 290 din **TFUE** ar trebui să fie delegată Comisiei. În special, ar trebui adoptate acte delegate în ceea ce priveşte criteriile şi cerinţele privind mecanismele de certificare, informaţiile care trebuie prezentate prin pictograme standardizate şi procedurile pentru furnizarea unor astfel de pictograme. Este deosebit de important ca, în cadrul activităţii sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experţi. Atunci când pregăteşte şi elaborează acte delegate, Comisia ar trebui să asigure transmiterea simultană, la timp şi în mod corespunzător a documentelor relevante către Parlamentul European şi către Consiliu.

(167) În vederea asigurării unor condiţii uniforme de punere în aplicare a prezentului regulament, Comisia ar trebui învestită cu competenţe de executare în situaţiile stabilite de prezentul regulament. Competenţele respective ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. **182/2011**. În acest context, Comisia ar trebui să ia în considerare măsuri specifice pentru microîntreprinderi şi pentru întreprinderile mici şi mijlocii.

(168) Procedura de examinare ar trebui utilizată pentru adoptarea de acte de punere în aplicare privind: clauzele contractuale standard dintre operatori şi persoanele împuternicite de operatori, precum şi dintre persoanele împuternicite de operatori; codurile de conduită; standardele tehnice şi mecanismele de certificare; nivelul adecvat de protecţie oferit de o ţară terţă, de un teritoriu sau de un anumit sector de prelucrare din ţara terţă respectivă, sau de o organizaţie internaţională; clauzele standard de protecţie a datelor; formatele şi procedurile pentru schimbul electronic de informaţii între operatori, persoanele împuternicite de operatori şi autorităţile de supraveghere pentru regulile corporatiste obligatorii; asistenţa reciprocă; precum şi modalităţile de realizare a schimbului electronic de informaţii între autorităţile de supraveghere, precum şi între autorităţile de supraveghere şi comitetul.

(169) Comisia ar trebui să adopte acte de punere în aplicare imediat aplicabile atunci când dovezile disponibile arată că o ţară terţă, un teritoriu sau un anumit sector de prelucrare din ţara terţă respectivă, sau o organizaţie internaţională nu asigură un nivel de protecţie adecvat, precum şi din motive imperative de urgenţă.

(170) Deoarece obiectivul prezentului regulament, şi anume asigurarea unui nivel echivalent de protecţie a persoanelor fizice şi libera circulaţie a datelor cu caracter personal în întreaga Uniune, nu poate fi realizat în mod satisfăcător de către statele membre dar, având în vedere amploarea sau efectele acţiunii, poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarităţii, astfel cum este definit la articolul 5 din **Tratatul privind Uniunea Europeană** ("Tratatul UE") . În conformitate cu principiul proporţionalităţii, astfel cum este definit la articolul respectiv, prezentul regulament nu depăşeşte ceea ce este necesar pentru realizarea obiectivelor menţionate.

(171) Directiva **95/46/CE** ar trebui să fie abrogată prin prezentul regulament. Prelucrările în derulare la data aplicării prezentului regulament ar trebui să fie aduse în conformitate cu prezentul regulament în termen de doi ani de la data intrării în vigoare a prezentului regulament. În cazul în care prelucrările se bazează pe consimţământ în temeiul Directivei **95/46/CE**, nu este necesar ca persoana vizată să îşi dea încă o dată consimţământul în cazul în care modul în care consimţământul a fost dat este în conformitate cu condiţiile din prezentul regulament, astfel încât operatorului să i se permită să continue o astfel de prelucrare după data aplicării prezentului regulament. Deciziile adoptate ale Comisiei şi autorizaţiile autorităţilor de supraveghere emise pe baza Directivei **95/46/CE** rămân în vigoare până când vor fi modificate, înlocuite sau abrogate.

(172) Autoritatea Europeană pentru Protecţia Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. **45/2001** şi a emis un aviz la 7 martie 2012 (1) .

(1) JO C 192, 30.6.2012, p. 7.

(173) Prezentul regulament ar trebui să se aplice tuturor aspectelor referitoare la protecţia drepturilor şi libertăţilor fundamentale legate de prelucrarea datelor cu caracter personal, care nu fac obiectul unor obligaţii specifice cu acelaşi obiectiv ca cel stabilit în Directiva **2002/58/CE** a Parlamentului European şi a Consiliului (2) , inclusiv obligaţiile privind operatorul şi drepturile persoanelor fizice. Pentru a se clarifica relaţia dintre prezentul regulament şi Directiva **2002/58/CE**, respectiva directivă ar trebui să fie modificată în consecinţă. După adoptarea prezentului regulament, Directiva **2002/58/CE** ar trebui să fie revizuită în special pentru a se asigura coerenţa cu prezentul regulament,

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

ADOPTĂ PREZENTUL REGULAMENT:
-****-

CAPITOLUL I: Dispoziţii generale

Art. 1: Obiect şi obiective

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

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

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

Art. 2: Domeniul de aplicare material

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

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

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

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

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

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

(3) Pentru prelucrarea datelor cu caracter personal de către instituţiile, organele, oficiile şi agenţiile Uniunii, se aplică Regulamentul (CE) nr. **45/2001**. Regulamentul (CE) nr. **45/2001** şi alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal se adaptează la principiile şi normele din prezentul regulament în conformitate cu articolul 98.

(4) Prezentul regulament nu aduce atingere aplicării Directivei **2000/31/CE**, în special normelor privind răspunderea furnizorilor de servicii intermediari, prevăzute la articolele 12-15 din directiva menţionată.

Art. 3: Domeniul de aplicare teritorial

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

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

a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăţi de către persoana vizată; sau

b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.

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

Art. 4: Definiţii

În sensul prezentului regulament:

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

2."prelucrare" înseamnă orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;

3."restricţionarea prelucrării" înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

4."creare de profiluri" înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

5."pseudonimizare" înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informaţii suplimentare, cu condiţia ca aceste informaţii suplimentare să fie stocate separat şi să facă obiectul unor măsuri de natură tehnică şi organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

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

7."operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

8."persoană împuternicită de operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

9."destinatar" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării;

10."parte terţă" înseamnă o persoană fizică sau juridică, autoritate publică, agenţie sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

11."consimţământ" al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

12."încălcarea securităţii datelor cu caracter personal" înseamnă o încălcare a securităţii care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

13."date genetice" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau

sănătatea persoanei respective şi care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

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

15."date privind sănătatea" înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;

16."sediu principal" înseamnă:

(a) în cazul unui operator cu sedii în cel puţin două state membre, locul în care se află administraţia centrală a acestuia în Uniune, cu excepţia cazului în care deciziile privind scopurile şi mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are competenţa de a dispune punerea în aplicare a acestor decizii, caz în care sediul care a luat deciziile respective este considerat a fi sediul principal;

(b) în cazul unei persoane împuternicite de operator cu sedii în cel puţin două state membre, locul în care se află administraţia centrală a acesteia în Uniune, sau, în cazul în care persoana împuternicită de operator nu are o administraţie centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activităţile principale de prelucrare, în contextul activităţilor unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligaţii specifice în temeiul prezentului regulament;

17."reprezentant" înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul articolului 27, care reprezintă operatorul sau persoana împuternicită în ceea ce priveşte obligaţiile lor respective care le revin în temeiul prezentului regulament;

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

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

20."reguli corporatiste obligatorii" înseamnă politicile în materie de protecţie a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce priveşte transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe ţări terţe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

21."autoritate de supraveghere" înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 51;

22."autoritate de supraveghere vizată" înseamnă o autoritate de supraveghere care este vizată de procesul de prelucrare a datelor cu caracter personal deoarece:

(a) operatorul sau persoana împuternicită de operator este stabilită pe teritoriul statului membru al autorităţii de supraveghere respective;

(b) persoanele vizate care îşi au reşedinţa în statul membru în care se află autoritatea de supraveghere respectivă sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare; sau

(c) la autoritatea de supraveghere respectivă a fost depusă o plângere;

23."prelucrare transfrontalieră" înseamnă:

(a) fie prelucrarea datelor cu caracter personal care are loc în contextul activităţilor sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puţin două state membre; sau

(b) fie prelucrarea datelor cu caracter personal care are loc în contextul activităţilor unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puţin două state membre;

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

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

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

26."organizaţie internaţională" înseamnă o organizaţie şi organismele sale subordonate reglementate de dreptul internaţional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe ţări sau în temeiul unui astfel de acord.

CAPITOLUL II: Principii

Art. 5: Principii legate de prelucrarea datelor cu caracter personal

(1) Datele cu caracter personal sunt:

a) prelucrate în mod legal, echitabil şi transparent faţă de persoana vizată ("legalitate, echitate şi transparenţă") ;

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

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

d) exacte şi, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt şterse sau rectificate fără întârziere ("exactitate") ;

e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1) , sub rezerva punerii în aplicare a măsurilor de ordin tehnic şi organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor şi libertăţilor persoanei vizate ("limitări legate de stocare") ;

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

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

Art. 6: Legalitatea prelucrării

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

a) persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

c) prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale care îi revine operatorului;

d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

e) prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul;

f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terţă, cu excepţia cazului în care prevalează interesele sau drepturile şi libertăţile fundamentale ale persoanei

vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

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

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

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

a) dreptul Uniunii; sau

b) dreptul intern care se aplică operatorului.

Scopul prelucrării este stabilit pe baza respectivului temei juridic sau, în ceea ce priveşte prelucrarea menţionată la alineatul (1) litera (e) , este necesar pentru îndeplinirea unei sarcini efectuate în interes public sau în cadrul exercitării unei funcţii publice atribuite operatorului. Respectivul temei juridic poate conţine dispoziţii specifice privind adaptarea aplicării normelor prezentului regulament, printre altele: condiţiile generale care reglementează legalitatea prelucrării de către operator; tipurile de date care fac obiectul prelucrării; persoanele vizate; entităţile cărora le pot fi divulgate datele şi scopul pentru care respectivele date cu caracter personal pot fi divulgate; limitările legate de scop; perioadele de stocare; şi operaţiunile şi procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale şi echitabile cum sunt cele pentru alte situaţii concrete de prelucrare astfel cum sunt prevăzute în capitolul IX. Dreptul Uniunii sau dreptul intern urmăreşte un obiectiv de interes public şi este proporţional cu obiectivul legitim urmărit.

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

a) orice legătură dintre scopurile în care datele cu caracter personal au fost colectate şi scopurile prelucrării ulterioare preconizate;

b) contextul în care datele cu caracter personal au fost colectate, în special în ceea ce priveşte relaţia dintre persoanele vizate şi operator;

c) natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date cu caracter personal, în conformitate cu articolul 9, sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale şi infracţiuni, în conformitate cu articolul 10;

d) posibilele consecinţe asupra persoanelor vizate ale prelucrării ulterioare preconizate;

e) existenţa unor garanţii adecvate, care pot include criptarea sau pseudonimizarea.

Art. 7: Condiţii privind consimţământul

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

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

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

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

Art. 8: Condiţii aplicabile în ceea ce priveşte consimţământul copiilor în legătură cu serviciile societăţii informaţionale

(1) În cazul în care se aplică articolul 6 alineatul (1) litera (a) , în ceea ce priveşte oferirea de servicii ale societăţii informaţionale în mod direct unui copil, prelucrarea datelor cu caracter personal ale unui copil este legală dacă copilul are cel puţin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă şi în măsura în care consimţământul respectiv este acordat sau autorizat de titularul răspunderii părinteşti asupra copilului. Statele membre pot prevedea prin lege o vârstă inferioară în aceste scopuri, cu condiţia ca acea vârstă inferioară să nu fie mai mică de 13 ani.

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

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

Art. 9: Prelucrarea de categorii speciale de date cu caracter personal

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

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

a) persoana vizată şi-a dat consimţământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepţia cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicţia prevăzută la alineatul (1) să nu poată fi ridicată prin consimţământul persoanei vizate;

b) prelucrarea este necesară în scopul îndeplinirii obligaţiilor şi al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forţei de muncă şi al securităţii sociale şi protecţiei sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanţii adecvate pentru drepturile fundamentale şi interesele persoanei vizate;

c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-şi da consimţământul;

d) prelucrarea este efectuată în cadrul activităţilor lor legitime şi cu garanţii adecvate de către o fundaţie, o asociaţie sau orice alt organism fără scop lucrativ şi cu specific politic, filozofic, religios sau sindical, cu condiţia ca prelucrarea să se refere numai la membrii sau la foştii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale şi ca datele cu caracter personal să nu fie comunicate terţilor fără consimţământul persoanelor vizate;

e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;

f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanţă sau ori de câte ori instanţele acţionează în exerciţiul funcţiei lor judiciare;

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

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

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

j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1) , în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia

datelor şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate.

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

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

Art. 10: Prelucrarea de date cu caracter personal referitoare la condamnări penale şi infracţiuni

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

Art. 11: Prelucrarea care nu necesită identificare

(1) În cazul în care scopurile pentru care un operator prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu are obligaţia de a păstra, obţine sau prelucra informaţii suplimentare pentru a identifica persoana vizată în scopul unic al respectării prezentului regulament.

(2) Dacă, în cazurile menţionate la alineatul (1) din prezentul articol, operatorul poate demonstra că nu este în măsură să identifice persoana vizată, operatorul informează persoana vizată în mod corespunzător, în cazul în care este posibil. În astfel de cazuri, articolele 15-20 nu se aplică, cu excepţia cazului în care persoana vizată, în scopul exercitării drepturilor sale în temeiul respectivelor articole, oferă informaţii suplimentare care permit identificarea sa.

CAPITOLUL III: Drepturile persoanei vizate

Secţiunea 1: Transparenţă şi modalităţi

Art. 12: Transparenţa informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor persoanei vizate

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

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

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

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

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

a) fie să perceapă o taxă rezonabilă ţinând cont de costurile administrative pentru furnizarea informaţiilor sau a comunicării sau pentru luarea măsurilor solicitate;

b) fie să refuze să dea curs cererii.

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

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

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

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

Secţiunea 2: Informare şi acces la date cu caracter personal

Art. 13: Informaţii care se furnizează în cazul în care datele cu caracter personal sunt colectate de la persoana vizată

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

a) identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;

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

c) scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;

d) în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f) , interesele legitime urmărite de operator sau de o parte terţă;

e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

f) dacă este cazul, intenţia operatorului de a transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională şi existenţa sau absenţa unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menţionate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf, o trimitere la garanţiile adecvate sau corespunzătoare şi la mijloacele de a obţine o copie a acestora, în cazul în care acestea au fost puse la dispoziţie.

(2) În plus faţă de informaţiile menţionate la alineatul (1) , în momentul în care datele cu caracter personal sunt obţinute, operatorul furnizează persoanei vizate următoarele informaţii suplimentare necesare pentru a asigura o prelucrare echitabilă şi transparentă:

a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

b) existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării sau a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;

c) atunci când prelucrarea se bazează pe articolul 6 alineatul (1) litera (a) sau pe articolul 9 alineatul (2) litera (a) , existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;

d) dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;

e) dacă furnizarea de date cu caracter personal reprezintă o obligaţie legală sau contractuală sau o obligaţie necesară pentru încheierea unui contract, precum şi dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii;

f) existenţa unui proces decizional automatizat incluzând crearea de profiluri, menţionat la articolul 22 alineatele (1) şi (4) , precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(3) În cazul în care operatorul intenţionează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de

această prelucrare ulterioară, informaţii privind scopul secundar respectiv şi orice informaţii suplimentare relevante, în conformitate cu alineatul (2) .

(4) Alineatele (1) , (2) şi (3) nu se aplică dacă şi în măsura în care persoana vizată deţine deja informaţiile respective.

Art. 14: Informaţii care se furnizează în cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată

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

a) identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;

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

c) scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;

d) categoriile de date cu caracter personal vizate;

e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;

f) dacă este cazul, intenţia operatorului de a transfera date cu caracter personal către un destinatar dintr-o ţară terţă sau o organizaţie internaţională şi existenţa sau absenţa unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menţionate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf, o trimitere la garanţiile adecvate sau corespunzătoare şi la mijloacele de a obţine o copie a acestora, în cazul în care acestea au fost puse la dispoziţie.

(2) Pe lângă informaţiile menţionate la alineatul (1) , operatorul furnizează persoanei vizate următoarele informaţii necesare pentru a asigura o prelucrare echitabilă şi transparentă în ceea ce priveşte persoana vizată:

a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

b) în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f) , interesele legitime urmărite de operator sau de o parte terţă;

c) existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării şi a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;

d) atunci când prelucrarea se bazează pe articolul 6 alineatul (1) litera (a) sau pe articolul 9 alineatul (2) litera (a) , existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;

e) dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;

f) sursa din care provin datele cu caracter personal şi, dacă este cazul, dacă acestea provin din surse disponibile public;

g) existenţa unui proces decizional automatizat incluzând crearea de profiluri, menţionat la articolul 22 alineatele (1) şi (4) , precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(3) Operatorul furnizează informaţiile menţionate la alineatele (1) şi (2) :

a) într-un termen rezonabil după obţinerea datelor cu caracter personal, dar nu mai mare de o lună, ţinându-se seama de circumstanţele specifice în care sunt prelucrate datele cu caracter personal;

b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă; sau

c) dacă se intenţionează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.

(4) În cazul în care operatorul intenţionează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obţinute, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informaţii privind scopul secundar respectiv şi orice informaţii suplimentare relevante, în conformitate cu alineatul (2) .

(5) Alineatele (1) -(4) nu se aplică dacă şi în măsura în care:

a) persoana vizată deţine deja informaţiile;

b) furnizarea acestor informaţii se dovedeşte a fi imposibilă sau ar implica eforturi disproporţionate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, sub rezerva condiţiilor şi a garanţiilor prevăzute la articolul 89 alineatul (1) , sau în măsura în care obligaţia menţionată la alineatul (1) din prezentul articol este susceptibil să facă

imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective In astfel de cazuri, operatorul ia măsuri adecvate pentru a proteja drepturile, libertăţile şi interesele legitime ale persoanei vizate, inclusiv punerea informaţiilor la dispoziţia publicului;

c) obţinerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern sub incidenţa căruia intră operatorul şi care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau

d) în cazul în care datele cu caracter personal trebuie să rămână confidenţiale în temeiul unei obligaţii statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligaţii legale de a păstra secretul.

Art. 15: Dreptul de acces al persoanei vizate

(1) Persoana vizată are dreptul de a obţine din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc şi, în caz afirmativ, acces la datele respective şi la următoarele informaţii:

a) scopurile prelucrării;

b) categoriile de date cu caracter personal vizate;

c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din ţări terţe sau organizaţii internaţionale;

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

e) existenţa dreptului de a solicita operatorului rectificarea sau ştergerea datelor cu caracter personal ori restricţionarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;

f) dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;

g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informaţii disponibile privind sursa acestora;

h) existenţa unui proces decizional automatizat incluzând crearea de profiluri, menţionat la articolul 22 alineatele (1) şi (4) , precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(2) În cazul în care datele cu caracter personal sunt transferate către o ţară terţă sau o organizaţie internaţională, persoana vizată are dreptul să fie informată cu privire la garanţiile adecvate în temeiul articolului 46 referitoare la transfer.

(3) Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative. În cazul în care persoana vizată introduce cererea în format electronic şi cu excepţia cazului în care persoana vizată solicită un alt format, informaţiile sunt furnizate într-un format electronic utilizat în mod curent.

(4) Dreptul de a obţine o copie menţionată la alineatul (3) nu aduce atingere drepturilor şi libertăţilor altora.

Secţiunea 3: Rectificare şi ştergere

Art. 16: Dreptul la rectificare

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

Art. 17: Dreptul la ştergerea datelor ("dreptul de a fi uitat")

(1) Persoana vizată are dreptul de a obţine din partea operatorului ştergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligaţia de a şterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:

a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

b) persoana vizată îşi retrage consimţământul pe baza căruia are loc prelucrarea, în conformitate cu articolul 6 alineatul (1) litera (a) sau cu articolul 9 alineatul (2) litera (a) , şi nu există niciun alt temei juridic pentru prelucrarea;

c) persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (1) şi nu există motive legitime care să prevaleze în ceea ce priveşte prelucrarea sau persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (2) ;

d) datele cu caracter personal au fost prelucrate ilegal;

e) datele cu caracter personal trebuie şterse pentru respectarea unei obligaţii legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidenţa căruia se află operatorul;

f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societăţii informaţionale menţionate la articolul 8 alineatul (1) .

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

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

a) pentru exercitarea dreptului la liberă exprimare şi la informare;

b) pentru respectarea unei obligaţii legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorităţi oficiale cu care este învestit operatorul;

c) din motive de interes public în domeniul sănătăţii publice, în conformitate cu articolul 9 alineatul (2) literele (h) şi (i) şi cu articolul 9 alineatul (3) ;

d) în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1) , în măsura în care dreptul menţionat la alineatul (1) este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau

e) pentru constatarea, exercitarea sau apărarea unui drept în instanţă.

Art. 18: Dreptul la restricţionarea prelucrării

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

a) persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;

b) prelucrarea este ilegală, iar persoana vizată se opune ştergerii datelor cu caracter personal, solicitând în schimb restricţionarea utilizării lor;

c) operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanţă; sau

d) persoana vizată s-a opus prelucrării în conformitate cu articolul 21 alineatul (1) , pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

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

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

Art. 19: Obligaţia de notificare privind rectificarea sau ştergerea datelor cu caracter personal sau restricţionarea prelucrării

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

Art. 20: Dreptul la portabilitatea datelor

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

a) prelucrarea se bazează pe consimţământ în temeiul articolului 6 alineatul (1) litera (a) sau

al articolului 9 alineatul (2) litera (a) sau pe un contract în temeiul articolului 6 alineatul (1) litera (b) ; şi

b) prelucrarea este efectuată prin mijloace automate.

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

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

(4) Dreptul menţionat la alineatul (1) nu aduce atingere drepturilor şi libertăţilor altora.

Secţiunea 4: Dreptul la opoziţie şi procesul decizional individual automatizat

Art. 21: Dreptul la opoziţie

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

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

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

(4) Cel târziu în momentul primei comunicări cu persoana vizată, dreptul menţionat la alineatele (1) şi (2) este adus în mod explicit în atenţia persoanei vizate şi este prezentat în mod clar şi separat de orice alte informaţii.

(5) În contextual utilizării serviciilor societăţii informaţionale şi în pofida Directivei **2002/58/CE**, persoana vizată îşi poate exercita dreptul de a se opune prin mijloace automate care utilizează specificaţii tehnice.

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

Art. 22: Procesul decizional individual automatizat, inclusiv crearea de profiluri

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

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

a) este necesară pentru încheierea sau executarea unui contract între persoana vizată şi un operator de date;

b) este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului şi care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate; sau

c) are la bază consimţământul explicit al persoanei vizate.

(3) În cazurile menţionate la alineatul (2) literele (a) şi (c) , operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate, cel puţin dreptul acesteia de a obţine intervenţie umană din partea operatorului, de a-şi exprima punctul de vedere şi de a contesta decizia.

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

Secţiunea 5: Restricţii

Art. 23: Restricţii

(1) Dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricţiona printr-o măsură legislativă domeniul de aplicare al obligaţiilor şi al drepturilor prevăzute la articolele 12-22 şi 34, precum şi la articolul 5 în măsura în care dispoziţiile acestuia corespund drepturilor şi obligaţiilor prevăzute la articolele 12-22, atunci când o astfel de restricţie respectă esenţa drepturilor şi libertăţilor fundamentale şi constituie o măsură necesară şi proporţională într-o societate democratică, pentru a asigura:

a) securitatea naţională;

b) apărarea;

c) securitatea publică;

d) prevenirea, investigarea, depistarea sau urmărirea penală a infracţiunilor sau executarea sancţiunilor penale, inclusiv protejarea împotriva ameninţărilor la adresa securităţii publice şi prevenirea acestora;

e) alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar şi fiscal şi în domeniul sănătăţii publice şi al securităţii sociale;

f) protejarea independenţei judiciare şi a procedurilor judiciare;

g) prevenirea, investigarea, depistarea şi urmărirea penală a încălcării eticii în cazul profesiilor reglementate;

h) funcţia de monitorizare, inspectare sau reglementare legată, chiar şi ocazional, de exercitarea autorităţii oficiale în cazurile menţionate la literele (a) -(e) şi (g) ;

i) protecţia persoanei vizate sau a drepturilor şi libertăţilor altora; (j) punerea în aplicare a pretenţiilor de drept civil.

(2) În special, orice măsură legislativă menţionată la alineatul (1) conţine dispoziţii specifice cel puţin, dacă este cazul, în ceea ce priveşte:

a) scopurile prelucrării sau ale categoriilor de prelucrare;

b) categoriile de date cu caracter personal;

c) domeniul de aplicare al restricţiilor introduse;

d) garanţiile pentru a preveni abuzurile sau accesul sau transferul ilegal;

e) menţionarea operatorului sau a categoriilor de operatori;

f) perioadele de stocare şi garanţiile aplicabile având în vedere natura, domeniul de aplicare şi scopurile prelucrării sau ale categoriilor de prelucrare;

g) riscurile pentru drepturile şi libertăţilor persoanelor vizate; şi

h) dreptul persoanelor vizate de a fi informate cu privire la restricţie, cu excepţia cazului în care acest lucru poate aduce atingere scopului restricţiei.

CAPITOLUL IV: Operatorul şi persoana împuternicită de operator

Secţiunea 1: Obligaţii generale

Art. 24: Responsabilitatea operatorului

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

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

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

Art. 25: Asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit

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

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

(3) Un mecanism de certificare aprobat în conformitate cu articolul 42 poate fi utilizat drept element care să demonstreze îndeplinirea cerinţelor prevăzute la alineatele (1) şi (2) ale prezentului articol.

Art. 26: Operatori asociaţi

(1) În cazul în care doi sau mai mulţi operatori stabilesc în comun scopurile şi mijloacele de prelucrare, aceştia sunt operatori asociaţi. Ei stabilesc într-un mod transparent responsabilităţile fiecăruia în ceea ce priveşte îndeplinirea obligaţiilor care le revin în temeiul prezentului regulament, în special în ceea ce priveşte exercitarea drepturilor persoanelor vizate şi îndatoririle fiecăruia de furnizare a informaţiilor prevăzute la articolele 13 şi 14, prin intermediul unui acord între ei, cu excepţia cazului şi în măsura în care responsabilităţile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

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

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

Art. 27: Reprezentanţii operatorilor sau ai persoanelor împuternicite de operatori care nu îşi au sediul în Uniune

(1) În cazul în care se aplică articolul 3 alineatul (2) , operatorul sau persoana împuternicită de operator desemnează în scris un reprezentant în Uniune.

(2) Obligaţia prevăzută la alineatul (1) din prezentul articol nu se aplică:

a) prelucrării care are un caracter ocazional, care nu include, pe scară largă, prelucrarea unor categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1) , sau prelucrarea unor date cu caracter personal referitoare la condamnări penale şi infracţiuni menţionată la articolul 10, şi care este puţin susceptibilă de a genera un risc pentru drepturile şi libertăţile persoanelor, ţinând cont de natura, contextul, domeniul de aplicare şi scopurile prelucrării; sau

b) unei autorităţi sau unui organism public.

(3) Reprezentantul îşi are sediul în unul dintre statele membre în care se află persoanele vizate ale căror date cu caracter personal sunt prelucrate în legătură cu furnizarea de bunuri şi servicii sau al căror comportament este monitorizat.

(4) Reprezentantul primeşte din partea operatorului sau a persoanei împuternicite de operator un mandat prin care autorităţile de supraveghere şi persoanele vizate, în special, se pot adresa reprezentantului, în plus faţă de operator sau persoana împuternicită de operator sau în locul acestora, cu privire la toate chestiunile legate de prelucrarea, în scopul asigurării respectării prezentului regulament.

(5) Desemnarea unui reprezentant de către operator sau persoana împuternicită de operator nu aduce atingere acţiunilor în justiţie care ar putea fi introduse împotriva operatorului sau persoanei împuternicite de operator înseşi.

Art. 28: Persoana împuternicită de operator

(1) În cazul în care prelucrarea urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane împuternicite care oferă garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să respecte cerinţele prevăzute în prezentul regulament şi să asigure protecţia drepturilor persoanei vizate.

(2) Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizaţie scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizaţii generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecţii faţă de aceste modificări.

(3) Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul şi care stabileşte obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate şi

obligaţiile şi drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoană împuternicită de operator:

a) prelucrează datele cu caracter personal numai pe baza unor instrucţiuni documentate din partea operatorului, inclusiv în ceea ce priveşte transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, cu excepţia cazului în care această obligaţie îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligaţie juridică operatorului înainte de prelucrare, cu excepţia cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

b) se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidenţialitatea sau au o obligaţie statutară adecvată de confidenţialitate;

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

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

e) ţinând seama de natura prelucrării, oferă asistenţă operatorului prin măsuri tehnice şi organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligaţiei operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute în capitolul III;

f) ajută operatorul să asigure respectarea obligaţiilor prevăzute la articolele 32-36, ţinând seama de caracterul prelucrării şi informaţiile aflate la dispoziţia persoanei împuternicite de operator;

g) la alegerea operatorului, şterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare şi elimină copiile existente, cu excepţia cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;

h) pune la dispoziţia operatorului toate informaţiile necesare pentru a demonstra respectarea obligaţiilor prevăzute la prezentul articol, permite desfăşurarea auditurilor, inclusiv a inspecţiilor, efectuate de operator sau alt auditor mandatat şi contribuie la acestea. În ceea ce priveşte primul paragraf litera (h) , persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucţiune încalcă prezentul regulament sau alte dispoziţii din dreptul intern sau din dreptul Uniunii referitoare la protecţia datelor.

(4) În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activităţi de prelucrare specifice în numele operatorului, aceleaşi obligaţii privind protecţia datelor prevăzute în contractul sau în alt act juridic încheiat între operator şi persoana împuternicită de operator, astfel cum se prevede la alineatul (3) , revin celei de a doua persoane împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul dreptului Uniunii sau al dreptului intern, în special furnizarea de garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerinţele prezentului regulament. În cazul în care această a doua persoană împuternicită nu îşi respectă obligaţiile privind protecţia datelor, persoana împuternicită iniţială rămâne pe deplin răspunzătoare faţă de operator în ceea ce priveşte îndeplinirea obligaţiilor acestei a doua persoane împuternicite.

(5) Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, menţionat la articolul 40, sau la un mecanism de certificare aprobat, menţionat la articolul 42, poate fi utilizată ca element prin care să se demonstreze existenţa garanţiilor suficiente menţionate la alineatele (1) şi (4) din prezentul articol.

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

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

(8) O autoritate de supraveghere poate să adopte clauze contractuale standard pentru aspectele menţionate la alineatele (3) şi (4) din prezentul articol şi în conformitate cu mecanismul pentru asigurarea coerenţei menţionat la articolul 63.

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

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

Art. 29: Desfăşurarea activităţii de prelucrare sub autoritatea operatorului sau a persoanei împuternicite de operator

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

Art. 30: Evidenţele activităţilor de prelucrare

(1) Fiecare operator şi, după caz, reprezentantul acestuia păstrează o evidenţă a activităţilor de prelucrare desfăşurate sub responsabilitatea lor. Respectiva evidenţă cuprinde toate următoarele informaţii:

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

b) scopurile prelucrării;

c) o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;

d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;

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

f) acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date;

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

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

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

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

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

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

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

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

(5) Obligaţiile menţionate la alineatele 1 şi 2 nu se aplică unei întreprinderi sau organizaţii cu mai puţin de 250 de angajaţi, cu excepţia cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1) , sau date cu caracter personal referitoare la condamnări penale şi infracţiuni, astfel cum se menţionează la articolul 10.

Art. 31: Cooperarea cu autoritatea de supraveghere

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

Secţiunea 2: Securitatea datelor cu caracter personal

Art. 32: Securitatea prelucrării

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

a) pseudonimizarea şi criptarea datelor cu caracter personal;

b) capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare;

c) capacitatea de a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

d) un proces pentru testarea, evaluarea şi aprecierea periodice ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.

(2) La evaluarea nivelului adecvat de securitate, se ţine seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

(3) Aderarea la un cod de conduită aprobat, menţionat la articolul 40, sau la un mecanism de certificare aprobat, menţionat la articolul 42, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerinţelor prevăzute la alineatul (1) din prezentul articol.

(4) Operatorul şi persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator şi care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepţia cazului în care această obligaţie îi revine în temeiul dreptului Uniunii sau al dreptului intern.

Art. 33: Notificarea autorităţii de supraveghere în cazul încălcării securităţii datelor cu caracter personal

(1) În cazul în care are loc o încălcare a securităţii datelor cu caracter personal, operatorul notifică acest lucru autorităţii de supraveghere competente în temeiul articolului 55, fără întârzieri nejustificate şi, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta, cu excepţia cazului în care este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice. În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoţită de o explicaţie motivată din partea autorităţii de supraveghere în cazul în care.

(2) Persoana împuternicită de operator înştiinţează operatorul fără întârzieri nejustificate după ce ia cunoştinţă de o încălcare a securităţii datelor cu caracter personal.

(3) Notificarea menţionată la alineatul (1) cel puţin:

a) descrie caracterul încălcării securităţii datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile şi numărul aproximativ al persoanelor vizate în cauză, precum şi categoriile şi numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;

b) comunică numele şi datele de contact ale responsabilului cu protecţia datelor sau un alt punct de contact de unde se pot obţine mai multe informaţii;

c) descrie consecinţele probabile ale încălcării securităţii datelor cu caracter personal;

d) descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securităţii datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

(4) Atunci când şi în măsura în care nu este posibil să se furnizeze informaţiile în acelaşi timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

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

Art. 34: Informarea persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal

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

(2) În informarea transmisă persoanei vizate prevăzută la alineatul (1) din prezentul articol se include o descriere într-un limbaj clar şi simplu a caracterului încălcării securităţii datelor cu caracter

personal, precum şi cel puţin informaţiile şi măsurile menţionate la articolul 33 alineatul (3) literele (b) , (c) şi (d) .

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

a) operatorul a implementat măsuri de protecţie tehnice şi organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securităţii datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile şi libertăţile persoanelor vizate menţionat la alineatul (1) nu mai este susceptibil să se materializeze;

c) ar necesita un efort disproporţionat. În această situaţie, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

(4) În cazul în care operatorul nu a comunicat deja încălcarea securităţii datelor cu caracter personal către persoana vizată, autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securităţii datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condiţiile menţionate la alineatul (3) sunt îndeplinite.

Secţiunea 3: Evaluarea impactului asupra protecţiei datelor şi consultarea prealabilă

Art. 35: Evaluarea impactului asupra protecţiei datelor

(1) Având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal. O evaluare unică poate aborda un set de operaţiuni de prelucrare similare care prezintă riscuri ridicate similare.

(2) La realizarea unei evaluări a impactului asupra protecţiei datelor, operatorul solicită avizul responsabilului cu protecţia datelor, dacă acesta a fost desemnat.

(3) Evaluarea impactului asupra protecţiei datelor menţionată la alineatul (1) se impune mai ales în cazul:

a) unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

b) prelucrării pe scară largă a unor categorii speciale de date, menţionată la articolul 9 alineatul (1) , sau a unor date cu caracter personal privind condamnări penale şi infracţiuni, menţionată la articolul 10; sau

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

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

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

(6) Înainte de adoptarea listelor menţionate la alineatele (4) şi (5) , autoritatea de supraveghere competentă aplică mecanismul pentru asigurarea coerenţei menţionat la articolul 63 în cazul în care aceste liste implică activităţi de prelucrare care presupun furnizarea de bunuri sau prestarea de servicii către persoane vizate sau monitorizarea comportamentului acestora în mai multe state membre ori care pot afecta în mod substanţial libera circulaţie a datelor cu caracter personal în cadrul Uniunii.

(7) Evaluarea conţine cel puţin:

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

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

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

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

(8) La evaluarea impactului operaţiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevante, se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate menţionate la articolul 40, în special în vederea unei evaluări a impactului asupra protecţiei datelor.

(9) Operatorul solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanţilor acestora privind prelucrarea prevăzută, fără a aduce atingere protecţiei intereselor comerciale sau publice ori securităţii operaţiunilor de prelucrare.

(10) Atunci când prelucrarea în temeiul articolului 6 alineatul (1) litera (c) sau (e) are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidenţa căruia intră operatorul, iar dreptul respectiv reglementează operaţiunea de prelucrare specifică sau setul de operaţiuni specifice în cauză şi deja s-a efectuat o evaluare a impactului asupra protecţiei datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, alineatele (1) -(7) nu se aplică, cu excepţia cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfăşurării activităţilor de prelucrare.

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

Art. 36: Consultarea prealabilă

(1) Operatorul consultă autoritatea de supraveghere înainte de prelucrarea atunci când evaluarea impactului asupra protecţiei datelor prevăzută la articolul 35 indică faptul că prelucrarea ar genera un risc ridicat în absenţa unor măsuri luate de operator pentru atenuarea riscului.

(2) Atunci când consideră că prelucrarea prevăzută menţionată la alineatul (1) ar încălca prezentul regulament, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris operatorului şi, după caz, persoanei împuternicite de operator, în cel mult opt săptămâni de la primirea cererii de consultare, şi îşi poate utiliza oricare dintre competenţele menţionate la articolul 58. Această perioadă poate fi prelungită cu şase săptămâni, ţinându-se seama de complexitatea prelucrării prevăzute. Autoritatea de supraveghere informează operatorul şi, după caz, persoana împuternicită de operator, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când autoritatea de supraveghere a obţinut informaţiile pe care le-a solicitat în scopul consultării.

(3) Atunci când consultă autoritatea de supraveghere în conformitate cu alineatul (1) , operatorul îi furnizează acesteia:

a) dacă este cazul, responsabilităţile respective ale operatorului, ale operatorilor asociaţi şi ale persoanelor împuternicite de operator implicate în activităţile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;

b) scopurile şi mijloacele prelucrării preconizate;

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

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

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

f) orice alte informaţii solicitate de autoritatea de supraveghere.

(4) Statele membre consultă autoritatea de supraveghere în cadrul procesului de pregătire a unei propuneri de măsură legislativă care urmează să fie adoptată de un parlament naţional sau a unei măsuri de reglementare întemeiate pe o astfel de măsură legislativă, care se referă la prelucrarea.

(5) În pofida alineatului (1) , dreptul intern poate impune operatorilor să se consulte cu autoritatea de supraveghere şi să obţină în prealabil autorizarea din partea acesteia în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecţia socială şi sănătatea publică.

Secţiunea 4: Responsabilul cu protecţia datelor

Art. 37: Desemnarea responsabilului cu protecţia datelor

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

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

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

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

(2) Un grup de întreprinderi poate numi un responsabil cu protecţia datelor unic, cu condiţia ca responsabilul cu protecţia datelor să fie uşor accesibil din fiecare întreprindere.

(3) În cazul în care operatorul sau persoana împuternicită de operator este o autoritate publică sau un organism public, poate fi desemnat un responsabil cu protecţia datelor unic pentru mai multe dintre aceste autorităţi sau organisme, luând în considerare structura organizatorică şi dimensiunea acestora.

(4) În alte cazuri decât cele menţionate la alineatul (1) , operatorul sau persoana împuternicită de operator ori asociaţiile şi alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot desemna sau, acolo unde dreptul Uniunii sau dreptul intern solicită acest lucru, desemnează un responsabil cu protecţia datelor. Responsabilul cu protecţia datelor poate să acţioneze în favoarea unor astfel de asociaţii şi alte organisme care reprezintă operatori sau persoane împuternicite de operatori.

(5) Responsabilul cu protecţia datelor este desemnat pe baza calităţilor profesionale şi, în special, a cunoştinţelor de specialitate în dreptul şi practicile din domeniul protecţiei datelor, precum şi pe baza capacităţii de a îndeplini sarcinile prevăzute la articolul 39.

(6) Responsabilul cu protecţia datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să îşi îndeplinească sarcinile în baza unui contract de servicii.

(7) Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecţia datelor şi le comunică autorităţii de supraveghere.

Art. 38: Funcţia responsabilului cu protecţia datelor

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

(2) Operatorul şi persoana împuternicită de operator sprijină responsabilul cu protecţia datelor în îndeplinirea sarcinilor menţionate la articolul 39, asigurându-i resursele necesare pentru executarea acestor sarcini, precum şi accesarea datelor cu caracter personal şi a operaţiunilor de prelucrare, şi pentru menţinerea cunoştinţelor sale de specialitate.

(3) Operatorul şi persoana împuternicită de operator se asigură că responsabilul cu protecţia datelor nu primeşte niciun fel de instrucţiuni în ceea ce priveşte îndeplinirea acestor sarcini. Acesta nu este demis sau sancţionat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. Responsabilul cu protecţia datelor răspunde direct în faţa celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.

(4) Persoanele v izate pot contacta responsabilul cu protecţia datelor cu privire la toate chestiunile legate de prelucrarea datelor lor şi la exercitarea drepturilor lor în temeiul prezentului regulament.

(5) Responsabilul cu protecţia datelor are obligaţia de a respecta secretul sau confidenţialitatea în ceea ce priveşte îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.

(6) Responsabilul cu protecţia datelor poate îndeplini şi alte sarcini şi atribuţii. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini şi atribuţii nu generează un conflict de interese.

Art. 39: Sarcinile responsabilului cu protecţia datelor

(1) Responsabilul cu protecţia datelor are cel puţin următoarele sarcini:

a) informarea şi consilierea operatorului, sau a persoanei împuternicite de operator, precum şi a angajaţilor care se ocupă de prelucrare cu privire la obligaţiile care le revin în temeiul prezentului regulament şi al altor dispoziţii de drept al Uniunii sau drept intern referitoare la protecţia datelor;

b) monitorizarea respectării prezentului regulament, a altor dispoziţii de drept al Uniunii sau de drept intern referitoare la protecţia datelor şi a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce priveşte protecţia datelor cu caracter personal, inclusiv alocarea responsabilităţilor şi

acţiunile de sensibilizare şi de formare a personalului implicat în operaţiunile de prelucrare, precum şi auditurile aferente;

c) furnizarea de consiliere la cerere în ceea ce priveşte evaluarea impactului asupra protecţiei datelor şi monitorizarea funcţionării acesteia, în conformitate cu articolul 35;

d) cooperarea cu autoritatea de supraveghere;

e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menţionată la articolul 36, precum şi, dacă este cazul, consultarea cu privire la orice altă chestiune.

(2) În îndeplinirea sarcinilor sale, responsabilul cu protecţia datelor ţine seama în mod corespunzător de riscul asociat operaţiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul şi scopurile prelucrării.

Secţiunea 5: Coduri de conduită şi certificare

Art. 40: Coduri de conduită

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

(2) Asociaţiile şi alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot pregăti coduri de conduită sau le pot modifica sau extinde pe cele existente, în scopul de a specifica modul de aplicare a prezentului regulament, cum ar fi în ceea ce priveşte:

a) prelucrarea în mod echitabil şi transparent;

b) interesele legitime urmărite de operatori în contexte specifice;

c) colectarea datelor cu caracter personal;

d) pseudonimizarea datelor cu caracter personal;

e) informarea publicului şi a persoanelor vizate;

f) exercitarea drepturilor persoanelor vizate;

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

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

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

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

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

(3) La codurile de conduită aprobate în temeiul alineatului (5) din prezentul articol şi care au o valabilitate generală în temeiul alineatului (9) din prezentul articol pot adera nu numai operatorii sau persoanele împuternicite de operatori care fac obiectul prezentului regulament, ci şi operatorii sau persoanele împuternicite de operatori care nu fac obiectul prezentului regulament în temeiul articolului 3, în scopul de a oferi garanţii adecvate în cadrul transferurilor de date cu caracter personal către ţări terţe sau organizaţii internaţionale în condiţiile menţionate la articolul 46 alineatul (2) litera (e) . Aceşti operatori sau persoane împuternicite de operatori îşi asumă angajamente cu caracter obligatoriu şi executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, în scopul aplicării garanţiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.

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

(5) Asociaţiile şi alte organisme menţionate la alineatul (2) din prezentul articol care intenţionează să pregătească un cod de conduită sau să modifice sau să extindă un cod existent transmit proiectul de cod, de modificare sau de extindere autorităţii de supraveghere care este competentă în temeiul articolului 55. Autoritatea de supraveghere emite un aviz cu privire la conformitatea cu prezentul regulament a

proiectului de cod, de modificare sau de extindere şi îl aprobă în cazul în care se constată că acesta oferă garanţii adecvate suficiente.

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

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

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

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

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

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

Art. 41: Monitorizarea codurilor de conduită aprobate

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

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

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

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

c) a instituit proceduri şi structuri pentru tratarea plângerilor privind încălcări ale codului sau privind modul în care codul a fost sau este pus în aplicare de un operator sau o persoană împuternicită de operator, precum şi pentru asigurarea transparenţei acestor proceduri şi structuri pentru persoanele vizate şi pentru public; şi

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

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

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

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

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

Art. 42: Certificare

(1) Statele membre, autorităţile de supraveghere, comitetul şi Comisia încurajează, în special la nivelul Uniunii, instituirea de mecanisme de certificare în domeniul protecţiei datelor, precum şi de sigilii şi mărci în acest domeniu, care să permită demonstrarea faptului că operaţiunile de prelucrare efectuate de

operatori şi de persoanele împuternicite de operatori respectă prezentul regulament. Sunt luate în considerare necesităţile specifice ale microîntreprinderilor şi ale întreprinderilor mici şi mijlocii.

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

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

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

(5) Organismele de certificare menţionate la articolul 43 sau autoritatea de supraveghere competentă emit o certificare în temeiul prezentului articol, pe baza criteriilor aprobate de către autoritatea de supraveghere competentă respectivă în temeiul articolului 58 alineatul (3) , sau de către comitet în temeiul articolului 63. În cazul în care criteriile sunt aprobate de comitet, aceasta poate duce la o certificare comună, şi anume sigiliul european privind protecţia datelor.

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

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

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

Art. 43: Organisme de certificare

(1) Fără a aduce atingere sarcinilor şi competenţelor autorităţii de supraveghere competente, prevăzute la articolele 57 şi 58, organismele de certificare care dispun de un nivel adecvat de competenţă în domeniul protecţiei datelor, după ce informează autoritatea de supraveghere pentru a-i permite să îşi exercite competenţele în temeiul articolului 58 alineatul (2) litera (h) , emit şi reînnoiesc certificarea. Statele membre se asigură că aceste organisme de certificare sunt acreditate de către una sau amândouă dintre următoarele entităţi:

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

b) organismul naţional de acreditare desemnat în conformitate cu Regulamentul (CE) nr. **765/2008** al Parlamentului European şi al Consiliului (1) în conformitate cu standardul ENISO/ IEC 17065/2012 şi cu cerinţele suplimentare stabilite de autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56.

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

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

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

b) s-a angajat să respecte criteriile menţionate la articolul 42 alineatul (5) şi aprobate de autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56, sau de către comitet în temeiul articolului 63;

c) a instituit proceduri pentru emiterea, revizuirea periodică şi retragerea certificării, a sigiliilor şi mărcilor din domeniul protecţiei datelor;

d) a instituit proceduri şi structuri pentru tratarea plângerilor privind încălcări ale certificării sau privind modul în care certificarea a fost sau este pusă în aplicare de un operator sau o persoană împuternicită de operator, precum şi pentru asigurarea transparenţei acestor proceduri şi structuri pentru persoanele vizate şi pentru public; şi

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

(3) Acreditarea organismelor de certificare menţionate la alineatele (1) şi (2) din prezentul articol se realizează pe baza criteriilor aprobate de către autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56, sau de către comitet în temeiul articolului 63. În cazul unei acreditări în conformitate cu alineatul (1) litera (b) din prezentul articol, aceste cerinţe le completează pe cele prevăzute în Regulamentul (CE) nr. **765/2008** şi normele tehnice care descriu metodele şi procedurile organismelor de certificare.

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

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

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

(7) Fără a aduce atingere dispoziţiilor capitolului VIII, autoritatea de supraveghere competentă sau organismul naţional de acreditare revocă acreditarea acordată unui organism de certificare în temeiul alineatului (1) din prezentul articol în cazul în care nu sunt sau nu mai sunt îndeplinite condiţiile pentru acreditare sau măsurile luate de organismul de acreditare încalcă prezentul regulament.

(8) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 92, în scopul specificării cerinţelor care trebuie luate în considerare pentru mecanismele de certificare din domeniul protecţiei datelor, menţionate la articolul 42 alineatul (1) .

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

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

Art. 44: Principiul general al transferurilor

Orice date cu caracter personal care fac obiectul prelucrării sau care urmează a fi prelucrate după ce sunt transferate într-o ţară terţă sau către o organizaţie internaţională pot fi transferate doar dacă, sub rezerva celorlalte dispoziţii ale prezentului regulament, condiţiile prevăzute în prezentul capitol sunt respectate de operator şi de persoana împuternicită de operator, inclusiv în ceea ce priveşte transferurile ulterioare de date cu caracter personal din ţara terţă sau de la organizaţia internaţională către o altă ţară terţă sau către o altă organizaţie internaţională. Toate dispoziţiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecţie a persoanelor fizice garantat prin prezentul regulament nu este subminat.

Art. 45: Transferuri în temeiul unei decizii privind caracterul adecvat al nivelului de protecţie

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

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

a) statul de drept, respectarea drepturilor omului şi a libertăţilor fundamentale, legislaţia relevantă, atât generală, cât şi sectorială, inclusiv privind securitatea publică, apărarea, securitatea naţională şi

dreptul penal, precum şi accesul autorităţilor publice la datele cu caracter personal, precum şi punerea în aplicare a acestei legislaţii, normele de protecţie a datelor, normele profesionale şi măsurile de securitate, inclusiv normele privind transferul ulterior de date cu caracter personal către o altă ţară terţă sau organizaţie internaţională, care sunt respectate în ţara terţă respectivă sau în organizaţia internaţională respectivă, jurisprudenţa, precum şi existenţa unor drepturi efective şi opozabile ale persoanelor vizate şi a unor reparaţii efective pe cale administrativă şi judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate;

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

c) angajamentele internaţionale la care a aderat ţara terţă sau organizaţia internaţională în cauză sau alte obligaţii care decurg din convenţii sau instrumente obligatorii din punct de vedere juridic, precum şi din participarea acesteia la sisteme multilaterale sau regionale, mai ales în domeniul protecţiei datelor cu caracter personal.

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

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

(5) În cazul în care informaţiile disponibile dezvăluie, în special în urma revizuirii menţionate la alineatul (3) din prezentul articol, că o ţară terţă, un teritoriu sau un sector specificat din acea ţară terţă sau o organizaţie internaţională nu mai asigură un nivel de protecţie adecvat în sensul alineatului (2) din prezentul articol, Comisia, dacă este necesar, abrogă, modifică sau suspendă, prin intermediul unui act de punere în aplicare, decizia menţionată la alineatul (3) din prezentul articol fără efect retroactiv. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menţionată la articolul 93 alineatul (2) . Din motive imperioase de urgenţă, Comisia adoptă acte de punere în aplicare imediat aplicabile în conformitate cu procedura menţionată la articolul 93 alineatul (3) .

(6) Comisia iniţiază consultări cu ţara terţă sau organizaţia internaţională în vederea remedierii situaţiei care a stat la baza deciziei luate în conformitate cu alineatul (5) .

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

(8) Comisia publică în Jurnalul Oficial al Uniunii Europene şi pe site-ul său o listă a ţărilor terţe, a teritoriilor şi sectoarelor specificate dintr-o ţară terţă şi a organizaţiilor internaţionale în cazul cărora a decis că nivelul de protecţie adecvat este asigurat sau nu mai este asigurat.

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

Art. 46: Transferuri în baza unor garanţii adecvate

(1) În absenţa unei decizii în temeiul articolului 45 alineatul (3) , operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională numai dacă operatorul sau persoana împuternicită de operator a oferit garanţii adecvate şi cu condiţia să existe drepturi opozabile şi căi de atac eficiente pentru persoanele vizate.

(2) Garanţiile adecvate menţionate la alineatul 1 pot fi furnizate fără să fie nevoie de nicio autorizaţie specifică din partea unei autorităţi de supraveghere, prin:

a) un instrument obligatoriu din punct de vedere juridic şi executoriu între autorităţile sau organismele publice;

b) reguli corporatiste obligatorii în conformitate cu articolul 47;

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

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

e) un cod de conduită aprobat în conformitate cu articolul 40, însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a persoanei împuternicite de operator din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

f) un mecanism de certificare aprobat în conformitate cu articolul 42, însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a persoanei împuternicite de operator din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate.

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

a) clauze contractuale între operator sau persoana împuternicită de operator şi operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din ţara terţă sau organizaţia internaţională; sau

b) dispoziţii care urmează să fie incluse în acordurile administrative dintre autorităţile sau organismele publice, care includ drepturi opozabile şi efective pentru persoanele vizate.

(4) Autoritatea de supraveghere aplică mecanismul pentru asigurarea coerenţei menţionat la articolul 63, în cazurile menţionate la alineatul (3) din prezentul articol.

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

Art. 47: Reguli corporatiste obligatorii

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

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

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

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

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

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

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

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

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

e) drepturile persoanelor vizate în ceea ce priveşte prelucrarea şi mijloacele de exercitare a acestor drepturi, inclusiv dreptul de a nu face obiectul unor decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, în conformitate cu articolul 22, dreptul de a depune o plângere în faţa autorităţii de supraveghere competente şi în faţa instanţelor competente ale statelor membre, în conformitate cu articolul 79, precum şi dreptul de a obţine reparaţii şi, după caz, despăgubiri pentru încălcarea regulilor corporatiste obligatorii;

f) acceptarea de către operator sau de persoana împuternicită de operator, care îşi are sediul pe teritoriul unui stat membru, a răspunderii pentru orice încălcare a regulilor corporatiste obligatorii de către

orice membru în cauză care nu îşi are sediul în Uniune; operatorul sau persoana împuternicită de operator este exonerat(ă) de această răspundere, integral sau parţial, numai dacă dovedeşte că membrul respectiv nu a fost răspunzător de evenimentul care a cauzat prejudiciul;

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

h) sarcinile oricărui responsabil cu protecţia datelor desemnat în conformitate cu articolul 37 sau ale oricărei alte persoane sau entităţi însărcinate cu monitorizarea respectării regulilor corporatiste obligatorii în cadrul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, a activităţilor de formare şi a gestionării plângerilor;

i) procedurile de formulare a plângerilor;

j) mecanismele din cadrul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, menite să asigure verificarea conformităţii cu regulile corporatiste obligatorii. Aceste mecanisme includ auditurile privind protecţia datelor şi metodele de asigurare a acţiunilor corective menite să protejeze drepturile persoanei vizate. Rezultatele acestor verificări ar trebui să fie comunicate persoanei sau entităţii menţionate la litera (h) şi consiliului de administraţie al întreprinderii care exercită controlul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună şi ar trebui să fie puse la dispoziţia autorităţii de supraveghere competente, la cerere;

k) mecanismele de raportare şi înregistrare a modificărilor aduse regulilor şi de raportare a acestor modificări autorităţii de supraveghere;

l) mecanismul de cooperare cu autoritatea de supraveghere în vederea asigurării respectării regulilor de către orice membru al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, în special prin punerea la dispoziţia autorităţii de supraveghere a rezultatelor verificărilor cu privire la măsurile menţionate la punctul (j) ;

m) mecanismele de raportare către autoritatea de supraveghere competentă a oricăror cerinţe legale impuse unui membru al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună într-o ţară terţă care pot avea un efect advers considerabil asupra garanţiilor furnizate prin regulile corporatiste obligatorii; şi

n) formarea corespunzătoare în domeniul protecţiei datelor a personalului care are un acces permanent sau periodic la date cu caracter personal.

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

Art. 48: Transferurile sau divulgările de informaţii neautorizate de dreptul Uniunii

Orice hotărâre a unei instanţe sau a unui tribunal şi orice decizie a unei autorităţi administrative a unei ţări terţe care impun unui operator sau persoanei împuternicite de operator să transfere sau să divulge date cu caracter personal poate fi recunoscută sau executată în orice fel numai dacă se bazează pe un acord internaţional, cum ar fi un tratat de asistenţă judiciară reciprocă în vigoare între ţara terţă solicitantă şi Uniune sau un stat membru, fără a se aduce atingere altor motive de transfer în temeiul prezentului capitol.

Art. 49: Derogări pentru situaţii specifice

(1) În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie în conformitate cu articolul 45 alineatul (3) sau a unor garanţii adecvate în conformitate cu articolul 46, inclusiv a regulilor corporatiste obligatorii, un transfer sau un set de transferuri de date cu caracter personal către o ţară terţă sau o organizaţie internaţională poate avea loc numai în una dintre condiţiile următoare:

a) persoana vizată şi-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a fost informată asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizată ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecţie şi a unor garanţii adecvate;

b) transferul este necesar pentru executarea unui contract între persoana vizată şi operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;

c) transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator şi o altă persoană fizică sau juridică;

d) transferul este necesar din considerente importante de interes public;

e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanţă;

f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-şi exprima acordul;

g) transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau al dreptului intern, are scopul de a furniza informaţii publicului şi care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în măsura în care sunt îndeplinite condiţiile cu privire la consultare prevăzute de dreptul Uniunii sau de dreptul intern în acel caz specific.

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

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

(3) Alineatul (1) primul paragraf literele (a) , (b) şi (c) şi paragraful al doilea nu se aplică în cazul activităţilor desfăşurate de autorităţile publice în exercitarea competenţelor lor publice.

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

(5) În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie, dreptul Uniunii sau dreptul intern poate, din considerente importante de interes public, să stabilească în mod expres limite asupra transferului unor categorii specifice de date cu caracter personal către o ţară terţă sau o organizaţie internaţională. Statele membre notifică aceste dispoziţii Comisiei.

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

Art. 50: Cooperarea internaţională în domeniul protecţiei datelor cu caracter personal

În ceea ce priveşte ţările terţe şi organizaţiile internaţionale, Comisia şi autorităţile de supraveghere iau măsurile corespunzătoare pentru:

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

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

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

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

CAPITOLUL VI: Autorităţi de supraveghere independente

Secţiunea 1: Statutul independent

Art. 51: Autoritatea de supraveghere

(1) Fiecare stat membru se asigură că una sau mai multe autorităţi publice independente sunt responsabile de monitorizarea aplicării prezentului regulament, în vederea protejării drepturilor şi libertăţilor fundamentale ale persoanelor fizice în ceea ce priveşte prelucrarea şi în vederea facilitării liberei circulaţii a datelor cu caracter personal în cadrul Uniunii ("autoritatea de supraveghere") .

(2) Fiecare autoritate de supraveghere contribuie la aplicarea coerentă a prezentului regulament în întreaga Uniune. În acest scop, autorităţile de supraveghere cooperează atât între ele, cât şi cu Comisia, în conformitate cu capitolul VII.

(3) În cazul în care mai multe autorităţi de supraveghere sunt instituite într-un stat membru, acesta desemnează autoritatea de supraveghere care reprezintă autorităţile respective în cadrul comitetului şi instituie un mecanism prin care să asigure respectarea de către celelalte autorităţi a normelor privind mecanismul pentru asigurarea coerenţei prevăzut la articolul 63.

(4) Fiecare stat membru notifică Comisiei dispoziţiile de drept pe care le adoptă în temeiul prezentului capitol până la 25 mai 2018 şi, fără întârziere, orice modificare ulterioară pe care o aduce acestor dispoziţii.

Art. 52: Independenţă

(1) Fiecare autoritate de supraveghere beneficiază de independenţă deplină în îndeplinirea sarcinilor sale şi exercitarea competenţelor sale în conformitate cu prezentul regulament.

(2) Membrul sau membrii fiecărei autorităţi de supraveghere, în cadrul îndeplinirii sarcinilor şi al exercitării competenţelor sale (lor) în conformitate cu prezentul regulament, rămâne (rămân) independent (independenţi) de orice influenţă externă directă sau indirectă şi nici nu solicită, nici nu acceptă instrucţiuni de la o parte externă.

(3) Membrul sau membrii fiecărei autorităţi de supraveghere se abţin de la a întreprinde acţiuni incompatibile cu atribuţiile lor, iar pe durata mandatului, nu desfăşoară activităţi incompatibile, remunerate sau nu.

(4) Fiecare stat membru se asigură că fiecare autoritate de supraveghere beneficiază de resurse umane, tehnice şi financiare, de un sediu şi de infrastructura necesară pentru îndeplinirea sarcinilor şi exercitarea efectivă a competenţelor sale, inclusiv a celor care urmează să fie aplicate în contextul asistenţei reciproce, al cooperării şi al participării în cadrul comitetului.

(5) Fiecare stat membru se asigură că fiecare autoritate de supraveghere îşi selectează personalul propriu şi deţine personal propriu aflat sub conducerea exclusivă a membrului sau membrilor autorităţii de supraveghere respective.

(6) Fiecare stat membru se asigură că fiecare autoritate de supraveghere face obiectul unui control financiar care nu aduce atingere independenţei sale şi că dispune de bugete anuale distincte, publice, care pot face parte din bugetul general de stat sau naţional.

Art. 53: Condiţii generale aplicabile membrilor autorităţii de supraveghere

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

- de parlament;
- de guvern;
- de şeful statului; sau
- de un organism independent împuternicit să facă numiri în temeiul dreptului intern.

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

(3) Atribuţiile unui membru încetează în cazul expirării mandatului, în cazul demisiei sau pensionării din oficiu în conformitate cu dreptul intern relevant.

(4) Un membru poate fi demis doar în cazuri de abateri grave sau dacă nu mai îndeplineşte condiţiile necesare pentru îndeplinirea atribuţiilor sale.

Art. 54: Norme privind instituirea autorităţii de supraveghere

(1) Fiecare stat membru prevede, pe cale legislativă, următoarele:

a) instituirea fiecărei autorităţi de supraveghere;

b) calificările şi condiţiile de eligibilitate necesare pentru a fi numit în calitate de membru al fiecărei autorităţi de supraveghere;

c) normele şi procedurile pentru numirea membrului sau a membrilor fiecărei autorităţi de supraveghere;

d) durata mandatului membrului sau membrilor fiecărei autorităţi de supraveghere, de minimum patru ani, cu excepţia primei numiri după 24 mai 2016, din care o parte poate fi pe o perioadă mai scurtă în cazul în care acest lucru este necesar pentru a proteja independenţa autorităţii de supraveghere printr-o procedură de numiri eşalonate;

e) dacă şi de câte ori este eligibil pentru reînnoire mandatul membrului sau membrilor fiecărei autorităţi de supraveghere;

f) condiţiile care reglementează obligaţiile membrului sau membrilor şi ale personalului fiecărei autorităţi de supraveghere, interdicţii privind acţiunile, ocupaţiile şi beneficiile incompatibile cu acestea în cursul mandatului şi după încetarea acestuia, precum şi normele care reglementează încetarea contractului de angajare.

(2) Membrul sau membrii şi personalul fiecărei autorităţi de supraveghere au obligaţia, în conformitate cu dreptul Uniunii sau cu dreptul intern, de a respecta atât pe parcursul mandatului, cât şi după încetarea acestuia, secretul profesional în ceea ce priveşte informaţiile confidenţiale de care au luat cunoştinţă în cursul îndeplinirii sarcinilor sau al exercitării competenţelor lor. Pe durata mandatului lor, această obligaţie de păstrare a secretului profesional se aplică în special în ceea ce priveşte raportarea de către persoane fizice a încălcărilor prezentului regulament.

Secţiunea 2: Abilităţi, sarcini şi competenţe

Art. 55: Competenţa

(1) Fiecare autoritate de supraveghere are competenţa să îndeplinească sarcinile şi să exercite competenţele care îi sunt conferite în conformitate cu prezentul regulament pe teritoriul statului membru de care aparţine.

(2) În cazul în care prelucrarea este efectuată de autorităţi publice sau de organisme private care acţionează pe baza literei (c) sau (e) de la articolul 6 alineatul (1) , este autoritatea de supraveghere din statul membru respectiv. În astfel de cazuri, nu se aplică articolul 56.

(3) Autorităţile de supraveghere nu sunt competente să supravegheze operaţiunile de prelucrare ale instanţelor care acţionează în exerciţiul funcţiei lor judiciare.

Art. 56: Competenţa autorităţii de supraveghere principale

(1) Fără a aduce atingere articolului 55, autoritatea de supraveghere a sediului principal sau a sediului unic al operatorului sau al persoanei împuternicite de operator este competentă să acţioneze în calitate de autoritate de supraveghere principală pentru prelucrarea transfrontalieră efectuată de respectivul operator sau respectiva persoană împuternicită în cauză în conformitate cu procedura prevăzută la articolul 60.

(2) Prin derogare de la alineatul (1) , fiecare autoritate de supraveghere este competentă să

trateze o plângere depusă în atenţia sa sau o eventuală încălcare a prezentului regulament, în cazul în care obiectul acesteia se referă numai la un sediu aflat în statul său membru sau afectează în mod semnificativ persoane vizate numai în statul său membru.

(3) În cazurile menţionate la alineatul (2) din prezentul articol, autoritatea de supraveghere informează fără întârziere autoritatea de supraveghere principală cu privire la această chestiune. În termen de trei săptămâni de la momentul informării, autoritatea de supraveghere principală decide dacă tratează sau nu cazul respectiv în conformitate cu procedura prevăzută la articolul 60, luând în considerare dacă există sau nu un sediu al operatorului sau al persoanei împuternicite de operator pe teritoriul statului membru a cărui autoritate de supraveghere a informat-o.

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

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

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

Art. 57: Sarcini

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

a) monitorizează şi asigură aplicarea prezentului regulament;

b) promovează acţiuni de sensibilizare şi de înţelegere în rândul publicului a riscurilor, normelor, garanţiilor şi drepturilor în materie de prelucrare. Se acordă atenţie specială activităţilor care se adresează în mod specific copiilor;

c) oferă consiliere, în conformitate cu dreptul intern, parlamentului naţional, guvernului şi altor instituţii şi organisme cu privire la măsurile legislative şi administrative referitoare la protecţia drepturilor şi libertăţilor persoanelor fizice în ceea ce priveşte prelucrarea;

d) promovează acţiuni de sensibilizare a operatorilor şi a persoanelor împuternicite de aceştia cu privire la obligaţiile care le revin în temeiul prezentului regulament;

e) la cerere, furnizează informaţii oricărei persoane vizate în legătură cu exercitarea drepturilor sale în conformitate cu prezentul regulament şi, dacă este cazul, cooperează cu autorităţile de supraveghere din alte state membre în acest scop;

f) tratează plângerile depuse de o persoană vizată, un organism, o organizaţie sau o asociaţie în conformitate cu articolul 80 şi investighează într-o măsură adecvată obiectul plângerii şi informează reclamantul cu privire la evoluţia şi rezultatul investigaţiei, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigaţii mai amănunţite sau coordonarea cu o altă autoritate de supraveghere;

g) cooperează, inclusiv prin schimb de informaţii, cu alte autorităţi de supraveghere şi îşi oferă asistenţă reciprocă pentru a asigura coerenţa aplicării şi respectării prezentului regulament;

h) desfăşoară investigaţii privind aplicarea prezentului regulament, inclusiv pe baza unor informaţii primite de la o altă autoritate de supraveghere sau de la o altă autoritate publică;

i) monitorizează evoluţiile relevante, în măsura în care acestea au impact asupra protecţiei datelor cu caracter personal, în special evoluţia tehnologiilor informaţiei şi comunicaţiilor şi a practicilor comerciale;

j) adoptă clauze contractuale standard menţionate la articolul 28 alineatul (8) şi la articolul 46 alineatul (2) litera (d) ;

k) întocmeşte şi menţine la zi o listă în legătură cu cerinţa privind evaluarea impactului asupra protecţiei datelor, în conformitate cu articolul 35 alineatul (4) ;

l) oferă consiliere cu privire la operaţiunile de prelucrare menţionate la articolul 36 alineatul (2) ;

m) încurajează elaborarea de coduri de conduită în conformitate cu articolul 40 alineatul (1) , îşi dă avizul cu privire la acestea şi le aprobă pe cele care oferă suficiente garanţii, în conformitate cu articolul 40 alineatul (5) ;

n) încurajează stabilirea unor mecanisme de certificare, precum şi a unor sigilii şi mărci în domeniul protecţiei datelor în conformitate cu articolul 42 alineatul (1) şi aprobă criteriile de certificare în conformitate cu articolul 42 alineatul (5) ;

o) acolo unde este cazul, efectuează o revizuire periodică a certificărilor acordate, în conformitate cu articolul 42 alineatul (7) ;

p) elaborează şi publică criteriile de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu articolul 41 şi a unui organism de certificare în conformitate cu articolul 43;

q) coordonează procedura de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu articolul 41 şi a unui organism de certificare în conformitate cu articolul 43;

r) autorizează clauzele şi dispoziţiile contractuale menţionate la articolul 46 alineatul (3) ;

s) aprobă regulile corporatiste obligatorii în conformitate cu articolul 47;

t) contribuie la activităţile comitetului;

u) menţine la zi evidenţe interne privind încălcările prezentului regulament şi măsurile luate, în special avertismentele emise şi sancţiunile impuse în conformitate cu articolul 58 alineatul (2) ; şi

v) îndeplineşte orice alte sarcini legate de protecţia datelor cu caracter personal.

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

(3) Îndeplinirea sarcinilor fiecărei autorităţi de supraveghere este gratuită pentru persoana vizată şi, după caz, pentru responsabilul cu protecţia datelor.

(4) În cazul în care cererile sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, autoritatea de supraveghere poate percepe o taxă rezonabilă, bazată pe costurile administrative, sau poate refuza să le trateze. Sarcina de a demonstra caracterul evident nefondat sau excesiv al cererii revine autorităţii de supraveghere.

Art. 58: Competenţe

(1) Fiecare autoritate de supraveghere are toate următoarele competenţe de investigare:

a) de a da dispoziţii operatorului şi persoanei împuternicite de operator şi, după caz, reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informaţii pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale;

b) de a efectua investigaţii sub formă de audituri privind protecţia datelor;

c) de a efectua o revizuire a certificărilor acordate în temeiul articolului 42 alineatul (7) ;

d) de a notifica operatorul sau persoana împuternicită de operator cu privire la presupusa încălcare a prezentului regulament;

e) de a obţine, din partea operatorului şi a persoanei împuternicite de operator, accesul la toate datele cu caracter personal şi la toate informaţiile necesare pentru îndeplinirea sarcinilor sale;

f) de a obţine accesul la oricare dintre incintele operatorului şi ale persoanei împuternicite de operator, inclusiv la orice echipamente şi mijloace de prelucrare a datelor, în conformitate cu dreptul Uniunii sau cu dreptul procesual intern.

(2) Fiecare autoritate de supraveghere are toate următoarele competenţe corective:

a) de a emite avertizări în atenţia unui operator sau a unei persoane împuternicite de operator cu privire la posibilitatea ca operaţiunile de prelucrare prevăzute să încalce dispoziţiile prezentului regulament;

b) de a emite mustrări adresate unui operator sau unei persoane împuternicite de operator în cazul în care operaţiunile de prelucrare au încălcat dispoziţiile prezentului regulament;

c) de a da dispoziţii operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-şi exercita drepturile în temeiul prezentului regulament;

d) de a da dispoziţii operatorului sau persoanei împuternicite de operator să asigure conformitatea operaţiunilor de prelucrare cu dispoziţiile prezentului regulament, specificând, după caz, modalitatea şi termenul-limită pentru aceasta;

e) de a obliga operatorul să informeze persoana vizată cu privire la o încălcare a protecţiei datelor cu caracter personal;

f) de a impune o limitare temporară sau definitivă, inclusiv o interdicţie asupra prelucrării;

g) de a dispune rectificarea sau ştergerea datelor cu caracter personal sau restricţionarea prelucrării, în temeiul articolelor 16, 17 şi 18, precum şi notificarea acestor acţiuni destinatarilor cărora le-au fost divulgate datele cu caracter personal, în conformitate cu articolul 17 alineatul (2) şi cu articolul 19;

h) de a retrage o certificare sau de a obliga organismul de certificare să retragă o certificare eliberată în temeiul articolul 42 şi 43 sau de a obliga organismul de certificare să nu elibereze o certificare în cazul în care cerinţele de certificare nu sunt sau nu mai sunt îndeplinite;

i) de a impune amenzi administrative în conformitate cu articolul 83, în completarea sau în locul măsurilor menţionate la prezentul alineat, în funcţie de circumstanţele fiecărui caz în parte;

j) de a dispune suspendarea fluxurilor de date către un destinatar dintr-o ţară terţă sau către o organizaţie internaţională.

(3) Fiecare autoritate de supraveghere are toate următoarele competenţe de autorizare şi de consiliere:

a) de a oferi consiliere operatorului în conformitate cu procedura de consultare prealabilă menţionată la articolul 36;

b) de a emite avize, din proprie iniţiativă sau la cerere, parlamentului naţional, guvernului statului membru sau, în conformitate cu dreptul intern, altor instituţii şi organisme, precum şi publicului, cu privire la orice aspect legat de protecţia datelor cu caracter personal;

c) de a autoriza prelucrarea menţionată la articolul 36 alineatul (5) , în cazul în care dreptul statului membru prevede o astfel de autorizare prealabilă;

d) de a emite un aviz şi de a aproba proiectele de coduri de conduită, în conformitate cu articolul 40 alineatul (5) ;

e) de a acredita organismele de certificare în conformitate cu articolul 43;

f) de a emite certificări şi de a aproba criterii de certificare în conformitate cu articolul 42 alineatul (5) ;

g) de a adopta clauzele standard în materie de protecţie a datelor menţionate la articolul 28 alineatul (8) şi la articolul 46 alineatul (2) litera (d) ;

h) de a autoriza clauzele contractuale menţionate la articolul 46 alineatul (3) litera (a) ;

i) de a autoriza acordurile administrative menţionate la articolul 46 alineatul (3) litera (b) ; şi

j) de a aproba reguli corporatiste obligatorii în conformitate cu articolul 47.

(4) Exercitarea competenţelor conferite autorităţii de supraveghere în temeiul prezentului articol face obiectul unor garanţii adecvate, inclusiv căi de atac judiciare eficiente şi procese echitabile, prevăzute în dreptul Uniunii şi în dreptul intern în conformitate cu **carta**.

(5) Fiecare stat membru prevede, pe cale legislativă, faptul că autoritatea sa de supraveghere are competenţa de a aduce în faţa autorităţilor judiciare cazurile de încălcare a prezentului regulament şi, după caz, de a iniţia sau de a se implica într-un alt mod în proceduri judiciare, în scopul de a asigura aplicarea dispoziţiilor prezentului regulament.

(6) Fiecare stat membru poate să prevadă în dreptul său faptul că autoritatea sa de supraveghere are competenţe suplimentare, în afara celor menţionate la alineatele (1) , (2) şi

(3) . Exercitarea acestor competenţe nu afectează modul de operare eficientă a capitolului VII.

Art. 59: Rapoarte de activitate

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

CAPITOLUL VII: Cooperare şi coerenţă

Secţiunea 1: Cooperare

Art. 60: Cooperarea dintre autoritatea de supraveghere principală şi celelalte autorităţi de supraveghere vizate

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

(2) Autoritatea de supraveghere principală poate solicita în orice moment altor autorităţi de supraveghere vizate să ofere asistenţă reciprocă în temeiul articolului 61 şi poate desfăşura operaţiuni comune în temeiul articolului 62, în special în vederea efectuării de investigaţii sau a monitorizării punerii în aplicare a unei măsuri referitoare la un operator sau o persoană împuternicită de operator, stabilit(ă) în alt stat membru.

(3) Autoritatea de supraveghere principală comunică fără întârziere informaţiile relevante referitoare la această chestiune celorlalte autorităţi de supraveghere vizate. Autoritatea de supraveghere principală transmite fără întârziere un proiect de decizie celorlalte autorităţi de supraveghere vizate, pentru a obţine avizul lor, şi ţine seama în mod corespunzător de opiniile acestora.

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

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

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

(7) Autoritatea de supraveghere principală adoptă decizia şi o notifică sediului principal sau sediului unic al operatorului sau al persoanei împuternicite de operator, după caz, şi informează celelalte autorităţi de supraveghere vizate şi comitetul cu privire la decizia în cauză, incluzând un rezumat al elementelor şi motivelor relevante. Autoritatea de supraveghere la care a fost depusă plângerea informează reclamantul cu privire la decizie.

(8) Prin derogare de la alineatul (7) , în cazul în care o plângere este refuzată sau respinsă, autoritatea de supraveghere la care s-a depus plângerea adoptă decizia, o notifică reclamantului şi informează operatorul cu privire la acest lucru.

(9) În cazul în care autoritatea de supraveghere principală şi autorităţile de supraveghere vizate sunt de acord să refuze sau să respingă anumite părţi ale unei plângeri şi să dea curs altor părţi ale plângerii respective, se adoptă o decizie separată pentru fiecare dintre aceste părţi. Autoritatea de supraveghere principală adoptă decizia pentru partea care vizează acţiunile referitoare la operator, o notifică sediului principal sau sediului unic al operatorului sau al persoanei împuternicite de operator de pe teritoriul statului membru în cauză şi informează reclamantul cu privire la acest lucru, în timp ce autoritatea de supraveghere a reclamantului adoptă decizia pentru partea care vizează refuzarea sau respingerea

plângerii respective, o notifică reclamantului şi informează operatorul sau persoana împuternicită de operator cu privire la acest lucru.

(10) În urma notificării deciziei autorităţii de supraveghere principale în temeiul alineatelor (7) şi (9) , operatorul sau persoana împuternicită de operator ia măsurile necesare pentru a se asigura că activităţile de prelucrare sunt în conformitate cu decizia în toate sediile sale din Uniune. Operatorul sau persoana împuternicită de operator notifică măsurile luate în vederea respectării deciziei autorităţii de supraveghere principale, care informează celelalte autorităţi de supraveghere vizate.

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

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

Art. 61: Asistenţă reciprocă

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

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

(3) Cererile de asistenţă cuprind toate informaţiile necesare, inclusiv scopul cererii şi motivele care stau la baza acesteia. Informaţiile care fac obiectul schimbului se utilizează numai în scopul în care au fost solicitate.

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

a) nu are competenţă privind obiectul cererii sau măsurile pe care este solicitată să le execute; sau

b) a da curs cererii ar încălca prezentul regulament sau dreptul Uniunii sau dreptului intern sub incidenţa căruia intră autoritatea de supraveghere care a primit cererea.

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

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

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

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

(9) Comisia, printr-un act de punere în aplicare, poate specifica forma şi procedurile pentru asistenţa reciprocă menţionată în prezentul articol, precum şi modalităţile de schimb de informaţii pe cale electronică între autorităţile de supraveghere şi între autorităţile de supraveghere şi comitet, în special formularul standard menţionat la alineatul (6) din prezentul articol. Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menţionată la articolul 93 alineatul (2) .

Art. 62: Operaţiuni comune ale autorităţilor de supraveghere

(1) După caz, autorităţile de supraveghere desfăşoară operaţiuni comune, inclusiv investigaţii comune şi măsuri comune de aplicare a legii, în care sunt implicaţi membri sau personal din autorităţile de supraveghere ale altor state membre.

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

(3) O autoritate de supraveghere poate, în conformitate cu dreptul intern şi cu acordul autorităţii de supraveghere din statul membru de origine, să acorde competenţe, inclusiv competenţe de investigare, membrilor sau personalului autorităţii de supraveghere din statul membru de origine implicaţi în operaţiuni comune sau, în măsura în care dreptul statului membru al autorităţii de supraveghere din statul membru de primire permite acest lucru, poate autoriza membrii sau personalul autorităţii de supraveghere din statul membru de origine să îşi exercite competenţele de investigare în conformitate cu dreptul statului membru al acestei din urmă autorităţi. Astfel de competenţe de investigare pot fi exercitate doar sub coordonarea şi în prezenţa membrilor sau personalului autorităţii de supraveghere din statul membru de primire. Membrii sau personalul autorităţii de supraveghere din statul membru de origine sunt supuşi dreptului intern sub incidenţa căruia intră autoritatea de supraveghere din statul membru de primire.

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

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

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

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

Secţiunea 2: Asigurarea coerenţei

Art. 63: Mecanismul pentru asigurarea coerenţei

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

Art. 64: Avizul comitetului

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

a) vizează adoptarea unei liste de operaţiuni de prelucrare care fac obiectul cerinţei de efectuare a unei evaluări a impactului asupra protecţiei datelor, în conformitate cu articolul 35 alineatul (4) ;

b) în conformitate cu articolul 40 alineatul (7) , se referă la conformitatea cu prezentul regulament a unui proiect de cod de conduită sau a unei modificări sau extinderi a unui cod de conduită;

c) vizează aprobarea criteriilor pentru acreditarea unui organism în conformitate cu articolul 41 alineatul (3) sau a unui organism de certificare în conformitate cu articolul 43 alineatul (3) ;

d) vizează determinarea clauzelor standard în materie de protecţie a datelor menţionate la articolul 46 alineatul (2) litera (d) sau la articolul 28 alineatul (8) ;

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

sau

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

(2) Orice autoritate de supraveghere, preşedintele comitetului sau Comisia poate solicita ca orice chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru să fie examinată de comitet în vederea obţinerii unui aviz, în special în cazul în care o autoritate de supraveghere competentă nu respectă obligaţiile privind asistenţa reciprocă în conformitate cu articolul 61 sau privind operaţiunile comune în conformitate cu articolul 62.

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

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

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

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

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

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

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

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

Art. 65: Soluţionarea litigiilor de către comitet

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

a) atunci când, în unul dintre cazurile menţionate la articolul 60 alineatul (4) , o autoritate de supraveghere vizată a formulat o obiecţie relevantă şi motivată la un proiect de decizie a autorităţii principale sau autoritatea principală a respins o astfel de obiecţie ca nefiind relevantă sau motivată. Decizia obligatorie se referă la toate chestiunile vizate de obiecţia relevantă şi motivată, în special la chestiunea dacă prezentul regulament a fost încălcat;

b) în cazul în care există opinii divergente cu privire la care dintre autorităţile de supraveghere vizate deţine competenţa pentru sediul principal;

c) în cazul în care o autoritate de supraveghere competentă nu solicită avizul comitetului în cazurile menţionate la articolul 64 alineatul (1) sau nu ţine seama de avizul comitetului emis în temeiul articolului 64. În acest caz, orice autoritate de supraveghere vizată sau Comisia poate comunica chestiunea comitetului.

(2) Decizia menţionată la alineatul (1) se adoptă în termen de o lună de la prezentarea chestiunii, cu o majoritate de două treimi a membrilor comitetului. Acest termen poate fi prelungit cu o lună, ţinându-se seama de complexitatea chestiunii. Decizia menţionată la alineatul (1) se motivează şi se adresează autorităţii de supraveghere principale şi tuturor autorităţilor de supraveghere vizate, fiind obligatorie pentru acestea.

(3) În cazul în care comitetul nu a fost în măsură să adopte o decizie în termenele menţionate la alineatul (2) , acesta îşi adoptă decizia în termen de două săptămâni de la data expirării celei de a doua luni menţionate la alineatul (2) , cu o majoritate simplă a membrilor săi. În cazul în care membrii comitetului au opinii divergente în proporţii egale, decizia se adoptă prin votul preşedintelui.

(4) Autorităţile de supraveghere vizate nu adoptă o decizie asupra chestiunii prezentate comitetului în conformitate cu alineatul (1) în termenele menţionate la alineatele (2) şi (3) .

(5) Preşedintele comitetului notifică, fără întârzieri nejustificate, decizia menţionată la alineatul (1) autorităţilor de supraveghere vizate. Comitetul informează Comisia cu privire la acest lucru. Decizia se publică pe site-ul comitetului, fără întârziere, după notificarea de către autoritatea de supraveghere a deciziei finale menţionate la alineatul (6) .

(6) Autoritatea de supraveghere principală sau, dacă este cazul, autoritatea de supraveghere la care s-a depus plângerea îşi adoptă decizia finală pe baza deciziei menţionate la alineatul (1) din prezentul articol, fără întârziere nejustificată şi în termen de cel mult o lună de la notificarea de către comitet a deciziei sale. Autoritatea de supraveghere principală sau, dacă este cazul, autoritatea de supraveghere la care s-a depus plângerea informează comitetul cu privire la data la care decizia sa finală este notificată operatorului sau persoanei împuternicite de operator şi, respectiv, persoanei vizate. Decizia finală a autorităţilor de supraveghere vizate se adoptă în conformitate cu condiţiile prevăzute la articolul 60 alineatele (7) , (8) şi

(9) . Decizia finală se referă la decizia menţionată la alineatul (1) din prezentul articol şi precizează faptul că decizia menţionată la respectivul alineat va fi publicată pe site-ul al comitetului, în conformitate cu alineatul (5) . La decizia finală se anexează decizia menţionată la alineatul (1) din prezentul articol.

Art. 66: Procedura de urgenţă

(1) În circumstanţe excepţionale, atunci când o autoritate de supraveghere vizată consideră că există o necesitate urgentă de a acţiona în scopul protejării drepturilor şi libertăţilor persoanelor vizate, aceasta poate, prin derogare de la mecanismul pentru asigurarea coerenţei menţionat la articolele 63, 64 şi 65 sau de la procedura menţionată la articolul 60, să adopte de îndată măsuri provizorii menite să producă efecte juridice pe propriul său teritoriu, cu o perioadă de valabilitate determinată, care să nu depăşească trei luni.

Autoritatea de supraveghere comunică fără întârziere aceste măsuri şi motivele adoptării lor celorlalte autorităţi de supraveghere vizate, comitetului şi Comisiei.

(2) În cazul în care o autoritate de supraveghere a adoptat o măsură în temeiul alineatului (1) şi consideră că este necesară adoptarea de urgenţă a unor măsuri definitive, aceasta poate solicita un aviz de urgenţă sau o decizie obligatorie urgentă din partea comitetului, indicând motivele pentru această solicitare.

(3) Orice autoritate de supraveghere poate solicita un aviz de urgenţă sau o decizie obligatorie urgentă, după caz, din partea comitetului în cazul în care o autoritate de supraveghere competentă nu a luat o măsură adecvată într-o situaţie în care există o necesitate urgentă de a acţiona pentru a proteja drepturile şi libertăţile persoanelor vizate, indicând motivele pentru solicitarea unui astfel de aviz sau a unei astfel de decizii, inclusiv pentru necesitatea urgentă de a acţiona.

(4) Prin derogare de la articolul 64 alineatul (3) şi de la articolul 65 alineatul (2) , un aviz de urgenţă sau o decizie obligatorie urgentă menţionat(ă) la alineatele (2) şi (3) de la prezentul articol este adoptat(ă) în termen de două săptămâni cu majoritate simplă a membrilor comitetului.

Art. 67: Schimb de informaţii

Comisia poate adopta acte de punere în aplicare cu un domeniu de aplicare general pentru a defini modalităţile de realizare a schimbului electronic de informaţii între autorităţile de supraveghere, precum şi între autorităţile de supraveghere şi comitet, în special formularul standard menţionat la articolul 64.

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

Secţiunea 3: Comitetul european pentru protecţia datelor

Art. 68: Comitetul european pentru protecţia datelor

(1) Comitetul european pentru protecţia datelor ("comitetul") este instituit ca organ al Uniunii şi are personalitate juridică.

(2) Comitetul este reprezentat de preşedintele său.

(3) Comitetul este alcătuit din şeful unei autorităţi de supraveghere din fiecare stat membru şi din Autoritatea Europeană pentru Protecţia Datelor sau reprezentanţii respectivi ai acestora.

(4) În cazul în care într-un stat membru mai multe autorităţi de supraveghere sunt responsabile de monitorizarea aplicării dispoziţiilor adoptate în temeiul prezentului regulament, se numeşte un reprezentant comun în conformitate cu dreptul intern al statului membru respectiv.

(5) Comisia are dreptul de a participa la activităţile şi reuniunile comitetului fără a avea drept de vot. Comisia numeşte un reprezentant. Preşedintele comitetului comunică Comisiei activităţile comitetului.

(6) În cazurile menţionate la articolul 65, Autoritatea Europeană pentru Protecţia Datelor deţine drept de vot numai cu privire la deciziile care privesc principiile şi normele aplicabile în ceea ce priveşte

instituţiile, organismele, oficiile şi agenţiile Uniunii care corespund pe fond cu cele din prezentul regulament.

Art. 69: Independenţă

(1) Comitetul acţionează independent în îndeplinirea sarcinilor sale sau în exercitarea competenţelor sale în conformitate cu articolele 70 şi 71.

(2) Fără a aduce atingere solicitărilor din partea Comisiei menţionate la articolul 70 alineatul (1) litera (b) şi la articolul 70 alineatul (2) , comitetul, în îndeplinirea sarcinilor sale sau în exercitarea competenţelor sale, nu solicită şi nu acceptă instrucţiuni de la nicio parte externă.

Art. 70: Sarcinile comitetului

(1) Comitetul asigură aplicarea coerentă a prezentului regulament. În acest scop, din proprie iniţiativă sau, după caz, la solicitarea Comisiei, comitetul are, în special, următoarele sarcini:

a) să monitorizeze şi să asigure aplicarea corectă a prezentului regulament, în cazurile prevăzute la articolele 64 şi 65, fără a aduce atingere sarcinilor autorităţilor naţionale de supraveghere;

b) să ofere consiliere Comisiei cu privire la orice aspect legat de protecţia datelor cu caracter personal în cadrul Uniunii, inclusiv cu privire la orice propunere de modificare a prezentului regulament;

c) să ofere consiliere Comisiei cu privire la formatul şi procedurile pentru schimbul de informaţii între operatori, persoanele împuternicite de operatori şi autorităţile de supraveghere pentru regulile corporatiste obligatorii;

d) să emită orientări, recomandări şi bune practici privind procedurile de ştergere a linkurilor către datele cu caracter personal, a copiilor sau a reproducerilor acestora de care dispun serviciile de comunicaţii accesibile publicului, astfel cum se menţionează la articolul 17 alineatul (2) ;

e) să examineze, din proprie iniţiativă, la cererea unuia dintre membrii săi sau la cererea Comisiei, orice chestiune referitoare la aplicarea prezentului regulament şi să emită orientări, recomandări şi bune practici pentru a încuraja aplicarea coerentă a prezentului regulament;

f) să emită orientări, recomandări şi bune practici în conformitate cu prezentul alineat litera (e) în vederea detalierii criteriilor şi condiţiilor pentru deciziile bazate pe crearea de profiluri menţionate la articolul 22 alineatul (2) ;

g) să emită orientări, recomandări şi bune practici în conformitate cu litera (e) din prezentul alineat pentru stabilirea încălcării securităţii datelor cu caracter personal şi stabilirii întârzierilor nejustificate menţionate la articolul 33 alineatele (1) şi (2) , precum şi pentru circumstanţele speciale în care un operator sau o persoană împuternicită de către operator are obligaţia de a notifica încălcarea securităţii datelor cu caracter personal;

h) să emită orientări, recomandări şi bune practici în conformitate cu litera (e) din prezentul alineat în ceea ce priveşte circumstanţele în care o încălcare a securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, menţionate la articolul 34 alineatul (1) ;

i) să emită orientări, recomandări şi bune practici în conformitate cu litera (e) din prezentul alineat în scopul detalierii criteriilor şi cerinţelor aplicabile transferurilor de date cu caracter personal bazate pe regulile corporatiste obligatorii care trebuie respectate de operatori şi cele care trebuie respectate de persoanele împuternicite de operatori, precum şi cu privire la cerinţe suplimentare necesare pentru a asigura protecţia datelor cu caracter personal ale persoanelor vizate menţionate la articolul 47;

j) să emită orientări, recomandări şi bune practici în conformitate cu litera (e) din prezentul alineat în vederea detalierii criteriilor şi cerinţelor pentru transferurile de date cu caracter personal menţionate la articolul 49 alineatul (1) ;

k) să elaboreze orientări destinate autorităţilor de supraveghere, referitoare la aplicarea măsurilor menţionate la articolul 58 alineatele (1) , (2) şi (3) şi să stabilească amenzile administrative în conformitate cu articolul 83;

l) să revizuiască aplicarea practică a orientărilor, recomandărilor şi bunelor practici menţionate la literele (e) şi (f) ;

m) să emită orientări, recomandări şi bune practici în conformitate cu litera (e) din prezentul alineat în vederea stabilirii procedurilor comune de raportare de către persoanele fizice a încălcărilor prezentului regulament în conformitate cu articolul 54 alineatul (2) ;

n) să încurajeze elaborarea de coduri de conduită şi stabilirea unor mecanisme de certificare, precum şi a unor sigilii şi mărci în domeniul protecţiei datelor, în conformitate cu articolele 40 şi 42;

o) să efectueze acreditarea organismelor de certificare şi revizuirea periodică a acreditării în conformitate cu articolul 43 şi să ţină un registru public al organismelor acreditate, în conformitate cu

articolul 43 alineatul (6) , şi al operatorilor acreditaţi sau al persoanelor împuternicite de operator acreditate, stabiliţi (stabilite) în ţări terţe, în conformitate cu articolul 42 alineatul (7) ;

p) să precizeze cerinţele menţionate la articolul 43 alineatul (3) , în vederea acreditării organismelor de certificare prevăzute la articolul 42;

q) să prezinte Comisiei un aviz privind cerinţele de certificare menţionate la articolul 43 alineatul (8) ;

r) să prezinte Comisiei un aviz privind pictogramele menţionate la articolul 12 alineatul (7) ;

s) să prezinte Comisiei un aviz pentru evaluarea caracterului adecvat al nivelului de protecţie într-o ţară terţă sau o organizaţie internaţională, inclusiv pentru a determina dacă o ţară terţă, un teritoriu, sau unul sau mai multe sectoare specificate din acea ţară terţă, sau o organizaţie internaţională nu mai asigură un nivel de protecţie adecvat. În acest scop, Comisia pune la dispoziţia comitetului toată documentaţia necesară, inclusiv corespondenţa purtată cu autorităţile publice ale ţării terţe, în ceea ce priveşte acea ţară terţă, acel teritoriu sau acel sector, sau cu organizaţia internaţională;

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

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

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

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

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

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

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

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

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

Art. 71: Rapoarte

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

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

Art. 72: Procedura

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

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

Art. 73: Preşedintele

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

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

Art. 74: Sarcinile preşedintelui

(1) Preşedintele are următoarele sarcini:

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

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

c) să asigure îndeplinirea la timp a sarcinilor comitetului, în special în ceea ce priveşte mecanismul pentru asigurarea coerenţei menţionat la articolul 63.

(2) Comitetul stabileşte în regulamentul său de procedură repartizarea sarcinilor între preşedinte şi vicepreşedinţi.

Art. 75: Secretariatul

(1) Comitetul dispune de un secretariat, care este asigurat de Autoritatea Europeană pentru Protecţia Datelor.

(2) Secretariatul îşi îndeplineşte sarcinile exclusiv pe baza instrucţiunilor preşedintelui comitetului.

(3) Personalul Autorităţii Europene pentru Protecţia Datelor implicat în îndeplinirea sarcinilor conferite comitetului în temeiul prezentului regulament face obiectul unor linii de raportare separate în raport cu personalul implicat în îndeplinirea sarcinilor conferite Autorităţii Europene pentru Protecţia Datelor.

(4) Dacă este oportun, comitetul şi Autoritatea Europeană pentru Protecţia Datelor elaborează şi publică un memorandum de înţelegere pentru punerea în aplicare a prezentului articol, care să stabilească condiţiile cooperării şi să se aplice personalului Autorităţii Europene pentru Protecţia Datelor implicat în îndeplinirea sarcinilor conferite comitetului în temeiul prezentului regulament.

(5) Secretariatul oferă sprijin analitic, administrativ şi logistic comitetului.

(6) Secretariatul este responsabil în special de următoarele:

a) gestionarea curentă a activităţii comitetului;

b) comunicarea dintre membrii comitetului, preşedintele acestuia şi Comisie;

c) comunicarea cu alte instituţii şi cu publicul;

d) utilizarea mijloacelor electronice pentru comunicarea internă şi externă;

e) traducerea informaţiilor relevante;

f) pregătirea şi monitorizarea acţiunilor ulterioare reuniunilor comitetului;

g) pregătirea, redactarea şi publicarea avizelor, deciziilor privind soluţionarea litigiilor dintre autorităţile de supraveghere şi a altor texte adoptate de comitet.

Art. 76: Confidenţialitate

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

(2) Accesul la documentele prezentate membrilor comitetului, experţilor şi reprezentanţilor părţilor terţe este reglementat prin Regulamentul (CE) nr. **1049/2001** al Parlamentului European şi al Consiliului (1) .

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

CAPITOLUL VIII: Căi de atac, răspundere şi sancţiuni

Art. 77: Dreptul de a depune o plângere la o autoritate de supraveghere

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

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

Art. 78: Dreptul la o cale de atac judiciară eficientă împotriva unei autorităţi de supraveghere

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

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

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

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

Art. 79: Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau unei persoane împuternicite de operator

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

(2) Acţiunile introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în faţa instanţelor din statul membru unde operatorul sau persoana împuternicită de operator îşi are un sediu. Alternativ, o astfel de acţiune poate fi prezentată în faţa instanţelor din statul membru în care persoana vizată îşi are reşedinţa obişnuită, cu excepţia cazului în care operatorul sau persoana împuternicită de operator este o autoritate publică a unui stat membru ce acţionează în exercitarea competenţelor sale publice.

Art. 80: Reprezentarea persoanelor vizate

(1) Persoana vizată are dreptul de a mandata un organism, o organizaţie sau o asociaţie fără scop lucrativ, care au fost constituite în mod corespunzător în conformitate cu dreptul intern, ale căror obiective statutare sunt de interes public, care sunt active în domeniul protecţiei drepturilor şi libertăţilor persoanelor vizate în ceea ce priveşte protecţia datelor lor cu caracter personal, să depună plângerea în numele său, să exercite în numele său drepturile menţionate la articolele 77, 78 şi 79, precum şi să exercite dreptul de a primi despăgubiri menţionat la articolul 82 în numele persoanei vizate, dacă acest lucru este prevăzut în dreptul intern.

(2) Statele membre pot prevedea că orice organism, organizaţie sau asociaţie menţionată la alineatul (1) din prezentul articol, independent de mandatul unei persoanei vizate, are dreptul de a depune în statul membru respectiv o plângere la autoritatea de supraveghere care este competentă în temeiul articolului 77 şi de a exercita drepturile menţionate la articolele 78 şi 79, în cazul în care consideră că drepturile unei persoane vizate în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării.

Art. 81: Suspendarea procedurilor

(1) În cazul în care o instanţă competentă a unui stat membru are informaţii că pe rolul unei instanţe dintr-un alt stat membru se află o acţiune având acelaşi obiect în ceea ce priveşte activităţile de prelucrare ale aceluiaşi operator sau ale aceleaşi persoane împuternicite de operator, instanţa respectivă contactează instanţa din celălalt stat membru pentru a confirma existenţa unor astfel de acţiuni.

(2) Atunci când pe rolul unei instanţe dintr-un alt stat membru se află o acţiune având acelaşi obiect în ceea ce priveşte activităţile de prelucrare ale aceluiaşi operator sau ale aceleaşi persoane împuternicite de operator, orice altă instanţă competentă decât instanţa sesizată iniţial poate suspenda acţiunea aflată la ea pe rol.

(3) În cazul în care o astfel de acţiune se judecă în primă instanţă, orice instanţă sesizată ulterior poate, de asemenea, la cererea uneia dintre părţi, să-şi decline competenţa, cu condiţia ca respectiva acţiune să fie de competenţa primei instanţe sesizate şi ca dreptul aplicabil acesteia să permită conexarea acţiunilor.

Art. 82: Dreptul la despăgubiri şi răspunderea

(1) Orice persoană care a suferit un prejudiciu materiale sau moral ca urmare a unei încălcări a prezentului regulament are dreptul să obţină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.

(2) Orice operator implicat în operaţiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operaţiunile sale de prelucrare care încalcă prezentul regulament. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligaţiile din prezentul regulament care revin în mod specific persoanelor împuternicite de operator sau a acţionat în afara sau în contradicţie cu instrucţiunile legale ale operatorului.

(3) Operatorul sau persoana împuternicită de operator este exonerat(ă) de răspundere în temeiul alineatului (2) dacă dovedeşte că nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul.

(4) În cazul în care mai mulţi operatori sau mai multe persoane împuternicite de operator, sau un operator şi o persoană împuternicită de operator sunt implicaţi (implicate) în aceeaşi operaţiune de

prelucrare şi răspund, în temeiul alineatelor (2) şi (3) , pentru orice prejudiciu cauzat de prelucrare, fiecare operator sau persoană împuternicită de operator este răspunzător (răspunzătoare) pentru întregul prejudiciu pentru a asigura despăgubirea efectivă a persoanei vizate.

(5) În cazul în care un operator sau o persoană împuternicită de operator a plătit, în conformitate cu alineatul (4) , în totalitate despăgubirile pentru prejudiciul ocazionat, respectivul operator sau respectiva persoană împuternicită de operator are dreptul să solicite de la ceilalţi operatori sau celelalte persoane împuternicite de operator implicate în aceeaşi operaţiune de prelucrare recuperarea acelei părţi din despăgubiri care corespunde părţii lor de răspundere pentru prejudiciu, în conformitate cu condiţiile stabilite la alineatul (2) .

(6) Acţiunile în exercitarea dreptului de recuperare a despăgubirilor plătite se introduc la instanţele competente în temeiul dreptului statului membru menţionat la articolul 79 alineatul (2) .

Art. 83: Condiţii generale pentru impunerea amenzilor administrative

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

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

a) natura, gravitatea şi durata încălcării, ţinându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum şi de numărul persoanelor vizate afectate şi de nivelul prejudiciilor suferite de acestea;

b) dacă încălcarea a fost comisă intenţionat sau din neglijenţă;

c) orice acţiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;

d) gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ţinându-se seama de măsurile tehnice şi organizatorice implementate de aceştia în temeiul articolelor 25 şi 32;

e) eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;

f) gradul de cooperare cu autoritatea de supraveghere pentru a remedia încălcarea şi a atenua posibilele efecte negative ale încălcării;

g) categoriile de date cu caracter personal afectate de încălcare;

h) modul în care încălcarea a fost adusă la cunoştinţa autorităţii de supraveghere, în special dacă şi în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;

i) în cazul în care măsurile menţionate la articolul 58 alineatul (2) au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la acelaşi obiect, respectarea respectivelor măsuri;

j) aderarea la coduri de conduită aprobate, în conformitate cu articolul 40, sau la mecanisme de certificare aprobate, în conformitate cu articolul 42; şi

k) orice alt factor agravant sau atenuant aplicabil circumstanţelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

(3) În cazul în care un operator sau o persoană împuternicită de operator încalcă în mod intenţionat sau din neglijenţă, pentru aceeaşi operaţiune de prelucrare sau pentru operaţiuni de prelucrare conexe, mai multe dispoziţii din prezentul regulament, cuantumul total al amenzii administrative nu poate depăşi suma prevăzută pentru cea mai gravă încălcare.

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

a) obligaţiile operatorului şi ale persoanei împuternicite de operator în conformitate cu articolele 8, 11, 25-39, 42 şi 43;

b) obligaţiile organismului de certificare în conformitate cu articolele 42 şi 43;

c) obligaţiile organismului de monitorizare în conformitate cu articolul 41 alineatul (4) .

(5) Pentru încălcările dispoziţiilor următoare, în conformitate cu alineatul (2) , se aplică amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de

afaceri mondială totală anuală corespunzătoare exerciţiului financiar anterior, luânduse în calcul cea mai mare valoare:

a) principiile de bază pentru prelucrare, inclusiv condiţiile privind consimţământul, în conformitate cu articolele 5, 6, 7 şi 9;

b) drepturile persoanelor vizate în conformitate cu articolele 12-22;

c) transferurile de date cu caracter personal către un destinatar dintr-o ţară terţă sau o organizaţie internaţională, în conformitate cu articolele 44-49;

d) orice obligaţii în temeiul legislaţiei naţionale adoptate în temeiul capitolului IX;

e) nerespectarea unui ordin sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării fluxurilor de date, emisă de către autoritatea de supraveghere în temeiul articolului 58 alineatul (2) , sau neacordarea accesului, încălcând articolul 58 alineatul (1) .

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

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

(8) Exercitarea de către autoritatea de supraveghere a competenţelor sale în temeiul prezentului articol are loc cu condiţia existenţei unor garanţii procedurale adecvate în conformitate cu dreptul Uniunii şi cu dreptul intern, inclusiv căi de atac judiciare eficiente şi dreptul la un proces echitabil.

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

Art. 84: Sancţiuni

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

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

CAPITOLUL IX: Dispoziţii referitoare la situaţii specifice de prelucrare

Art. 85: Prelucrarea şi libertatea de exprimare şi de informare

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

(2) Pentru prelucrarea efectuată în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare, statele membre prevăd exonerări sau derogări de la dispoziţiile capitolului II (principii) , ale capitolului III (drepturile persoanei vizate) , ale capitolului IV (operatorul şi persoana împuternicită de operator) , ale capitolului V (transferul datelor cu caracter personal către ţări terţe sau organizaţii internaţionale) , ale capitolului VI (autorităţi de supraveghere independente) , ale capitolului VII (cooperare şi coerenţă) şi ale capitolului IX (situaţii specifice de prelucrare a datelor) în cazul în care acestea sunt necesare pentru a asigura un echilibru între dreptul la protecţia datelor cu caracter personal şi libertatea de exprimare şi de informare.

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

Art. 86: Prelucrarea şi accesul public la documente oficiale

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

Art. 87: Prelucrarea unui număr de identificare naţional

Statele membre pot detalia în continuare condiţiile specifice de prelucrare a unui număr de identificare naţional sau a oricărui alt identificator cu aplicabilitate generală. În acest caz, numărul de identificare naţional sau orice alt identificator cu aplicabilitate generală este folosit numai în temeiul unor garanţii corespunzătoare pentru drepturile şi libertăţile persoanei vizate în temeiul prezentului regulament.

Art. 88: Prelucrarea în contextul ocupării unui loc de muncă

(1) Prin lege sau prin acorduri colective, statele membre pot prevedea norme mai detaliate pentru a asigura protecţia drepturilor şi a libertăţilor cu privire la prelucrarea datelor cu caracter personal ale angajaţilor în contextul ocupării unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligaţiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării şi organizării muncii, al egalităţii şi diversităţii la locul de muncă, al asigurării sănătăţii şi securităţii la locul de muncă, al protejării proprietăţii angajatorului sau a clientului, precum şi în scopul exercitării şi beneficierii, în mod individual sau colectiv, de drepturile şi beneficiile legate de ocuparea unui loc de muncă, precum şi pentru încetarea raporturilor de muncă.

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

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

Art. 89: Garanţii şi derogări privind prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice

(1) Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice are loc cu condiţia existenţei unor garanţii corespunzătoare, în conformitate cu prezentul regulament, pentru drepturile şi libertăţile persoanelor vizate.

Respectivele garanţii asigură faptul că au fost instituite măsuri tehnice şi organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor. Respectivele măsuri pot include pseudonimizarea, cu condiţia ca respectivele scopuri să fie îndeplinite în acest mod. Atunci când respectivele scopuri pot fi îndeplinite printr-o prelucrare ulterioară care nu permite sau nu mai permite identificarea persoanelor vizate, scopurile respective sunt îndeplinite în acest mod.

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

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

(4) În cazul în care prelucrarea menţionată la alineatele (2) şi (3) serveşte în acelaşi timp şi altui scop, derogările se aplică numai prelucrării în scopurile menţionate la alineatele respective.

Art. 90: Obligaţii privind păstrarea confidenţialităţii

(1) Statele membre pot adopta norme specifice pentru a stabili competenţele autorităţilor de supraveghere, prevăzute la articolul 58 alineatul (1) literele (e) şi (f) , în legătură cu operatori sau cu persoane împuternicite de operatori care, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organismele naţionale competente, au obligaţia de a păstra secretul

profesional sau alte obligaţii echivalente de confidenţialitate, în cazul în care acest lucru este necesar şi proporţional pentru a stabili un echilibru între dreptul la protecţia datelor cu caracter personal şi obligaţia păstrării confidenţialităţii. Respectivele norme se aplică doar în ceea ce priveşte datele cu caracter personal pe care operatorul sau persoana împuternicită de operator le-a primit în urma sau în contextul unei activităţi care intră sub incidenţa acestei obligaţii de păstrare a confidenţialităţii.

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

Art. 91: Normele existente în domeniul protecţiei datelor pentru biserici şi asociaţii religioase

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

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

CAPITOLUL X: Acte delegate şi acte de punere în aplicare

Art. 92: Exercitarea delegării

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

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

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

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

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

Art. 93: Procedura comitetului

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

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

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

CAPITOLUL XI: Dispoziţii finale

Art. 94: Abrogarea Directivei 95/46/CE

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

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

Art. 95: Relaţia cu Directiva 2002/58/CE

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

Art. 96: Relaţia cu acordurile încheiate anterior

Acordurile internaţionale care implică transferul de date cu caracter personal către ţări terţe sau organizaţii internaţionale, care au fost încheiate de statele membre înainte de 24 mai 2016 şi care sunt în

conformitate cu dreptul Uniunii aplicabil înainte de data respectivă, rămân în vigoare până când vor fi modificate, înlocuite sau revocate.

Art. 97: Rapoartele Comisiei

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

(2) În contextul evaluărilor şi revizuirilor menţionate la alineatul (1) , Comisia examinează în special aplicarea şi funcţionarea:

a) capitolului V privind transferul datelor cu caracter personal către ţări terţe sau organizaţii internaţionale, având în vedere în special deciziile adoptate în temeiul articolului 45 alineatul (3) din prezentul regulament şi deciziile adoptate în temeiul articolului 25 alineatul (6) din Directiva **95/46/CE**;

b) capitolul VII privind cooperarea şi coerenţa.

(3) În scopul alineatului (1) , Comisia poate solicita informaţii de la statele membre şi de la autorităţile de supraveghere.

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

(5) Comisia transmite, dacă este necesar, propuneri corespunzătoare de modificare a prezentului regulament, în special ţinând seama de evoluţiile din domeniul tehnologiei informaţiei şi având în vedere progresele societăţii informaţionale.

Art. 98: Revizuirea altor acte juridice ale Uniunii în materie de protecţie a datelor

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

Art. 99: Intrare în vigoare şi aplicare

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

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

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

-****-

Adoptat la Bruxelles, 27 aprilie 2016.

Pentru Parlamentul European

Preşedintele

M. SCHULZ

Pentru Consiliu

Preşedintele

J.A. HENNIS-PLASSCHAERT

Publicat în Jurnalul Oficial cu numărul 119L din data de 4 mai 2016__