REGULAMENT nr. 679
din 27 aprilie 2016
privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE (Regulamentul general privind protectia datelor)
(Text cu relevanta pentru SEE) - (General Data Protection Regulation - GDPR)

PARLAMENTUL EUROPEAN SI CONSILIUL UNIUNII EUROPENE,
avand in vedere Tratatul privind functionarea Uniunii Europene, in special articolul 16,
avand in vedere propunerea Comisiei Europene,
dupa transmiterea proiectului de act legislativ catre parlamentele nationale,
avand in vedere avizul Comitetului Economic si Social European [(1)],
[(1)] JO C 229, 31.7.2012.

avand in vedere avizul Comitetului Regiunilor [(2)],
[(2)] JO C 391, 18.12.2012.

hotarand in conformitate cu procedura legislativa ordinara [(3)],
[(3)] Pozitia Parlamentului European din 12 martie 2014 (nepublicata inca in Jurnalul Oficial) si Pozitia in prima lectura a Consiliului din 8 aprilie 2016 (nepublicata inca in Jurnalul Oficial). Pozitia Parlamentului European din 14 aprilie 2016.

intrucat:
(1) Protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene ("carta") si articolul 16 alineatul (1) din Tratatul privind functionarea Uniunii Europene (TFUE) prevad dreptul oricarei persoane la protectia datelor cu caracter personal care o privesc.
(2) Principiile si normele referitoare la protectia persoanelor fizice in ceea ce priveste prelucrarea datelor lor cu caracter personal ar trebui, indiferent de cetatenia sau de locul de resedinta al persoanelor fizice, sa respecte drepturile si libertatile fundamentale ale acestora, in special dreptul la protectia datelor cu caracter personal. Prezentul regulament urmareste sa contribuie la realizarea unui spatiu de libertate, securitate si justitie si a unei uniuni economice, la progresul economic si social, la consolidarea si convergenta economiilor in cadrul pietei interne si la bunastarea persoanelor fizice.
(3) Directiva 95/46/CE a Parlamentului European si a Consiliului[(4)] vizeaza armonizarea nivelului de protectie a drepturilor si libertatilor fundamentale ale persoanelor fizice in ceea ce priveste activitatile de prelucrare si asigurarea liberei circulatii a datelor cu caracter personal intre statele membre.
[(4)] Directiva 95/46/CE a Parlamentului European si a Consiliului din 24 octombrie 1995 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si libera circulatie a acestor date.
(4) Prelucrarea datelor cu caracter personal ar trebui sa fie in serviciul cetatenilor. Dreptul la protectia datelor cu caracter personal nu este un drept absolut; acesta trebuie luat in considerare in raport cu functia pe care o indeplineste in societate si echilibrat cu alte drepturi fundamentale, in conformitate cu principiul proportionalitatii. Prezentul regulament respecta toate drepturile fundamentale si libertatile si principiile recunoscute in carta astfel cum sunt consacrate in tratate, in special respectarea vietii private si de familie, a resedintei si a comunicatiilor, a protectiei datelor cu caracter personal, a libertatii de gandire, de constiinta si de religie, a libertatii de exprimare si de informare, a libertatii de a desfasura o activitate comerciala, dreptul la o cale de atac eficienta si la un proces echitabil, precum si diversitatea culturala, religioasa si lingvistica.
(5) Integrarea economica si sociala care rezulta din functionarea pietei interne a condus la o crestere substantiala a fluxurilor transfrontaliere de date cu caracter personal. Schimbul de date cu caracter personal intre actori publici si privati, inclusiv persoane fizice, asociatii si intreprinderi, s-a intensificat in intreaga Uniune. Conform dreptului Uniunii, autoritatile nationale din statele membre sunt chemate sa coopereze si sa faca schimb de date cu caracter personal pentru a putea sa isi indeplineasca atributiile sau sa execute sarcini in numele unei autoritati dintr-un alt stat membru.
(6) Evolutiile tehnologice rapide si globalizarea au generat noi provocari pentru protectia datelor cu caracter personal. Amploarea colectarii si a schimbului de date cu caracter personal a crescut in mod semnificativ. Tehnologia permite atat societatilor private, cat si autoritatilor publice sa utilizeze date cu caracter personal la

un nivel fara precedent in cadrul activitatilor lor. Din ce in ce mai mult, persoanele fizice fac publice la nivel mondial informatii cu caracter personal. Tehnologia a transformat deopotriva economia si viata sociala si ar trebui sa faciliteze in continuare libera circulatie a datelor cu caracter personal in cadrul Uniunii si transferul catre tari terte si organizatii internationale, asigurand, totodata, un nivel ridicat de protectie a datelor cu caracter personal.

(7) Aceste evolutii impun un cadru solid si mai coerent in materie de protectie a datelor in Uniune, insotit de o aplicare riguroasa a normelor, luand in considerare importanta crearii unui climat de incredere care va permite economiei digitale sa se dezvolte pe piata interna. Persoanele fizice ar trebui sa aiba control asupra propriilor date cu caracter personal, iar securitatea juridica si practica pentru persoane fizice, operatori economici si autoritati publice ar trebui sa fie consolidata.

(8) In cazul in care prezentul regulament prevede specificari sau restrictionari ale normelor sale de catre dreptul intern, statele membre pot, in masura in care acest lucru este necesar pentru coerenta si pentru a asigura intelegerea dispozitiilor nationale de catre persoanele carora li se aplica acestea, sa incorporeze elemente din prezentul regulament in dreptul lor intern.

(9) Obiectivele si principiile Directivei 95/46/CE raman solide, dar aceasta nu a prevenit fragmentarea modului in care protectia datelor este pusa in aplicare in Uniune, insecuritatea juridica sau perceptia publica larg raspandita conform careia exista riscuri semnificative pentru protectia persoanelor fizice, in special in legatura cu activitatea online. Diferentele dintre nivelurile de protectie a drepturilor si libertatilor persoanelor fizice, in special a dreptului la protectia datelor cu caracter personal, in ceea ce priveste prelucrarea datelor cu caracter personal din statele membre pot impiedica libera circulatie a datelor cu caracter personal in intreaga Uniune. Aceste diferente pot constitui, prin urmare, un obstacol in desfasurarea de activitati economice la nivelul Uniunii, pot denatura concurenta si pot impiedica autoritatile sa indeplineasca responsabilitatile care le revin in temeiul dreptului Uniunii. Aceasta diferenta intre nivelurile de protectie este cauzata de existenta unor deosebiri in ceea ce priveste transpunerea si aplicarea Directivei 95/46/CE.

(10) Pentru a se asigura un nivel consecvent si ridicat de protectie a persoanelor fizice si pentru a se indeparta obstacolele din calea circulatiei datelor cu caracter personal in cadrul Uniunii, nivelul protectiei drepturilor si libertatilor persoanelor fizice in ceea ce priveste prelucrarea unor astfel de date ar trebui sa fie echivalent in toate statele membre. Aplicarea consecventa si omogena a normelor in materie de protectie a drepturilor si libertatilor fundamentale ale persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal ar trebui sa fie asigurata in intreaga Uniune. In ceea ce priveste prelucrarea datelor cu caracter personal in vederea respectarii unei obligatii legale, a indeplinirii unei sarcini care serveste unui interes public sau care rezulta din exercitarea autoritatii publice cu care este investit operatorul, statelor membre ar trebui sa li se permita sa mentina sau sa introduca dispozitii de drept intern care sa clarifice intr-o mai mare masura aplicarea normelor prezentului regulament. In coroborare cu legislatia generala si orizontala privind protectia datelor, prin care este pusa in aplicare Directiva 95/46/CE, statele membre au mai multe legi sectoriale specifice in domenii care necesita dispozitii mai precise. Prezentul regulament ofera, de asemenea, statelor membre o marja de manevra in specificarea normelor sale, inclusiv in ceea ce priveste prelucrarea categoriilor speciale de date cu caracter personal ("date sensibile"). In acest sens, prezentul regulament nu exclude dreptul statelor membre care stabileste circumstantele aferente unor situatii de prelucrare specifice, inclusiv stabilirea cu o mai mare precizie a conditiilor in care prelucrarea datelor cu caracter personal este legala.

(11) Protectia efectiva a datelor cu caracter personal in intreaga Uniune necesita nu numai consolidarea si stabilirea in detaliu a drepturilor persoanelor vizate si a obligatiilor celor care prelucreaza si decid prelucrarea datelor cu caracter personal, ci si competente echivalente pentru monitorizarea si asigurarea conformitatii cu normele de protectie a datelor cu caracter personal si sanctiuni echivalente pentru infractiuni in statele membre.

(12) Articolul 16 alineatul (2) din TFUE mandateaza Parlamentul European si Consiliul sa stabileasca normele privind protectia persoanelor fizice referitor la prelucrarea datelor cu caracter personal, precum si normele privind libera circulatie a acestor date.

(13) In vederea asigurarii unui nivel uniform de protectie pentru persoanele fizice in intreaga Uniune si a preintampinarii discrepantelor care impiedica libera circulatie a datelor in cadrul pietei interne, este necesar un regulament in scopul de a furniza securitate juridica si transparenta pentru operatorii economici, inclusiv microintreprinderi si intreprinderi mici si mijlocii, precum si de a oferi persoanelor fizice in toate statele membre acelasi nivel de drepturi, obligatii si responsabilitati opozabile din punct de vedere juridic pentru operatori si persoanele imputernicite de acestia, pentru a se asigura o monitorizare coerenta a prelucrarii datelor cu caracter personal, sanctiuni echivalente in toate statele membre, precum si cooperarea eficace a autoritatilor de supraveghere ale diferitelor state membre. Pentru buna functionare a pietei interne este necesar ca libera

circulatie a datelor cu caracter personal in cadrul Uniunii sa nu fie restrictionata sau interzisa din motive legate de protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal. Pentru a se lua in considerare situatia specifica a microintreprinderilor si a intreprinderilor mici si mijlocii, prezentul regulament include o derogare pentru organizatiile cu mai putin de 250 de angajati in ceea ce priveste pastrarea evidentelor. In plus, institutiile si organele Uniunii si statele membre si autoritatile lor de supraveghere sunt incurajate sa ia in considerare necesitatile specifice ale microintreprinderilor si ale intreprinderilor mici si mijlocii in aplicarea prezentului regulament. Notiunea de microintreprinderi si de intreprinderi mici si mijlocii ar trebui sa 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 microintreprinderilor si a intreprinderilor mici si mijlocii [C (2003) 1422] (JO L 124, 20.5.2003, p. 36).

(14) Protectia conferita de prezentul regulament ar trebui sa vizeze persoanele fizice, indiferent de cetatenia sau de locul de resedinta al acestora, in ceea ce priveste prelucrarea datelor cu caracter personal ale acestora. Prezentul regulament nu se aplica prelucrarii datelor cu caracter personal care privesc persoane juridice si, in special, intreprinderi cu personalitate juridica, inclusiv numele si tipul de persoana juridica si datele de contact ale persoanei juridice.

(15) Pentru a preveni aparitia unui risc major de eludare, protectia persoanelor fizice ar trebui sa fie neutra din punct de vedere tehnologic si sa nu depinda de tehnologiile utilizate. Protectia persoanelor fizice ar trebui sa se aplice prelucrarii datelor cu caracter personal prin mijloace automatizate, precum si prelucrarii manuale, in cazul in care datele cu caracter personal sunt cuprinse sau destinate sa fie cuprinse intr-un sistem de evidenta. Dosarele sau seturile de dosare, precum si copertele acestora, care nu sunt structurate in conformitate cu criterii specificenu ar trebui sa intre in domeniul de aplicare al prezentului regulament.

(16) Prezentul regulament nu se aplica chestiunilor de protectie a drepturilor si libertatilor fundamentale sau la libera circulatie a datelor cu caracter personal referitoare la activitati care nu intra in domeniul de aplicare al dreptului Uniunii, de exemplu activitatile privind securitatea nationala. Prezentul regulament nu se aplica prelucrarii datelor cu caracter personal de catre statele membre atunci cand acestea desfasoara activitati legate de politica externa si de securitatea comuna a Uniunii.

(17) Regulamentul (CE) nr. 45/2001 al Parlamentului European si al Consiliului se aplica prelucrarii de date cu caracter personal de catre institutiile, organele, oficiile si agentiile Uniunii. Regulamentul (CE) nr. 45/2001 si alte acte juridice ale Uniunii aplicabile unei asemenea prelucrari a datelor cu caracter personal ar trebui adaptate la principiile si normele stabilite in prezentul regulament si aplicate in conformitate cu prezentul regulament. In vederea asigurarii unui cadru solid si coerent in materie de protectie a datelor in Uniune, ar trebui ca dupa adoptarea prezentului regulament sa se aduca Regulamentului (CE) nr. 45/2001 adaptarile necesare, astfel incat acestea sa poata fi aplicate odata cu prezentul regulament.

(18) Prezentul regulament nu se aplica prelucrarii datelor cu caracter personal de catre o persoana fizica in cadrul unei activitati exclusiv personale sau domestice si care, prin urmare, nu are legatura cu o activitate profesionala sau comerciala. Activitatile personale sau domestice ar putea include corespondenta si repertoriul de adrese sau activitatile din cadrul retelelor sociale si activitatile online desfasurate in contextul respectivelor activitati. Cu toate acestea, prezentul regulament se aplica operatorilor sau persoanelor imputernicite de operatori care furnizeaza mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activitati personale sau domestice.

(19) Protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal de catre autoritatile competente in scopul prevenirii, investigarii, depistarii sau urmaririi penale a infractiunilor sau al executarii pedepselor, inclusiv al protejarii impotriva amenintarilor la adresa sigurantei publice si al prevenirii acestora, precum si libera circulatie a acestor date, face obiectul unui act juridic specific al Uniunii. Prin urmare, prezentul regulament nu ar trebui sa se aplice activitatilor de prelucrare in aceste scopuri. Cu toate acestea, datele cu caracter personal prelucrate de catre autoritatile publice in temeiul prezentului regulament, atunci cand sunt utilizate in aceste scopuri, ar trebui sa fie reglementate printr-un act juridic mai specific al Uniunii, si anume Directiva (UE) 2016/680 a Parlamentului European si a Consiliului. Statele membre pot incredinta autoritatilor competente in sensul Directivei (UE) 2016/680 sarcini care nu sunt neaparat indeplinite in scopul prevenirii, investigarii, depistarii sau urmaririi penale a infractiunilor sau al executarii pedepselor, inclusiv al protejarii impotriva amenintarilor la adresa sigurantei publice si al prevenirii acestora, astfel incat prelucrarea datelor cu caracter personal pentru alte scopuri, in masura in care se incadreaza in domeniul de aplicare al dreptului Uniunii, sa intre in domeniul de aplicare al prezentului regulament.

In ceea ce priveste prelucrarea datelor cu caracter personal de catre aceste autoritati competente in scopuri care intra in domeniul de aplicare al prezentului regulament, statele membre ar trebui sa poata mentine sau

introduce dispozitii mai detaliate pentru a adapta aplicarea normelor din prezentul regulament. Aceste dispozitii pot stabili mai precis cerinte specifice pentru prelucrarea datelor cu caracter personal de catre respectivele autoritati competente in aceste alte scopuri, tinand seama de structura constitutionala, organizatorica si administrativa a statului membru in cauza. Atunci cand prelucrarea de date cu caracter personal de catre organisme private face obiectul prezentului regulament, prezentul regulament ar trebui sa prevada posibilitatea ca statele membre, in anumite conditii, sa impuna prin lege restrictii asupra anumitor obligatii si drepturi, in cazul in care asemenea restrictii constituie o masura necesara si proportionala intr-o societate democratica in scopul garantarii unor interese specifice importante, printre care se numara siguranta publica si prevenirea, investigarea, depistarea si urmarirea penala a infractiunilor sau executarea pedepselor, inclusiv protejarea impotriva amenintarilor la adresa sigurantei publice si prevenirea acestora. Acest lucru este relevant, de exemplu, in cadrul combaterii spalarii de bani sau al activitatilor laboratoarelor criminalistice.

(20) Desi prezentul regulament se aplica, inter alia, activitatilor instantelor si ale altor autoritati judiciare, dreptul Uniunii sau al statelor membre ar putea sa precizeze operatiunile si procedurile de prelucrare in ceea ce priveste prelucrarea datelor cu caracter personal de catre instante si alte autoritati judiciare. Prelucrarea datelor cu caracter personal nu ar trebui sa fie de competenta autoritatilor de supraveghere in cazul in care instantele isi exercita atributiile judiciare, in scopul garantarii independentei sistemului judiciar in indeplinirea sarcinilor sale judiciare, inclusiv in luarea deciziilor. Supravegherea unor astfel de operatiuni de prelucrare a datelor ar trebui sa poata fi incredintata unor organisme specifice din cadrul sistemului judiciar al statului membru, care ar trebui sa asigure in special respectarea normelor prevazute de prezentul regulament, sa sensibilizeze membrii sistemului judiciar cu privire la obligatiile care le revin in temeiul prezentului regulament si sa trateze plangerile in legatura cu astfel de operatiuni de prelucrare a datelor.

(21) Prezentul regulament nu aduce atingere aplicarii Directivei 2000/31/CE a Parlamentului European si a Consiliului, in special normelor privind raspunderea furnizorilor intermediari de servicii prevazute la articolele 12-15 din directiva mentionata. Respectiva directiva isi propune sa contribuie la buna functionare a pietei interne, prin asigurarea liberei circulatii a serviciilor societatii informationale intre statele membre.

(22) Orice prelucrare a datelor cu caracter personal in cadrul activitatilor unui sediu al unui operator sau al unei persoane imputernicite de operator din Uniune ar trebui efectuata in conformitate cu prezentul regulament, indiferent daca procesul de prelucrare in sine are loc sau nu in cadrul Uniunii. Sediul implica exercitarea efectiva si reala a unei activitati in cadrul unor intelegeri stabile. Forma juridica a unor astfel de intelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridica, nu este factorul determinant in aceasta privinta.

(23) Pentru a se asigura ca persoanele fizice nu sunt lipsite de protectia la care au dreptul in temeiul prezentului regulament, prelucrarea datelor cu caracter personal ale persoanelor vizate care se afla pe teritoriul Uniunii de catre un operator sau o persoana imputernicita de acesta care nu isi are sediul in Uniune ar trebui sa faca obiectul prezentului regulament in cazul in care activitatile de prelucrare au legatura cu oferirea de bunuri sau servicii unor astfel de persoane vizate, indiferent daca acestea sunt sau nu legate de o plata. Pentru a determina daca un astfel de operator sau o astfel de persoana imputernicita de operator ofera bunuri sau servicii unor persoane vizate care se afla pe teritoriul Uniunii, ar trebui sa se stabileasca daca reiese ca operatorul sau persoana imputernicita de operator intentioneaza sa furnizeze servicii persoanelor vizate din unul sau mai multe state membre din Uniune. Intrucat simplul fapt ca exista acces la un site al operatorului, al persoanei imputernicite de operator sau al unui intermediar in Uniune, ca este disponibila o adresa de e-mail si alte date de contact sau ca este utilizata o limba folosita in general in tara terta in care operatorul isi are sediul este insuficient pentru a confirma o astfel de intentie, factori precum utilizarea unei limbi sau a unei monede utilizate in general in unul sau mai multe state membre cu posibilitatea de a comanda bunuri si servicii in respectiva limba sau mentionarea unor clienti sau utilizatori care se afla pe teritoriul Uniunii pot conduce la concluzia ca operatorul intentioneaza sa ofere bunuri sau servicii unor persoane vizate in Uniune.

(24) Prelucrarea datelor cu caracter personal ale persoanelor vizate care se afla pe teritoriul Uniunii de catre un operator sau o persoana imputernicita de acesta care nu isi are sediul in Uniune ar trebui, de asemenea, sa faca obiectul prezentului regulament in cazul in care este legata de monitorizarea comportamentului unor astfel de persoane vizate, in masura in care acest comportament se manifesta pe teritoriul Uniunii. Pentru a se determina daca o activitate de prelucrare poate fi considerata ca "monitorizare a comportamentului" persoanelor vizate, ar trebui sa se stabileasca daca persoanele fizice sunt urmarite pe internet, inclusiv posibila utilizare ulterioara a unor tehnici de prelucrare a datelor cu caracter personal care constau in crearea unui profil al unei persoane fizice, in special in scopul de a lua decizii cu privire la aceasta sau de a analiza sau de a face previziuni referitoare la preferintele personale, comportamentele si atitudinile acesteia.

(25) In cazul in care dreptul unui stat membru se aplica in temeiul dreptului international public, prezentul regulament ar trebui sa se aplice, de asemenea, unui operator care nu este stabilit in Uniune, ci, de exemplu, intr-o misiune diplomatica sau intr-un oficiu consular al unui stat membru.

(26) Principiile protectiei datelor ar trebui sa se aplice oricarei informatii referitoare la o persoana fizica identificata sau identificabila. Datele cu caracter personal care au fost supuse pseudonimizarii, care ar putea fi atribuite unei persoane fizice prin utilizarea de informatii suplimentare, ar trebui considerate informatii referitoare la o persoana fizica identificabila. Pentru a se determina daca o persoana fizica este identificabila, ar trebui sa se ia in considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, in mod rezonabil, sa le utilizeze fie operatorul, fie o alta persoana, in scopul identificarii, in mod direct sau indirect, a persoanei fizice respective. Pentru a se determina daca este probabil, in mod rezonabil, sa fie utilizate mijloace pentru identificarea persoanei fizice, ar trebui luati in considerare toti factorii obiectivi, precum costurile si intervalul de timp necesare pentru identificare, tinandu-se seama atat de tehnologia disponibila la momentul prelucrarii, cat si de dezvoltarea tehnologica. Principiile protectiei datelor ar trebui, prin urmare, sa nu se aplice informatiilor anonime, adica informatiilor care nu sunt legate de o persoana fizica identificata sau identificabila sau datelor cu caracter personal care sunt anonimizate astfel incat persoana vizata nu este sau nu mai este identificabila. Prin urmare, prezentul regulament nu se aplica prelucrarii unor astfel de informatii anonime, inclusiv in cazul in care acestea sunt utilizate in scopuri statistice sau de cercetare.

(27) Prezentul regulament nu se aplica datelor cu caracter personal referitoare la persoane decedate. Statele membre pot sa prevada norme privind prelucrarea datelor cu caracter personal referitoare la persoane decedate.

(28) Aplicarea pseudonimizarii datelor cu caracter personal poate reduce riscurile pentru persoanele vizate si poate ajuta operatorii si persoanele imputernicite de acestia sa isi indeplineasca obligatiile de protectie a datelor. Introducerea explicita a conceptului de "pseudonimizare" in prezentul regulament nu este destinata sa impiedice alte eventuale masuri de protectie a datelor.

(29) Pentru a crea stimulente pentru aplicarea pseudonimizarii atunci cand sunt prelucrate date cu caracter personal, ar trebui sa fie posibile masuri de pseudonimizare, permitand in acelasi timp analiza generala, in cadrul aceluiasi operator atunci cand operatorul a luat masurile tehnice si organizatorice necesare pentru a se asigura ca prezentul regulament este pus in aplicare in ceea ce priveste respectiva prelucrare a datelor si ca informatiile suplimentare pentru atribuirea datelor cu caracter personal unei anumite persoane vizate sunt pastrate separat. Operatorul care prelucreaza datele cu caracter personal ar trebui sa indice persoanele autorizate din cadrul aceluiasi operator.

(30) Persoanele fizice pot fi asociate cu identificatorii online furnizati de dispozitivele, aplicatiile, instrumentele si protocoalele lor, cum ar fi adresele IP, identificatorii cookie sau alti identificatori precum etichetele de identificare prin frecvente radio. Acestia pot lasa urme care, in special atunci cand sunt combinate cu identificatori unici si alte informatii primite de servere, pot fi utilizate pentru crearea de profiluri ale persoanelor fizice si pentru identificarea lor.

(31) Autoritatile publice carora le sunt divulgate date cu caracter personal in conformitate cu o obligatie legala in vederea exercitarii functiei lor oficiale, cum ar fi autoritatile fiscale si vamale, unitatile de investigare financiara, autoritatile administrative independente sau autoritatile pietelor financiare responsabile de reglementarea si supravegherea pietelor titlurilor de valoare, nu ar trebui sa fie considerate destinatari in cazul in care primesc date cu caracter personal care sunt necesare pentru efectuarea unei anumite anchete de interes general, in conformitate cu dreptul Uniunii sau cel al statelor membre. Cererile de divulgare trimise de autoritatile publice ar trebui sa fie intotdeauna prezentate in scris, motivate si ocazionale si nu ar trebui sa se refere la un sistem de evidenta in totalitate sau sa conduca la interconectarea sistemelor de evidenta. Prelucrarea datelor cu caracter personal de catre autoritatile publice respective ar trebui sa respecte normele aplicabile in materie de protectie a datelor in conformitate cu scopurile prelucrarii.

(32) Consimtamantul ar trebui acordat printr-o actiune neechivoca care sa constituie o manifestare liber exprimata, specifica, in cunostinta de cauza si clara a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declaratie facuta in scris, inclusiv in format electronic, sau verbal. Acesta ar putea include bifarea unei casute atunci cand persoana viziteaza un site, alegerea parametrilor tehnici pentru serviciile societatii informationale sau orice alta declaratie sau actiune care indica in mod clar in acest context acceptarea de catre persoana vizata a prelucrarii propuse a datelor sale cu caracter personal. Prin urmare, absenta unui raspuns, casutele bifate in prealabil sau absenta unei actiuni nu ar trebui sa constituie un consimtamant. Consimtamantul ar trebui sa vizeze toate activitatile de prelucrare efectuate in acelasi scop sau in aceleasi scopuri. Daca prelucrarea datelor se face in mai multe scopuri, consimtamantul ar trebui dat pentru toate scopurile prelucrarii. In cazul in care consimtamantul persoanei vizate trebuie acordat in urma unei cereri

transmise pe cale electronica, cererea respectiva trebuie sa fie clara si concisa si sa nu perturbe in mod inutil utilizarea serviciului pentru care se acorda consimtamantul.

(33) Adesea nu este posibil, in momentul colectarii datelor cu caracter personal, sa se identifice pe deplin scopul prelucrarii datelor in scopuri de cercetare stiintifica. Din acest motiv, persoanelor vizate ar trebui sa li se permita sa isi exprime consimtamantul pentru anumite domenii ale cercetarii stiintifice atunci cand sunt respectate standardele etice recunoscute pentru cercetarea stiintifica. Persoanele vizate ar trebui sa aiba posibilitatea de a-si exprima consimtamantul doar pentru anumite domenii de cercetare sau parti ale proiectelor de cercetare in masura permisa de scopul preconizat.

(34) Datele genetice ar trebui definite drept date cu caracter personal referitoare la caracteristicile genetice mostenite sau dobandite ale unei persoane fizice, care rezulta in urma unei analize a unei mostre de material biologic al persoanei fizice in cauza, in special a unei analize cromozomiale, a unei analize a acidului dezoxiribonucleic (ADN) sau a acidului ribonucleic (ARN) sau a unei analize a oricarui alt element ce permite obtinerea unor informatii echivalente.

(35) Datele cu caracter personal privind sanatatea ar trebui sa includa toate datele avand legatura cu starea de sanatate a persoanei vizate care dezvaluie informatii despre starea de sanatate fizica sau mentala trecuta, prezenta sau viitoare a persoanei vizate. Acestea includ informatii despre persoana fizica colectate in cadrul inscrierii acesteia la serviciile de asistenta medicala sau in cadrul acordarii serviciilor respective persoanei fizice in cauza, astfel cum sunt mentionate in Directiva 2011/24/UE a Parlamentului European si a Consiliului; un numar, un simbol sau un semn distinctiv atribuit unei persoane fizice pentru identificarea singulara a acesteia in scopuri medicale; informatii rezultate din testarea sau examinarea unei parti a corpului sau a unei substante corporale, inclusiv din date genetice si esantioane de material biologic; precum si orice informatii privind, de exemplu, o boala, un handicap, un risc de imbolnavire, istoricul medical, tratamentul clinic sau starea fiziologica sau biomedicala a persoanei vizate, indiferent de sursa acestora, ca de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro.

(36) Sediul principal al unui operator in Uniune ar trebui sa fie locul in care se afla administratia centrala a acestuia in Uniune, cu exceptia cazului in care deciziile privind scopurile si mijloacele de prelucrare a datelor cu caracter personal se iau intr-un alt sediu al operatorului in Uniune. In acest caz, acesta din urma ar trebui considerat drept sediul principal. Sediul principal al unui operator in Uniune ar trebui sa fie determinat conform unor criterii obiective si ar trebui sa implice exercitarea efectiva si reala a unor activitati de gestionare care sa determine principalele decizii cu privire la scopurile si mijloacele de prelucrare in cadrul unor intelegeri stabile. Acest criteriu nu ar trebui sa depinda de realizarea prelucrarii datelor cu caracter personal in locul respectiv. Prezenta si utilizarea mijloacelor tehnice si a tehnologiilor de prelucrare a datelor cu caracter personal sau activitatile de prelucrare nu constituie un sediu principal si, prin urmare, nu sunt criteriul determinant in acest sens. Sediul principal al persoanei imputernicite de operator ar trebui sa fie locul in care se afla administratia centrala a acestuia in Uniune sau, in cazul in care nu are o administratie centrala in Uniune, locul in care se desfasoara principalele activitati de prelucrare in Uniune. In cazurile care implica atat operatorul, cat si persoana imputernicita de operator, autoritatea de supraveghere principala competenta ar trebui sa ramana autoritatea de supraveghere a statului membru in care operatorul isi are sediul principal, dar autoritatea de supraveghere a persoanei imputernicite de operator ar trebui considerata ca fiind o autoritate de supraveghere vizata si acea autoritate de supraveghere ar trebui sa participe la procedura de cooperare prevazuta de prezentul regulament. In orice caz, autoritatile de supraveghere ale statului membru sau ale statelor membre in care persoana imputernicita de operator are unul sau mai multe sedii nu ar trebui considerate ca fiind autoritati de supraveghere vizate in cazul in care proiectul de decizie nu se refera decat la operator. In cazul in care prelucrarea este efectuata de un grup de intreprinderi, sediul principal al intreprinderii care exercita controlul ar trebui considerat drept sediul principal al grupului de intreprinderi, cu exceptia cazului in care scopurile si mijloacele aferente prelucrarii sunt stabilite de o alta intreprindere.

(37) Un grup de intreprinderi ar trebui sa cuprinda o intreprindere care exercita controlul si intreprinderile controlate de aceasta, in cadrul caruia intreprinderea care exercita controlul ar trebui sa fie intreprinderea care poate exercita o influenta dominanta asupra celorlalte intreprinderi, de exemplu in temeiul proprietatii, al participarii financiare sau al regulilor care o reglementeaza sau al competentei de a pune in aplicare norme in materie de protectie a datelor cu caracter personal. O intreprindere care controleaza prelucrarea datelor cu caracter personal in intreprinderile sale afiliate ar trebui considerata, impreuna cu acestea din urma, drept "grup de intreprinderi".

(38) Copiii au nevoie de o protectie specifica a datelor lor cu caracter personal, intrucat pot fi mai putin constienti de riscurile, consecintele, garantiile in cauza si drepturile lor in ceea ce priveste prelucrarea datelor cu

caracter personal. Aceasta protectie specifica ar trebui sa se aplice in special utilizarii datelor cu caracter personal ale copiilor in scopuri de marketing sau pentru crearea de profiluri de personalitate sau de utilizator si la colectarea datelor cu caracter personal privind copiii in momentul utilizarii serviciilor oferite direct copiilor. Consimtamantul titularului raspunderii parintesti nu ar trebui sa fie necesar in contextul serviciilor de prevenire sau consiliere oferite direct copiilor.

(39) Orice prelucrare de date cu caracter personal ar trebui sa fie legala si echitabila. Ar trebui sa fie transparent pentru persoanele fizice ca sunt colectate, utilizate, consultate sau prelucrate in alt mod datele cu caracter personal care le privesc si in ce masura datele cu caracter personal sunt sau vor fi prelucrate. Principiul transparentei prevede ca orice informatii si comunicari referitoare la prelucrarea respectivelor date cu caracter personal sunt usor accesibile si usor de inteles si ca se utilizeaza un limbaj simplu si clar. Acest principiu se refera in special la informarea persoanelor vizate privind identitatea operatorului si scopurile prelucrarii, precum si la oferirea de informatii suplimentare, pentru a asigura o prelucrare echitabila si transparenta in ceea ce priveste persoanele fizice vizate si dreptul acestora de a li se confirma si comunica datele cu caracter personal care le privesc care sunt prelucrate. Persoanele fizice ar trebui informate cu privire la riscurile, normele, garantiile si drepturile in materie de prelucrare a datelor cu caracter personal si cu privire la modul in care sa isi exercite drepturile in legatura cu prelucrarea. In special, scopurile specifice in care datele cu caracter personal sunt prelucrate ar trebui sa fie explicite si legitime si sa fie determinate la momentul colectarii datelor respective. Datele cu caracter personal ar trebui sa fie adecvate, relevante si limitate la ceea ce este necesar pentru scopurile in care sunt prelucrate. Aceasta necesita, in special, asigurarea faptului ca perioada pentru care datele cu caracter personal sunt stocate este limitata strict la minimum. Datele cu caracter personal ar trebui prelucrate doar daca scopul prelucrarii nu poate fi indeplinit in mod rezonabil prin alte mijloace. In vederea asigurarii faptului ca datele cu caracter personal nu sunt pastrate mai mult timp decat este necesar, ar trebui sa se stabileasca de catre operator termene pentru stergere sau revizuirea periodica. Ar trebui sa fie luate toate masurile rezonabile pentru a se asigura ca datele cu caracter personal care sunt inexacte sunt rectificate sau sterse. Datele cu caracter personal ar trebui prelucrate intr-un mod care sa asigure in mod adecvat securitatea si confidentialitatea acestora, inclusiv in scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizata a datelor cu caracter personal si a echipamentului utilizat pentru prelucrare.

(40) Pentru ca prelucrarea datelor cu caracter personal sa fie legala, aceasta ar trebui efectuata pe baza consimtamantului persoanei vizate sau in temeiul unui alt motiv legitim, prevazut de lege, fie in prezentul regulament, fie in alt act din dreptul Uniunii sau din dreptul intern, dupa cum se prevede in prezentul regulament, inclusiv necesitatea respectarii obligatiilor legale la care este supus operatorul sau necesitatea de a executa un contract la care persoana vizata este parte sau pentru a parcurge etapele premergatoare incheierii unui contract, la solicitarea persoanei vizate.

(41) Ori de cate ori prezentul regulament face trimitere la un temei juridic sau la o masura legislativa, aceasta nu necesita neaparat un act legislativ adoptat de catre un parlament, fara a aduce atingere cerintelor care decurg din ordinea constitutionala a statului membru in cauza. Cu toate acestea, un astfel de temei juridic sau o astfel de masura legislativa ar trebui sa fie clara si precisa, iar aplicarea acesteia ar trebui sa fie previzibila pentru persoanele vizate de aceasta, in conformitate cu jurisprudenta Curtii de Justitie a Uniunii Europene ("Curtea de Justitie") si a Curtii Europene a Drepturilor Omului.

(42) In cazul in care prelucrarea se bazeaza pe consimtamantul persoanei vizate, operatorul ar trebui sa fie in masura sa demonstreze faptul ca persoana vizata si-a dat consimtamantul pentru operatiunea de prelucrare. In special, in contextul unei declaratii scrise cu privire la un alt aspect, garantiile ar trebui sa asigure ca persoana vizata este constienta de faptul ca si-a dat consimtamantul si in ce masura a facut acest lucru. In conformitate cu Directiva 93/13/CEE a Consiliului, ar trebui furnizata o declaratie de consimtamant formulata in prealabil de catre operator, intr-o forma inteligibila si usor accesibila, utilizand un limbaj clar si simplu, iar aceasta declaratie nu ar trebui sa contina clauze abuzive. Pentru ca acordarea consimtamantului sa fie in cunostinta de cauza, persoana vizata ar trebui sa fie la curent cel putin cu identitatea operatorului si cu scopurile prelucrarii pentru care sunt destinate datele cu caracter personal. Consimtamantul nu ar trebui considerat ca fiind acordat in mod liber daca persoana vizata nu dispune cu adevarat de libertatea de alegere sau nu este in masura sa refuze sau sa isi retraga consimtamantul fara a fi prejudiciata.

(43) Pentru a garanta faptul ca a fost acordat in mod liber, consimtamantul nu ar trebui sa constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal in cazul particular in care exista un dezechilibru evident intre persoana vizata si operator, in special in cazul in care operatorul este o autoritate publica, iar acest lucru face improbabila acordarea consimtamantului in mod liber in toate circumstantele aferente respectivei situatii particulare. Consimtamantul este considerat a nu fi acordat in mod liber in cazul in care aceasta nu

permite sa se acorde consimtamantul separat pentru diferitele operatiuni de prelucrare a datelor cu caracter personal, desi acest lucru este adecvat in cazul particular, sau daca executarea unui contract, inclusiv furnizarea unui serviciu, este conditionata de consimtamant, in ciuda faptului ca consimtamantul in cauza nu este necesar pentru executarea contractului.

(44) Prelucrarea ar trebui sa fie considerata legala in cazul in care este necesara in cadrul unui contract sau in vederea incheierii unui contract.

(45) In cazul in care prelucrarea este efectuata in conformitate cu o obligatie legala a operatorului sau in cazul in care prelucrarea este necesara pentru indeplinirea unei sarcini care serveste unui interes public sau care face parte din exercitarea autoritatii publice, prelucrarea ar trebui sa aiba un temei in dreptul Uniunii sau in dreptul intern. Prezentul regulament nu impune existenta unei legi specifice pentru fiecare prelucrare in parte. Poate fi suficienta o singura lege drept temei pentru mai multe operatiuni de prelucrare efectuate in conformitate cu o obligatie legala a operatorului sau in cazul in care prelucrarea este necesara pentru indeplinirea unei sarcini care serveste unui interes public sau care face parte din exercitarea autoritatii publice. De asemenea, ar trebui ca scopul prelucrarii sa fie stabilit in dreptul Uniunii sau in dreptul intern. Mai mult decat atat, dreptul respectiv ar putea sa specifice conditiile generale ale prezentului regulament care reglementeaza legalitatea prelucrarii datelor cu caracter personal, sa determine specificatiile pentru stabilirea operatorului, a tipului de date cu caracter personal care fac obiectul prelucrarii, a persoanelor vizate, a entitatilor carora le pot fi divulgate datele cu caracter personal, a limitarilor in functie de scop, a perioadei de stocare si a altor masuri pentru a garanta o prelucrare legala si echitabila. De asemenea, ar trebui sa se stabileasca in dreptul Uniunii sau in dreptul intern daca operatorul care indeplineste o sarcina care serveste unui interes public sau care face parte din exercitarea autoritatii publice ar trebui sa fie o autoritate publica sau o alta persoana fizica sau juridica guvernata de dreptul public sau, atunci cand motive de interes public justifica acest lucru, inclusiv in scopuri medicale, precum sanatatea publica si protectia sociala, precum si gestionarea serviciilor de asistenta medicala, de dreptul privat, cum ar fi o asociatie profesionala.

(46) Prelucrarea datelor cu caracter personal ar trebui, de asemenea, sa fie considerata legala in cazul in care este necesara in scopul asigurarii protectiei unui interes care este esential pentru viata persoanei vizate sau pentru viata unei alte persoane fizice. Prelucrarea datelor cu caracter personal care are drept temei interesele vitale ale unei alte persoane fizice ar trebui efectuata numai in cazul in care prelucrarea nu se poate baza in mod evidentpe un alt temei juridic. Unele tipuri de prelucrare pot servi atat unor motive importante de interes public, cat si intereselor vitale ale persoanei vizate, de exemplu in cazul in care prelucrarea este necesara in scopuri umanitare, inclusiv in vederea monitorizarii unei epidemii si a raspandirii acesteia sau in situatii de urgente umanitare, in special in situatii de dezastre naturale sau provocate de om.

(47) Interesele legitime ale unui operator, inclusiv cele ale unui operator caruia ii pot fi divulgate datele cu caracter personal sau ale unei terte parti, pot constitui un temei juridic pentru prelucrare, cu conditia sa nu prevaleze interesele sau drepturile si libertatile fundamentale ale persoanei vizate, luand in considerare asteptarile rezonabile ale persoanelor vizate bazate pe relatia acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci cand exista o relatie relevanta si adecvata intre persoana vizata si operator, cum ar fi cazul in care persoana vizata este un client al operatorului sau se afla in serviciul acestuia. In orice caz, existenta unui interes legitim ar necesita o evaluare atenta, care sa stabileasca inclusiv daca o persoana vizata poate preconiza in mod rezonabil, in momentul si in contextul colectarii datelor cu caracter personal, posibilitatea prelucrarii in acest scop. Interesele si drepturile fundamentale ale persoanei vizate ar putea prevala in special in raport cu interesul operatorului de date atunci cand datele cu caracter personal sunt prelucrate in circumstante in care persoanele vizate nu preconizeaza in mod rezonabil o prelucrare ulterioara. Intrucat legiuitorul trebuie sa furnizeze temeiul juridic pentru prelucrarea datelor cu caracter personal de catre autoritatile publice, temeiul juridic respectiv nu ar trebui sa se aplice prelucrarii de catre autoritatile publice in indeplinirea sarcinilor care le revin. Prelucrarea de date cu caracter personal strict necesara in scopul prevenirii fraudelor constituie, de asemenea, un interes legitim al operatorului de date in cauza. Prelucrarea de date cu caracter personal care are drept scop marketingul direct poate fi considerata ca fiind desfasurata pentru un interes legitim.

(48) Operatorii care fac parte dintr-un grup de intreprinderi sau institutii afiliate unui organism central pot avea un interes legitim de a transmite date cu caracter personal in cadrul grupului de intreprinderi in scopuri administrative interne, inclusiv in scopul prelucrarii datelor cu caracter personal ale clientilor sau angajatilor. Principiile generale ale transferului de date cu caracter personal, in cadrul unui grup de intreprinderi, catre o intreprindere situata intr-o tara terta raman neschimbate.

(49) Prelucrarea datelor cu caracter personal in masura strict necesara si proportionala in scopul asigurarii securitatii retelelor si a informatiilor, si anume capacitatea unei retele sau a unui sistem de informatii de a face fata, la un anumit nivel de incredere, evenimentelor accidentale sau actiunilor ilegale sau rau intentionate care compromit disponibilitatea, autenticitatea, integritatea si confidentialitatea datelor cu caracter personal stocate sau transmise, precum si securitatea serviciilor conexe oferite de aceste retele si sisteme, sau accesibile prin intermediul acestora, de catre autoritatile publice, echipele de interventie in caz de urgenta informatica, echipele de interventie in cazul producerii unor incidente care afecteaza securitatea informatica, furnizorii de retele si servicii de comunicatii electronice, precum si de catre furnizorii de servicii si tehnologii de securitate, constituie un interes legitim al operatorului de date in cauza. Acesta ar putea include, de exemplu, prevenirea accesului neautorizat la retelele de comunicatii electronice si a difuzarii de coduri daunatoare si oprirea atacurilor de "blocare a serviciului", precum si prevenirea daunelor aduse calculatoarelor si sistemelor de comunicatii electronice.

(50) Prelucrarea datelor cu caracter personal in alte scopuri decat scopurile pentru care datele cu caracter personal au fost initial colectate ar trebui sa fie permisa doar atunci cand prelucrarea este compatibila cu scopurile respective pentru care datele cu caracter personal au fost initial colectate. In acest caz nu este necesar un temei juridic separat de cel pe baza caruia a fost permisa colectarea datelor cu caracter personal. In cazul in care prelucrarea este necesara pentru indeplinirea unei sarcini care serveste unui interes public sau care rezulta din exercitarea autoritatii publice cu care este investit operatorul, dreptul Uniunii sau dreptul intern poate stabili si specifica sarcinile si scopurile pentru care prelucrarea ulterioara ar trebui considerata a fi compatibila si legala. Prelucrarea ulterioara in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice ar trebui considerata ca reprezentand operatiuni de prelucrare legale compatibile. Temeiul juridic prevazut in dreptul Uniunii sau in dreptul intern pentru prelucrarea datelor cu caracter personal poate constitui, de asemenea, un temei juridic pentru prelucrarea ulterioara. Pentru a stabili daca scopul prelucrarii ulterioare este compatibil cu scopul pentru care au fost colectate initial datele cu caracter personal, operatorul, dupa ce a indeplinit toate cerintele privind legalitatea prelucrarii initiale, ar trebui sa tina seama, printre altele, de orice legatura intre respectivele scopuri si scopurile prelucrarii ulterioare preconizate, de contextul in care au fost colectate datele cu caracter personal, in special de asteptarile rezonabile ale persoanelor vizate, bazate pe relatia lor cu operatorul, in ceea ce priveste utilizarea ulterioara a datelor, de natura datelor cu caracter personal, de consecintele prelucrarii ulterioare preconizate asupra persoanelor vizate, precum si de existenta garantiilor corespunzatoare atat in cadrul operatiunilor de prelucrare initiale, cat si in cadrul operatiunilor de prelucrare ulterioare preconizate.

In cazul in care persoana vizata si-a dat consimtamantul sau prelucrarea se bazeaza pe dreptul Uniunii sau pe dreptul intern, care constituie o masura necesara si proportionala intr-o societate democratica pentru a proteja, in special, obiective importante de interes public general, operatorul ar trebui sa aiba posibilitatea de a prelucra in continuare datele cu caracter personal, indiferent de compatibilitatea scopurilor. In orice caz, aplicarea principiilor stabilite de prezentul regulament si, in special, informarea persoanei vizate cu privire la aceste alte scopuri si la drepturile sale, inclusiv dreptul la opozitie, ar trebui sa fie garantate. Indicarea unor posibile infractiuni sau amenintari la adresa sigurantei publice de catre operator si transmiterea catre o autoritate competenta a datelor cu caracter personal relevante in cazuri individuale sau in mai multe cazuri legate de aceeasi infractiune sau de aceleasi amenintari la adresa sigurantei publice ar trebui considerata ca fiind in interesul legitim urmarit de operator. Cu toate acestea, o astfel de transmitere in interesul legitim al operatorului sau prelucrarea ulterioara a datelor cu caracter personal ar trebui interzisa in cazul in care prelucrarea nu este compatibila cu o obligatie legala, profesionala sau cu o alta obligatie de pastrare a confidentialitatii.

(51) Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile in ceea ce priveste drepturile si libertatile fundamentale necesita o protectie specifica, deoarece contextul prelucrarii acestora ar putea genera riscuri considerabile la adresa drepturilor si libertatilor fundamentale. Aceste date cu caracter personal ar trebui sa includa datele cu caracter personal care dezvaluie originea rasiala sau etnica, utilizarea termenului "origine rasiala" in prezentul regulament neimplicand o acceptare de catre Uniune a teoriilor care urmaresc sa stabileasca existenta unor rase umane separate. Prelucrarea fotografiilor nu ar trebui sa fie considerata in mod sistematic ca fiind o prelucrare de categorii speciale de date cu caracter personal, intrucat fotografiile intra sub incidenta definitiei datelor biometrice doar in cazurile in care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unica sau autentificarea unei persoane fizice. Asemenea date cu caracter personal nu ar trebui prelucrate, cu exceptia cazului in care prelucrarea este permisa in cazuri specifice prevazute de prezentul regulament, tinand seama de faptul ca dreptul statelor membre poate prevedea dispozitii specifice cu privire la protectia datelor in scopul adaptarii aplicarii normelor din prezentul regulament in vederea respectarii unei

obligatii legale sau a indeplinirii unei sarcini care serveste unui interes public sau care rezulta din exercitarea autoritatii publice cu care este investit operatorul. Pe langa cerintele specifice pentru o astfel de prelucrare, ar trebui sa se aplice principiile generale si alte norme prevazute de prezentul regulament, in special in ceea ce priveste conditiile pentru prelucrarea legala. Ar trebui prevazute in mod explicit derogari de la interdictia generala de prelucrare a acestor categorii speciale de date cu caracter personal, printre altele atunci cand persoana vizata isi da consimtamantul explicit sau in ceea ce priveste nevoile specifice in special atunci cand prelucrarea este efectuata in cadrul unor activitati legitime de catre anumite asociatii sau fundatii al caror scop este de a permite exercitarea libertatilor fundamentale.

(52) Derogarea de la interdictia privind prelucrarea categoriilor speciale de date cu caracter personal ar trebui sa fie permisa, de asemenea, in cazul in care dreptul Uniunii sau dreptul intern prevede acest lucru si ar trebui sa faca obiectul unor garantii adecvate, astfel incat sa fie protejate datele cu caracter personal si alte drepturi fundamentale, atunci cand acest lucru se justifica din motive de interes public, in special in cazul prelucrarii datelor cu caracter personal in domeniul legislatiei privind ocuparea fortei de munca, protectia sociala, inclusiv pensiile, precum si in scopuri de securitate, supraveghere si alerta in materie de sanatate, pentru prevenirea sau controlul bolilor transmisibile si a altor amenintari grave la adresa sanatatii. Aceasta derogare poate fi acordata in scopuri medicale, inclusiv sanatatea publica si gestionarea serviciilor de asistenta medicala, in special in vederea asigurarii calitatii si eficientei din punctul de vedere al costurilor ale procedurilor utilizate pentru solutionarea cererilor de prestatii si servicii in cadrul sistemului de asigurari de sanatate, sau in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice. De asemenea, prelucrarea unor asemenea date cu caracter personal ar trebui permisa, printr-o derogare, atunci cand este necesara pentru constatarea, exercitarea sau apararea unui drept in justitie, indiferent daca are loc in cadrul unei proceduri in fata unei instante sau in cadrul unei proceduri administrative sau a unei proceduri extrajudiciare.

(53) Categoriile speciale de date cu caracter personal care necesita un nivel mai ridicat de protectie ar trebui prelucrate doar in scopuri legate de sanatate atunci cand este necesar pentru realizarea acestor scopuri in beneficiul persoanelor fizice si al societatii in general, in special in contextul gestionarii serviciilor si sistemelor de sanatate sau de asistenta sociala, inclusiv prelucrarea acestor date de catre autoritatile de management si de catre autoritatile centrale nationale din domeniul sanatatii in scopul controlului calitatii, furnizarii de informatii de gestiune si al supravegherii generale a sistemului de sanatate sau de asistenta sociala la nivel national si local, precum si in contextul asigurarii continuitatii asistentei medicale sau sociale si a asistentei medicale transfrontaliere ori in scopuri de securitate, supraveghere si alerta in materie de sanatate ori in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice in temeiul dreptului Uniunii sau al dreptului intern, care trebuie sa urmareasca un obiectiv de interes public, precum si in cazul studiilor realizate in interes public in domeniul sanatatii publice. Prin urmare, prezentul regulament ar trebui sa prevada conditii armonizate pentru prelucrarea categoriilor speciale de date cu caracter personal privind sanatatea, in ceea ce priveste nevoile specifice, in special atunci cand prelucrarea acestor date este efectuata in anumite scopuri legate de sanatate de catre persoane care fac obiectul unei obligatii legale de a pastra secretul profesional. Dreptul Uniunii sau dreptul intern ar trebui sa prevada masuri specifice si adecvate pentru a proteja drepturile fundamentale si datele cu caracter personal ale persoanelor fizice. Statele membre ar trebui sa aiba posibilitatea de a mentine sau de a introduce conditii suplimentare, inclusiv restrictii, in ceea ce priveste prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sanatatea. Totusi, acest lucru nu ar trebui sa impiedice libera circulatie a datelor cu caracter personal in cadrul Uniunii atunci cand aceste conditii se aplica prelucrarii transfrontaliere a unor astfel de date.

(54) Prelucrarea categoriilor speciale de date cu caracter personal poate fi necesara din motive de interes public in domeniile sanatatii publice, fara consimtamantul persoanei vizate. O astfel de prelucrare ar trebui conditionata de masuri adecvate si specifice destinate sa protejeze drepturile si libertatile persoanelor fizice. In acest context, conceptul de "sanatate publica" ar trebui interpretat astfel cum este definit in Regulamentul (CE) nr. 1338/2008 al Parlamentului European si al Consiliului, si anume toate elementele referitoare la sanatate si anume starea de sanatate, inclusiv morbiditatea sau handicapul, factorii determinanti care au efect asupra starii de sanatate, necesitatile in domeniul asistentei medicale, resursele alocate asistentei medicale, furnizarea asistentei medicale si asigurarea accesului universal la aceasta, precum si cheltuielile si sursele de finantare in domeniul sanatatii si cauzele mortalitatii. Aceasta prelucrare a datelor privind sanatatea din motive de interes public nu ar trebui sa duca la prelucrarea acestor date in alte scopuri de catre parti terte, cum ar fi angajatorii sau societatile de asigurari si bancile.

(55) In plus, prelucrarea datelor cu caracter personal de catre autoritatile publice in vederea realizarii obiectivelor prevazute de dreptul constitutional sau de dreptul international public, ale asociatiilor religioase recunoscute oficial se efectueaza din motive de interes public.

(56) In cazul in care, in cadrul activitatilor electorale, functionarea sistemului democratic necesita, intr-un stat membru, ca partidele politice sa colecteze date cu caracter personal privind opiniile politice ale persoanelor, prelucrarea unor astfel de date poate fi permisa din motive de interes public, cu conditia sa se prevada garantiile corespunzatoare.

(57) Daca datele cu caracter personal prelucrate de un operator nu ii permit acestuia sa identifice o persoana fizica, operatorul de date nu ar trebui sa aiba obligatia de a obtine informatii suplimentare in vederea identificarii persoanei vizate, cu unicul scop de a respecta oricare dintre dispozitiile prezentului regulament. Cu toate acestea, operatorul nu ar trebui sa refuze sa preia informatiile suplimentare furnizate de persoana vizata cu scopul de a sprijini exercitarea drepturilor acesteia. Identificarea ar trebui sa includa identificarea digitala a unei persoane vizate, de exemplu prin mecanisme de autentificare precum aceleasi acreditari utilizate de catre persoana vizata pentru a accesa serviciile online oferite de operatorul de date.

(58) Principiul transparentei prevede ca orice informatii care se adreseaza publicului sau persoanei vizate sa fie concise, usor accesibile si usor de inteles si sa se utilizeze un limbaj simplu si clar, precum si vizualizare acolo unde este cazul. Aceste informatii ar putea fi furnizate in format electronic, de exemplu atunci cand sunt adresate publicului, prin intermediul unui site. Acest lucru este important in special in situatii in care datorita multitudinii actorilor si a complexitatii, din punct de vedere tehnologic, a practicii, este dificil ca persoana vizata sa stie si sa inteleaga daca datele cu caracter personal care o privesc sunt colectate, de catre cine si in ce scop, cum este cazul publicitatii online. Intrucat copiii necesita o protectie specifica, orice informatii si orice comunicare, in cazul in care prelucrarea vizeaza un copil, ar trebui sa fie exprimate intr-un limbaj simplu si clar, astfel incat copilul sa il poata intelege cu usurinta.

(59) Ar trebui sa fie prevazute modalitati de facilitare a exercitarii de catre persoana vizata a drepturilor care ii sunt conferite prin prezentul regulament, inclusiv mecanismele prin care aceasta poate solicita si, daca este cazul, obtine, in mod gratuit, in special, acces la datele cu caracter personal, precum si rectificarea sau stergerea acestora, si exercitarea dreptului la opozitie. Operatorul ar trebui sa ofere, de asemenea, modalitati de introducere a cererilor pe cale electronica, mai ales in cazul in care datele cu caracter personal sunt prelucrate prin mijloace electronice. Operatorul ar trebui sa aiba obligatia de a raspunde cererilor persoanelor vizate fara intarzieri nejustificate si cel tarziu in termen de o luna si, in cazul in care nu intentioneaza sa se conformeze respectivele cereri, sa motiveze acest refuz.

(60) Conform principiilor prelucrarii echitabile si transparente, persoana vizata este informata cu privire la existenta unei operatiuni de prelucrare si la scopurile acesteia. Operatorul ar trebui sa furnizeze persoanei vizate orice informatii suplimentare necesare pentru a asigura o prelucrare echitabila si transparenta, tinand seama de circumstantele specifice si de contextul in care sunt prelucrate datele cu caracter personal. In plus, persoana vizata ar trebui informata cu privire la crearea de profiluri, precum si la consecintele acesteia. Atunci cand datele cu caracter personal sunt colectate de la persoana vizata, aceasta ar trebui informata, de asemenea, daca are obligatia de a furniza datele cu caracter personal si care sunt consecintele in cazul unui refuz. Aceste informatii pot fi furnizate in combinatie cu pictograme standardizate pentru a oferi intr-un mod usor vizibil, inteligibil si clar lizibil o imagine de ansamblu semnificativa asupra prelucrarii avute in vedere. In cazul in care pictogramele sunt prezentate in format electronic, acestea ar trebui sa poata fi citite automat.

(61) Informatiile in legatura cu prelucrarea datelor cu caracter personal referitoare la persoana vizata ar trebui furnizate acesteia la momentul colectarii de la persoana vizata sau, in cazul in care datele cu caracter personal sunt obtinute din alta sursa, intr-o perioada rezonabila, in functie de circumstantele cazului. In cazul in care datele cu caracter personal pot fi divulgate in mod legitim unui alt destinatar, persoana vizata ar trebui informata atunci cand datele cu caracter personal sunt divulgate pentru prima data destinatarului. In cazul in care operatorul intentioneaza sa prelucreze datele cu caracter personal intr-un alt scop decat cel pentru care acestea au fost colectate, operatorul ar trebui sa furnizeze persoanei vizate, inainte de aceasta prelucrare ulterioara, informatii privind scopul secundar respectiv si alte informatii necesare. In cazul in care originea datelor cu caracter personal nu a putut fi comunicata persoanei vizate din cauza ca au fost utilizate surse diverse, informatiile generale ar trebui furnizate.

(62) Cu toate acestea, nu este necesara impunerea obligatiei de a furniza informatii in cazul in care persoana vizata detine deja informatiile, in cazul in care inregistrarea sau divulgarea datelor cu caracter personal este prevazuta in mod expres de lege sau in cazul in care informarea persoanei vizate se dovedeste imposibila sau ar implica eforturi disproportionate. Acesta din urma ar putea fi cazul in special atunci cand prelucrarea se

efectueaza in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice. In aceasta privinta, ar trebui luate in considerare numarul persoanelor vizate, vechimea datelor si orice garantii adecvate adoptate.

(63) O persoana vizata ar trebui sa aiba drept de acces la datele cu caracter personal colectate care o privesc si ar trebui sa isi exercite acest drept cu usurinta si la intervale de timp rezonabile, pentru a fi informata cu privire la prelucrare si pentru a verifica legalitatea acesteia. Acest lucru include dreptul persoanelor vizate de a avea acces la datele lor privind sanatatea, de exemplu datele din registrele lor medicale continand informatii precum diagnostice, rezultate ale examinarilor, evaluari ale medicilor curanti si orice tratament sau interventie efectuata. Orice persoana vizata ar trebui, prin urmare, sa aiba dreptul de a cunoaste si de a i se comunica in special scopurile in care sunt prelucrate datele, daca este posibil perioada pentru care se prelucreaza datele cu caracter personal, destinatarii datelor cu caracter personal, logica de prelucrare automata a datelor cu caracter personal si, cel putin in cazul in care se bazeaza pe crearea de profiluri, consecintele unei astfel de prelucrari. Daca acest lucru este posibil, operatorul de date ar trebui sa poata furniza acces de la distanta la un sistem sigur, care sa ofere persoanei vizate acces direct la datele sale cu caracter personal. Acest drept nu ar trebui sa aduca atingere drepturilor sau libertatilor altora, inclusiv secretului comercial sau proprietatii intelectuale si, in special, drepturilor de autor care asigura protectia programelor software. Cu toate acestea, consideratiile de mai sus nu ar trebui sa aiba drept rezultat refuzul de a furniza toate informatiile persoanei vizate. Atunci cand operatorul prelucreaza un volum mare de informatii privind persoana vizata, operatorul ar trebui sa poata solicita ca, inainte de a ii fi furnizate informatiile, persoana vizata sa precizeze informatiile sau activitatile de prelucrare la care se refera cererea sa.

(64) Operatorul ar trebui sa ia toate masurile rezonabile pentru a verifica identitatea unei persoane vizate care solicita acces la date, in special in contextul serviciilor online si al identificatorilor online. Un operator nu ar trebui sa retina datele cu caracter personal in scopul exclusiv de a fi in masura sa reactioneze la cereri potentiale.

(65) O persoana vizata ar trebui sa aiba dreptul la rectificarea datelor cu caracter personal care o privesc si "dreptul de a fi uitata", in cazul in care pastrarea acestor date incalca prezentul regulament sau dreptul Uniunii sau dreptul intern sub incidenta caruia intra operatorul. In special, persoanele vizate ar trebui sa aiba dreptul ca datele lor cu caracter personal sa fie sterse si sa nu mai fie prelucrate, in cazul in care datele cu caracter personal nu mai sunt necesare pentru scopurile in care sunt colectate sau sunt prelucrate, in cazul in care persoanele vizate si-au retras consimtamantul pentru prelucrare sau in cazul in care acestea se opun prelucrarii datelor cu caracter personal care le privesc sau in cazul in care prelucrarea datelor cu caracter personal ale acestora nu este conforma cu prezentul regulament. Acest drept este relevant in special in cazul in care persoana vizata si-a dat consimtamantul cand era copil si nu cunostea pe deplin riscurile pe care le implica prelucrarea, iar ulterior doreste sa elimine astfel de date cu caracter personal, in special de pe internet. Persoana vizata ar trebui sa aiba posibilitatea de a-si exercita acest drept in pofida faptului ca nu mai este copil. Cu toate acestea, pastrarea in continuare a datelor cu caracter personal ar trebui sa fie legala in cazul in care este necesara pentru exercitarea dreptului la libertatea de exprimare si de informare, pentru respectarea unei obligatii legale, pentru indeplinirea unei sarcini care serveste unui interes public sau care rezulta din exercitarea autoritatii publice cu care este investit operatorul, din motive de interes public in domeniul sanatatii publice, in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice sau pentru constatarea, exercitarea sau apararea unui drept in instanta.

(66) Pentru a se consolida "dreptul de a fi uitat" in mediul online, dreptul de stergere ar trebui sa fie extins astfel incat un operator care a facut publice date cu caracter personal ar trebui sa aiba obligatia de a informa operatorii care prelucreaza respectivele date cu caracter personal sa stearga orice linkuri catre datele respective sau copii sau reproduceri ale acestora. In acest scop, operatorul in cauza ar trebui sa ia masuri rezonabile, tinand seama de tehnologia disponibila si de mijloacele aflate la dispozitia lui, inclusiv masuri tehnice, pentru a informa operatorii care prelucreaza datele cu caracter personal in ceea ce priveste cererea persoanei vizate.

(67) Metodele de restrictionare a prelucrarii de date cu caracter personal ar putea include, printre altele, mutarea temporara a datelor cu caracter personal selectate intr-un alt sistem de prelucrare, sau anularea accesului utilizatorilor la datele selectate sau inlaturarea temporara a datelor publicate de pe un site. In ceea ce priveste sistemele automatizate de evidenta a datelor, restrictionarea prelucrarii ar trebui, in principiu, asigurata prin mijloace tehnice in asa fel incat datele cu caracter personal sa nu faca obiectul unor operatiuni de prelucrare ulterioara si sa nu mai poata fi schimbate. Faptul ca prelucrarea datelor cu caracter personal este restrictionata ar trebui indicat in mod clar in sistem.

(68) Pentru a spori suplimentar controlul asupra propriilor date, persoana vizata ar trebui, in cazul in care datele cu caracter personal sunt prelucrate prin mijloace automate, sa poata primi datele cu caracter personal care o privesc si pe care le-a furnizat unui operator, intr-un format structurat, utilizat in mod curent, prelucrabil automat si interoperabil si sa le poata transmite unui alt operator. Operatorii de date ar trebui sa fie incurajati sa dezvolte formate interoperabile care sa permita portabilitatea datelor. Acest drept ar trebui sa se aplice in cazul in care persoana vizata a furnizat datele cu caracter personal pe baza propriului consimtamant sau in cazul in care prelucrarea datelor este necesara pentru executarea unui contract. Acest drept nu ar trebui sa se aplice in cazul in care prelucrarea se bazeaza pe un alt temei juridic decat consimtamantul sau contractul. Prin insasi natura sa, acest drept nu ar trebui exercitat impotriva operatorilor care prelucreaza date cu caracter personal in cadrul exercitarii functiilor lor publice. Acesta nu ar trebui sa se aplice in special in cazul in care prelucrarea de date cu caracter personal este necesara in vederea respectarii unei obligatii legale careia ii este supus operatorul sau in cazul indeplinirii unei sarcini care serveste unui interes public sau care rezulta din exercitarea unei autoritati publice cu care este investit operatorul. Dreptul persoanei vizate de a transmite sau de a primi date cu caracter personal care o privesc nu ar trebui sa creeze pentru operatori obligatia de a adopta sau de a mentine sisteme de prelucrare care sa fie compatibile din punct de vedere tehnic. In cazul in care, intr-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 sa aduca atingere drepturilor si libertatilor altor persoane vizate, in conformitate cu prezentul regulament. De asemenea, acest drept nu ar trebui sa aduca atingere dreptului persoanei vizate de a obtine stergerea datelor cu caracter personal si limitarilor dreptului respectiv, astfel cum sunt prevazute in prezentul regulament, si nu ar trebui, in special, sa implice stergerea acelor date cu caracter personal referitoare la persoana vizata care au fost furnizate de catre aceasta in vederea executarii unui contract, in masura in care si atat timp cat datele respective sunt necesare pentru executarea contractului. Persoana vizata ar trebui sa aiba dreptul ca datele cu caracter personal sa fie transmise direct de la un operator la altul, daca acest lucru este fezabil din punct de vedere tehnic.

(69) In cazurile in care datele cu caracter personal ar putea fi prelucrate in mod legal deoarece prelucrarea este necesara pentru indeplinirea unei sarcini care serveste unui interes public sau care rezulta din exercitarea autoritatii publice cu care este investit operatorul sau pe baza intereselor legitime ale unui operator sau ale unei parti terte, o persoana vizata ar trebui sa aiba totusi dreptul de a se opune prelucrarii oricaror date cu caracter personal care se refera la situatia sa particulara. Ar trebui sa revina operatorului sarcina de a demonstra ca interesele sale legitime si imperioase prevaleaza asupra intereselor sau a drepturilor si libertatilor fundamentale ale persoanei vizate.

(70) In cazul in care datele cu caracter personal sunt prelucrate in scopuri de marketing direct, persoana vizata ar trebui sa aiba dreptul de a se opune unei astfel de prelucrari, inclusiv crearii de profiluri in masura in care aceasta are legatura cu marketingul direct, indiferent daca prelucrarea in cauza este cea initiala sau una ulterioara, in orice moment si in mod gratuit. Acest drept ar trebui adus in mod explicit in atentia persoanei vizate si prezentat in mod clar si separat de orice alte informatii.

(71) Persoana vizata ar trebui sa aiba dreptul de a nu face obiectul unei decizii, care poate include o masura, care evalueaza aspecte personale referitoare la persoana vizata, care se bazeaza exclusiv pe prelucrarea automata si care produce efecte juridice care privesc persoana vizata sau o afecteaza in mod similar intr-o masura semnificativa, cum ar fi refuzul automat al unei cereri de credit online sau practicile de recrutare pe cale electronica, fara interventie umana. O astfel de prelucrare include "crearea de profiluri", care consta in orice forma de prelucrare automata a datelor cu caracter personal prin evaluarea aspectelor personale referitoare la o persoana fizica, in special in vederea analizarii sau preconizarii anumitor aspecte privind randamentul la locul de munca al persoanei vizate, situatia economica, starea de sanatate, preferintele sau interesele personale, fiabilitatea sau comportamentul, locatia sau deplasarile, atunci cand aceasta produce efecte juridice care privesc persoana vizata sau o afecteaza in mod similar intr-o masura semnificativa. Cu toate acestea, luarea de decizii pe baza unei astfel de prelucrari, inclusiv crearea de profiluri, ar trebui permisa in cazul in care este autorizata in mod expres in dreptul Uniunii sau in dreptul intern care se aplica operatorului, inclusiv in scopul monitorizarii si prevenirii fraudei si a evaziunii fiscale, desfasurate in conformitate cu reglementarile, standardele si recomandarile institutiilor Uniunii sau ale organismelor nationale de supraveghere, si in scopul asigurarii securitatii si fiabilitatii unui serviciu oferit de operator sau in cazul in care este necesara pentru incheierea sau executarea unui contract intre persoana vizata si un operator sau in cazul in care persoana vizata si-a dat in mod explicit consimtamantul. In orice caz, o astfel de prelucrare ar trebui sa faca obiectul unor garantii corespunzatoare, care ar trebui sa includa o informare specifica a persoanei vizate si dreptul acesteia de a obtine interventie umana, de a-si exprima punctul de vedere, de a primi o explicatie privind decizia luata in urma unei

astfel de evaluari, precum si dreptul de a contesta decizia. O astfel de masura nu ar trebui sa se refere la un copil.

Pentru a asigura o prelucrare echitabila si transparenta in ceea ce priveste persoana vizata, avand in vedere circumstantele specifice si contextul in care sunt prelucrate datele cu caracter personal, operatorul ar trebui sa utilizeze proceduri matematice sau statistice adecvate pentru crearea de profiluri, sa implementeze masuri tehnice si organizatorice adecvate pentru a asigura in special faptul ca factorii care duc la inexactitati ale datelor cu caracter personal sunt corectati si ca riscul de erori este redus la minimum, precum si sa securizeze datele cu caracter personal intr-un mod care sa tina seama de pericolele potentiale la adresa intereselor si drepturilor persoanei vizate si care sa previna, printre altele, efectele discriminatorii impotriva persoanelor pe motiv de rasa sau origine etnica, opinii politice, religie sau convingeri, apartenenta sindicala, caracteristici genetice, stare de sanatate sau orientare sexuala sau care sa duca la masuri care sa aiba astfel de efecte. Procesul decizional automatizat si crearea de profiluri pe baza unor categorii speciale de date cu caracter personal ar trebui permise numai in conditii specifice.

(72) Crearea de profiluri este supusa normelor prezentului regulament care reglementeaza prelucrarea datelor cu caracter personal, precum temeiurile juridice ale prelucrarii sau principiile de protectie a datelor. Comitetul european pentru protectia datelor instituit prin prezentul regulament ("comitetul") ar trebui sa poata emite orientari in acest context.

(73) Dreptul Uniunii sau dreptul intern poate impune restrictii in privinta unor principii specifice, in privinta dreptului de informare, a dreptului de acces la datele cu caracter personal si de rectificare sau stergere a acestora, in privinta dreptului la portabilitatea datelor, a dreptului la opozitie, a deciziilor bazate pe crearea de profiluri, precum si in privinta comunicarii unei incalcari a securitatii datelor cu caracter personal persoanei vizate si a anumitor obligatii conexe ale operatorilor, in masura in care acest lucru este necesar si proportional intr-o societate democratica pentru a se garanta siguranta publica, inclusiv protectia vietii oamenilor, in special ca raspuns la dezastre naturale sau provocate de om, prevenirea, investigarea si urmarirea penala a infractiunilor sau executarea pedepselor, inclusiv protejarea impotriva amenintarilor la adresa sigurantei publice sau impotriva incalcarii eticii in cazul profesiilor reglementate si prevenirea acestora, alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, in special un interes economic sau financiar important al Uniunii sau al unui stat membru, mentinerea de registre publice din motive de interes public general, prelucrarea ulterioara a datelor cu caracter personal arhivate pentru a transmite informatii specifice legate de comportamentul politic in perioada regimurilor fostelor state totalitare, protectia persoanei vizate sau a drepturilor si libertatilor unor terti, inclusiv protectia sociala, sanatatea publica si scopurile umanitare. Aceste restrictii ar trebui sa fie conforme cu cerintele prevazute de carta si de Conventia europeana pentru apararea drepturilor omului si a libertatilor fundamentale.

(74) Ar trebui sa se stabileasca responsabilitatea si raspunderea operatorului pentru orice prelucrare a datelor cu caracter personal efectuata de catre acesta sau in numele sau. In special, operatorul ar trebui sa fie obligat sa implementeze masuri adecvate si eficace si sa fie in masura sa demonstreze conformitatea activitatilor de prelucrare cu prezentul regulament, inclusiv eficacitatea masurilor. Aceste masuri ar trebui sa tina seama de natura, domeniul de aplicare, contextul si scopurile prelucrarii, precum si de riscul pentru drepturile si libertatile persoanelor fizice.

(75) Riscul pentru drepturile si libertatile persoanelor fizice, prezentand grade diferite de probabilitate de materializare si de gravitate, poate fi rezultatul unei prelucrari a datelor cu caracter personal care ar putea genera prejudicii de natura fizica, materiala sau morala, in special in cazurile in care: prelucrarea poate conduce la discriminare, furt sau frauda a identitatii, pierdere financiara, compromiterea reputatiei, pierderea confidentialitatii datelor cu caracter personal protejate prin secret profesional, inversarea neautorizata a pseudonimizarii sau la orice alt dezavantaj semnificativ de natura economica sau sociala; persoanele vizate ar putea fi private de drepturile si libertatile lor sau impiedicate sa-si exercite controlul asupra datelor lor cu caracter personal; datele cu caracter personal prelucrate sunt date care dezvaluie originea rasiala sau etnica, opiniile politice, religia sau convingerile filozofice, apartenenta sindicala; sunt prelucrate date genetice, date privind sanatatea sau date privind viata sexuala sau privind condamnarile penale si infractiunile sau masurile de securitate conexe; sunt evaluate aspecte de natura personala, in special analizarea sau previzionarea unor aspecte privind randamentul la locul de munca, situatia economica, starea de sanatate, preferintele sau interesele personale, fiabilitatea sau comportamentul, locatia sau deplasarile, in scopul de a se crea sau de a se utiliza profiluri personale; sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, in special ale unor copii; sau prelucrarea implica un volum mare de date cu caracter personal si afecteaza un numar larg de persoane vizate.

(76) Probabilitatea de a se materializa si gravitatea riscului pentru drepturile si libertatile persoanei vizate ar trebui sa fie determinate in functie de natura, domeniul de aplicare, contextul si scopurile prelucrarii datelor cu caracter personal. Riscul ar trebui apreciat pe baza unei evaluari obiective prin care se stabileste daca operatiunile de prelucrare a datelor prezinta un risc sau un risc ridicat.

(77) Orientari pentru implementarea unor masuri adecvate si pentru demonstrarea conformitatii de catre operator sau persoana imputernicita de operator, mai ales in ceea ce priveste identificarea riscului legat de prelucrare, evaluarea acestuia din punctul de vedere al originii, naturii, probabilitatii de a se materializa si al gravitatii, precum si identificarea bunelor practici pentru atenuarea riscului ar putea fi oferite in special prin coduri de conduita aprobate, certificari aprobate, orientari ale comitetului sau prin indicatii furnizate de un responsabil cu protectia datelor. Comitetul poate, de asemenea, sa emita orientari cu privire la operatiunile de prelucrare care sunt considerate putin susceptibile de a genera un risc ridicat pentru drepturile si libertatile persoanelor fizice si sa indice masurile care se pot dovedi suficiente in asemenea cazuri pentru a aborda un astfel de risc.

(78) Protectia drepturilor si libertatilor persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal necesita adoptarea de masuri tehnice si organizatorice corespunzatoare pentru a se asigura indeplinirea cerintelor din prezentul regulament. Pentru a fi in masura sa demonstreze conformitatea cu prezentul regulament, operatorul ar trebui sa adopte politici interne si sa puna in aplicare masuri care sa respecte in special principiul protectiei datelor incepand cu momentul conceperii si cel al protectiei implicite a datelor. Astfel de masuri ar putea consta, printre altele, in reducerea la minimum a prelucrarii datelor cu caracter personal, pseudonimizarea acestor date cat mai curand posibil, transparenta in ceea ce priveste functiile si prelucrarea datelor cu caracter personal, abilitarea persoanei vizate sa monitorizeze prelucrarea datelor, abilitarea operatorului sa creeze elemente de siguranta si sa le imbunatateasca. Atunci cand elaboreaza, proiecteaza, selecteaza si utilizeaza aplicatii, servicii si produse care se bazeaza pe prelucrarea datelor cu caracter personal sau care prelucreaza date cu caracter personal pentru a-si indeplini rolul, producatorii acestor produse si furnizorii acestor servicii si aplicatii ar trebui sa fie incurajati sa aiba in vedere dreptul la protectia datelor la momentul elaborarii si proiectarii unor astfel de produse, servicii si aplicatii si, tinand cont de stadiul actual al dezvoltarii, sa se asigure ca operatorii si persoanele imputernicite de operatori sunt in masura sa isi indeplineasca obligatiile referitoare la protectia datelor.Principiul protectiei datelor incepand cu momentul conceperii si cel al protectiei implicite a datelor ar trebui sa fie luate in considerare si in contextul licitatiilor publice.

(79) Protectia drepturilor si libertatilor persoanelor vizate, precum si responsabilitatea si raspunderea operatorilor si a persoanelor imputernicite de operator, inclusiv in ceea ce priveste monitorizarea de catre autoritatile de supraveghere si masurile adoptate de acestea, necesita o atribuire clara a responsabilitatilor in temeiul prezentului regulament, inclusiv in cazul in care un operator stabileste scopurile si mijloacele prelucrarii impreuna cu alti operatori sau in cazul in care o operatiune de prelucrare este efectuata in numele unui operator.

(80) Atunci cand un operator sau o persoana imputernicita de operator care nu este stabilita in Uniune prelucreaza date cu caracter personal ale unor persoane vizate care se afla pe teritoriul Uniunii, iar activitatile sale de prelucrare au legatura cu oferirea de bunuri sau servicii unor astfel de persoane vizate in Uniune, indiferent daca se solicita sau nu efectuarea unei plati de catre persoana vizata, sau cu monitorizarea comportamentului unor persoane vizate daca acesta se manifesta in cadrul Uniunii, operatorul sau persoana imputernicita de operator ar trebui sa desemneze un reprezentant, cu exceptia cazului in care prelucrarea are caracter ocazional, nu include prelucrarea pe scara larga a unor categorii speciale de date cu caracter personal si nici prelucrarea de date referitoare la condamnari penale si la infractiuni, si este putin susceptibila sa genereze un risc pentru drepturile si libertatile persoanelor fizice, avand in vedere natura, contextul, domeniul de aplicare si scopurile prelucrarii, precum si a cazului in care operatorul este o autoritate publica sau un organism public. Reprezentantul ar trebui sa actioneze in numele operatorului sau al persoanei imputernicite de operator, putand fi contactat de orice autoritate de supraveghere. Reprezentantul ar trebui desemnat in mod explicit, printr-un mandat scris al operatorului sau al persoanei imputernicite de operator, sa actioneze in numele acestuia (acesteia) in ceea ce priveste obligatiile lor in temeiul prezentului regulament. Desemnarea unui astfel de reprezentant nu aduce atingere responsabilitatii sau raspunderii operatorului sau a persoanei imputernicite de operator in temeiul prezentului regulament. Un astfel de reprezentant ar trebui sa isi indeplineasca sarcinile in conformitate cu mandatul primit de la operator sau de la persoana imputernicita de operator, inclusiv sa coopereze cu autoritatile de supraveghere competente in ceea ce priveste orice actiune intreprinsa pentru a asigura respectarea prezentului regulament. Reprezentantul desemnat ar trebui sa fie supus unor proceduri de

asigurare a respectarii legii in cazul nerespectarii prezentului regulament de catre operator sau de catre persoana imputernicita de operator.

(81) Pentru a asigura respectarea cerintelor impuse de prezentul regulament in ceea ce priveste prelucrarea care trebuie efectuata in numele operatorului de catre persoana imputernicita de operator, atunci cand atribuie activitati de prelucrare unei persoane imputernicite de operator, acesta din urma ar trebui sa utilizeze numai persoane imputernicite care ofera garantii suficiente, in special in ceea ce priveste cunostintele de specialitate, fiabilitatea si resursele, pentru a implementa masuri tehnice si organizatorice care indeplinesc cerintele impuse de prezentul regulament, inclusiv pentru securitatea prelucrarii. Aderarea de catre persoana imputernicita de operator la un cod de conduita aprobat sau la un mecanism de certificare aprobat poate fi utilizata drept element care sa demonstreze respectarea obligatiilor de catre operator. Efectuarea prelucrarii de catre o persoana imputernicita de un operator ar trebui sa fie reglementata printr-un contract sau un alt tip de act juridic, in temeiul dreptului Uniunii sau al dreptului intern, care creeaza obligatii pentru persoana imputernicita de operator in raport cu operatorul si care stabileste obiectul si durata prelucrarii, natura si scopurile prelucrarii, tipul de date cu caracter personal si categoriile de persoane vizate, si ar trebui sa tina seama de sarcinile si responsabilitatile specifice ale persoanei imputernicite de operator in contextul prelucrarii care trebuie efectuata, precum si de riscul pentru drepturile si libertatile persoanei vizate. Operatorul si persoana imputernicita de operator pot alege sa utilizeze un contract individual sau clauze contractuale standard care sunt adoptate fie direct de Comisie, fie de o autoritate de supraveghere in conformitate cu mecanismul de asigurare a coerentei si apoi adoptate de Comisie. Dupa finalizarea prelucrarii in numele operatorului, persoana imputernicita de operator ar trebui sa returneze sau sa stearga, in functie de optiunea operatorului, datele cu caracter personal, cu exceptia cazului in care exista o cerinta de stocare a datelor cu caracter personal in temeiul dreptului Uniunii sau al dreptului intern care instituie obligatii pentru persoana imputernicita de operator.

(82) In vederea demonstrarii conformitatii cu prezentul regulament, operatorul sau persoana imputernicita de operator ar trebui sa pastreze evidente ale activitatilor de prelucrare aflate in responsabilitatea sa. Fiecare operator si fiecare persoana imputernicita de operator ar trebui sa aiba obligatia de a coopera cu autoritatea de supraveghere si de a pune la dispozitia acesteia, la cerere, aceste evidente, pentru a putea fi utilizate in scopul monitorizarii operatiunilor de prelucrare respective.

(83) In vederea mentinerii securitatii si a prevenirii prelucrarilor care incalca prezentul regulament, operatorul sau persoana imputernicita de operator ar trebui sa evalueze riscurile inerente prelucrarii si sa implementeze masuri pentru atenuarea acestor riscuri, cum ar fi criptarea. Masurile respective ar trebui sa asigure un nivel corespunzator de securitate, inclusiv confidentialitatea, luand in considerare stadiul actual al dezvoltarii si costurile implementarii in raport cu riscurile si cu natura datelor cu caracter personal a caror protectie trebuie asigurata. La evaluarea riscului pentru securitatea datelor cu caracter personal, ar trebui sa se acorde atentie riscurilor pe care le prezinta prelucrarea datelor, cum ar fi distrugerea, pierderea, modificarea, divulgarea neautorizata sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate in alt mod, in mod accidental sau ilegal, care pot duce in special la prejudicii fizice, materiale sau morale.

(84) Pentru a favoriza respectarea dispozitiilor prezentului regulament in cazurile in care operatiunile de prelucrare sunt susceptibile sa genereze un risc ridicat pentru drepturile si libertatile persoanelor fizice, operatorul ar trebui sa fie responsabil de efectuarea unei evaluari a impactului asupra protectiei datelor, care sa estimeze, in special, originea, natura, specificitatea si gravitatea acestui risc. Rezultatul evaluarii ar trebui luat in considerare la stabilirea masurilor adecvate care trebuie luate pentru a demonstra ca prelucrarea datelor cu caracter personal respecta prezentul regulament. In cazul in care o evaluare a impactului asupra protectiei datelor arata ca operatiunile de prelucrare implica un risc ridicat, pe care operatorul nu il poate atenua prin masuri adecvate sub aspectul tehnologiei disponibile si al costurilor implementarii, ar trebui sa aiba loc o consultare a autoritatii de supraveghere inainte de prelucrare.

(85) Daca nu este solutionata la timp si intr-un mod adecvat, o incalcare a securitatii 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 frauda de identitate, pierdere financiara, inversarea neautorizata a pseudonimizarii, compromiterea reputatiei, pierderea confidentialitatii datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natura economica sau sociala adus persoanei fizice in cauza. Prin urmare, de indata ce a luat cunostinta de producerea unei incalcari a securitatii datelor cu caracter personal, operatorul ar trebui sa notifice aceasta incalcare autoritatii de supraveghere, fara intarziere nejustificata si, daca este posibil, in cel mult 72 de ore dupa ce a luat la cunostinta de existenta acesteia, cu exceptia cazului in care operatorul este in masura sa demonstreze, in conformitate cu principiul responsabilitatii, ca incalcarea securitatii datelor cu caracter personal

nu este susceptibila sa genereze un risc pentru drepturile si libertatile persoanelor fizice. Atunci cand notificarea nu se poate realiza in termen de 72 de ore, aceasta ar trebui sa cuprinda motivele intarzierii, iar informatiile pot fi furnizate treptat, fara alta intarziere.

(86) Operatorul ar trebui sa comunice persoanei vizate o incalcare a securitatii datelor cu caracter personal, fara intarzieri nejustificate, atunci cand incalcarea este susceptibila sa genereze un risc ridicat pentru drepturile si libertatile persoanei fizice, pentru a-i permite sa ia masurile de precautie necesare. Comunicarea ar trebui sa descrie natura incalcarii securitatii datelor cu caracter personal si sa cuprinda recomandari pentru persoana fizica in cauza in scopul atenuarii eventualelor efecte negative. Comunicarile catre persoanele vizate ar trebui efectuate in cel mai scurt timp posibil in mod rezonabil si in stransa cooperare cu autoritatea de supraveghere, respectandu-se orientarile furnizate de aceasta sau de alte autoritati competente, cum ar fi autoritatile de aplicare a legii. De exemplu, necesitatea de a atenua un risc imediat de producere a unui prejudiciu ar presupune comunicarea cu promptitudine catre persoanele vizate, in timp ce necesitatea de a implementa masuri corespunzatoare impotriva incalcarii in continuare a securitatii datelor cu caracter personal sau impotriva unor incalcari similare ale securitatii datelor cu caracter personal ar putea justifica un termen mai indelungat pentru comunicare.

(87) Ar trebui sa se stabileasca daca au fost implementate toate masurile tehnologice de protectie si organizatorice corespunzatoare in scopul de a se stabili imediat daca s-a produs o incalcare a securitatii datelor cu caracter personal si de a se informa cu promptitudine autoritatea de supraveghere si persoana vizata. Faptul ca notificarea a fost efectuata fara intarziere nejustificata ar trebui stabilit luandu-se in considerare, in special, natura si gravitatea incalcarii securitatii datelor cu caracter personal, precum si consecintele si efectele negative ale acesteia asupra persoanei vizate. Aceasta notificare poate conduce la o interventie a autoritatii de supraveghere, in conformitate cu sarcinile si competentele specificate in prezentul regulament.

(88) La stabilirea de norme detaliate privind formatul si procedurile aplicabile notificarii referitoare la incalcarile securitatii datelor cu caracter personal, ar trebui sa se acorde atentia cuvenita circumstantelor in care a avut loc incalcarea, stabilindu-se inclusiv daca protectia datelor cu caracter personal a fost sau nu a fost asigurata prin masuri tehnice de protectie corespunzatoare, care sa limiteze efectiv probabilitatea fraudarii identitatii sau a altor forme de utilizare abuziva. In plus, astfel de norme si proceduri ar trebui sa tina cont de interesele legitime ale autoritatilor de aplicare a legii in cazurile in care divulgarea timpurie ar putea ingreuna in mod inutil investigarea circumstantelor in care a avut loc o incalcare a datelor cu caracter personal.

(89) Directiva 95/46/CE a prevazut o obligatie generala de a notifica prelucrarea datelor cu caracter personal autoritatilor de supraveghere. Cu toate ca obligatia respectiva genereaza sarcini administrative si financiare, aceasta nu a contribuit intotdeauna la imbunatatirea protectiei datelor cu caracter personal. Prin urmare, astfel de obligatii de notificare generala nediferentiata ar trebui sa fie abrogate si inlocuite cu proceduri si mecanisme eficace care sa puna accentul, in schimb, pe acele tipuri de operatiuni de prelucrare susceptibile sa genereze un risc ridicat pentru drepturile si libertatile persoanelor fizice prin insasi natura lor, prin domeniul lor de aplicare, prin contextul si prin scopurile lor. Astfel de tipuri de operatiuni de prelucrare pot fi cele care presupun, in special, utilizarea unor noi tehnologii sau care reprezinta un nou tip de operatiuni, pentru care nicio evaluare a impactului asupra protectiei datelor nu a fost efectuata anterior de catre operator ori care devin necesare data fiind perioada de timp care s-a scurs de la prelucrarea initiala.

(90) In astfel de cazuri, operatorul ar trebui sa efectueze, inainte de prelucrare, o evaluare a impactului asupra protectiei datelor, in scopul evaluarii gradului specific de probabilitate a materializarii riscului ridicat si gravitatea acestuia, avand in vedere natura, domeniul de aplicare, contextul si scopurile prelucrarii, precum si sursele riscului. Respectiva evaluare a impactului ar trebui sa includa, in special, masurile, garantiile si mecanismele avute in vedere pentru atenuarea riscului respectiv, pentru asigurarea protectiei datelor cu caracter personal si pentru demonstrarea conformitatii cu prezentul regulament.

(91) Aceasta ar trebui sa se aplice, in special, operatiunilor de prelucrare la scara larga, care au drept obiectiv prelucrarea unui volum considerabil de date cu caracter personal la nivel regional, national sau supranational, care ar putea afecta un numar mare de persoane vizate si care sunt susceptibile de a genera un risc ridicat, de exemplu, din cauza sensibilitatii lor, in cazul in care, in conformitate cu nivelul atins al cunostintelor tehnologice, se foloseste la scara larga o tehnologie noua, precum si altor operatiuni de prelucrare care genereaza un risc ridicat pentru drepturile si libertatile persoanelor vizate, in special in cazul in care operatiunile respective limiteaza capacitatea persoanelor vizate de a-si exercita drepturile. Ar trebui efectuata o evaluare a impactului asupra protectiei datelor si in situatiile in care datele cu caracter personal sunt prelucrate in scopul luarii de decizii care vizeaza anumite persoane fizice in urma unei evaluari sistematice si cuprinzatoare a aspectelor personale referitoare la persoane fizice, pe baza crearii de profiluri pentru datele respective, sau in

urma prelucrarii unor categorii speciale de date cu caracter personal, a unor date biometrice sau a unor date privind condamnarile penale si infractiunile sau masurile de securitate conexe. Este la fel de necesara o evaluare a impactului asupra protectiei datelor pentru monitorizarea la scara larga a zonelor accesibile publicului, mai ales in cazul utilizarii dispozitivelor optoelectronice sau pentru orice alte operatiuni in cazul in care autoritatea de supraveghere competenta considera ca prelucrarea este susceptibila de a genera un risc ridicat pentru drepturile si libertatile persoanelor vizate, in special deoarece acestea impiedica persoanele vizate sa exercite un drept sau sa utilizeze un serviciu ori un contract, sau deoarece acestea sunt efectuate in mod sistematic la scara larga. Prelucrarea datelor cu caracter personal nu ar trebui considerata a fi la scara larga in cazul in care prelucrarea se refera la date cu caracter personal de la pacienti sau clienti de catre un anumit medic, un alt profesionist in domeniul sanatatii sau un avocat. In aceste cazuri, o evaluare a impactului asupra protectiei datelor nu ar trebui sa fie obligatorie.

(92) In unele circumstante ar putea fi rezonabil si util din punct de vedere economic ca o evaluare a impactului asupra protectiei datelor sa aiba o perspectiva mai extinsa decat cea a unui singur proiect, de exemplu in cazul in care autoritati sau organisme publice intentioneaza sa instituie o aplicatie sau o platforma de prelucrare comuna sau in cazul in care mai multi operatori preconizeaza sa introduca o aplicatie comuna sau un mediu de prelucrare comun in cadrul unui sector sau segment industrial sau pentru o activitate orizontala utilizata la scara larga.

(93) In contextul adoptarii legislatiei nationale pe care se bazeaza indeplinirea sarcinilor autoritatii publice sau ale organismului public si care reglementeaza operatiunea sau seria de operatiuni de prelucrare in cauza, statele membre pot considera ca este necesara efectuarea unei astfel de evaluari inaintea desfasurarii activitatilor de prelucrare.

(94) In cazul in care o evaluare a impactului asupra protectiei datelor arata ca prelucrarea ar genera, in absenta garantiilor, masurilor de securitate si mecanismelor de atenuare a riscului, un risc ridicat pentru drepturile si libertatile persoanelor fizice, iar operatorul considera ca riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile si al costurilor implementarii, autoritatea de supraveghere ar trebui sa fie consultata inainte de inceperea activitatilor de prelucrare. Un astfel de risc ridicat este susceptibil sa fie generat de anumite tipuri de prelucrare, precum si de amploarea si frecventa prelucrarii, care pot duce si la producerea unor prejudicii sau pot atinge drepturile si libertatile persoanelor fizice. Autoritatea de supraveghere ar trebui sa raspunda cererii de consultare intr-un anumit termen. Cu toate acestea, lipsa unei reactii din partea autoritatii de supraveghere in termenul respectiv ar trebui sa nu aduca atingere niciunei interventii a autoritatii de supraveghere in conformitate cu sarcinile si competentele sale prevazute in prezentul regulament, inclusiv competenta de a interzice operatiuni de prelucrare. Ca parte a acestui proces de consultare, rezultatul unei evaluari a impactului asupra protectiei datelor efectuate cu privire la prelucrarea in cauza poate fi transmis autoritatii de supraveghere, in special masurile avute in vedere pentru a atenua riscul pentru drepturile si libertatile persoanelor fizice.

(95) Persoana imputernicita de operator ar trebui sa acorde asistenta operatorului, daca este necesar si la cerere, la asigurarea respectarii obligatiilor care decurg din realizarea de evaluari ale impactului asupra protectiei datelor si din consultarea prealabila a autoritatii de supraveghere.

(96) In timpul elaborarii unei masuri legislative sau de reglementare care prevede prelucrarea unor date cu caracter personal ar trebui, de asemenea, sa aiba loc o consultare a autoritatii de supraveghere, pentru a garanta conformitatea prelucrarii avute in vedere cu prezentul regulament si, in special, pentru a atenua riscul la care este expusa persoana vizata.

(97) In cazul in care prelucrarea este efectuata de o autoritate publica, cu exceptia instantelor sau a autoritatilor judiciare independente atunci cand actioneaza in calitatea lor judiciara, in cazul in care, in sectorul privat, prelucrarea este efectuata de un operator a carui activitate principala consta in operatiuni de prelucrare care necesita o monitorizare regulata si sistematica a persoanelor vizate pe scara larga, sau in cazul in care activitatea principala a operatorului sau a persoanei imputernicite de operator consta in prelucrarea pe scara larga de categorii speciale de date cu caracter personal si de date privind condamnarile penale si infractiunile, o persoana care detine cunostinte de specialitate in materie de legislatie si practici privind protectia datelor ar trebui sa acorde asistenta operatorului sau persoanei imputernicite de operator pentru monitorizarea conformitatii, la nivel intern, cu prezentul regulament. In sectorul privat, activitatile principale ale unui operator se refera la activitatile sale de baza, si nu la prelucrarea datelor cu caracter personal drept activitati auxiliare. Nivelul necesar al cunostintelor de specialitate ar trebui sa fie stabilit in special in functie de operatiunile de prelucrare a datelor efectuate si de nivelul de protectie impus pentru datele cu caracter personal prelucrate de operator sau de persoana imputernicita de operator. Acesti responsabili cu protectia datelor, indiferent daca sunt

sau nu angajati ai operatorului, ar trebui sa fie in masura sa isi indeplineasca atributiile si sarcinile in mod independent.

(98) Asociatiile sau alte organisme care reprezinta categorii de operatori sau de persoane imputernicite de operatori ar trebui incurajate sa elaboreze coduri de conduita, in limitele prezentului regulament, astfel incat sa se faciliteze aplicarea efectiva a prezentului regulament, luandu-se in considerare caracteristicile specifice ale prelucrarii efectuate in anumite sectoare si necesitatile specifice ale microintreprinderilor si ale intreprinderilor mici si mijlocii. In special, astfel de coduri de conduita ar putea sa ajusteze obligatiile operatorilor si ale persoanelor imputernicite de operatori, tinand seama de riscul aferent prelucrarii care este susceptibil de a fi generat pentru drepturile si libertatile persoanelor fizice.

(99) Atunci cand elaboreaza un cod de conduita sau cand modifica sau extind un astfel de cod, asociatiile si alte organisme care reprezinta categorii de operatori sau persoane imputernicite de operatori ar trebui sa consulte partile implicate relevante, inclusiv persoanele vizate, daca este fezabil, si sa ia in considerare contributiile transmise si opiniile exprimate in cadrul unor astfel de consultari.

(100) Pentru a se imbunatati transparenta si conformitatea cu prezentul regulament, ar trebui sa se incurajeze instituirea de mecanisme de certificare, precum si de sigilii si marci in materie de protectie a datelor, care sa permita persoanelor vizate sa evalueze rapid nivelul de protectie a datelor aferent produselor si serviciilor relevante.

(101) Fluxurile de date cu caracter personal catre si dinspre tari situate in afara Uniunii si organizatii internationale sunt necesare pentru dezvoltarea comertului international si a cooperarii internationale. Cresterea acestor fluxuri a generat noi provocari si preocupari cu privire la protectia datelor cu caracter personal. Cu toate acestea, in cazul in care se transfera date cu caracter personal din Uniune catre operatori, persoane imputernicite de operatori sau alti destinatari din tari terte sau organizatii internationale, nivelul de protectie a persoanelor fizice asigurat in Uniune prin prezentul regulament nu ar trebui sa fie diminuat, inclusiv in cazurile de transferuri ulterioare de date cu caracter personal dinspre tara terta sau organizatia internationala catre operatori, persoane imputernicite de operatori din aceeasi sau dintr-o alta tara terta sau organizatie internationala. In orice caz, transferurile catre tari terte si organizatii internationale pot fi desfasurate numai in conformitate deplina cu prezentul regulament. Un transfer ar putea avea loc numai daca, sub rezerva respectarii celorlalte dispozitii ale prezentului regulament, operatorul sau persoana imputernicita de operator indeplineste conditiile prevazute de dispozitiile prezentului regulament privind transferul de date cu caracter personal catre tari terte sau organizatii internationale.

(102) Prezentul regulament nu aduce atingere acordurilor internationale incheiate intre Uniune si tari terte in vederea reglementarii transferului de date cu caracter personal, inclusiv garantii adecvate pentru persoanele vizate. Statele membre pot incheia acorduri internationale care implica transferul de date cu caracter personal catre tari terte sau organizatii internationale, in masura in care astfel de acorduri nu afecteaza prezentul regulament si nici alte dispozitii din dreptul Uniunii si includ un nivel corespunzator de protectie a drepturilor fundamentale ale persoanelor vizate.

(103) Comisia poate decide, cu efect in intreaga Uniune, ca o tara terta, un teritoriu sau un anumit sector dintr-o tara terta sau o organizatie internationala ofera un nivel adecvat de protectie a datelor, asigurand astfel securitate juridica si uniformitate in Uniune in ceea ce priveste tara terta sau organizatia internationala care este considerata a furniza un astfel de nivel de protectie. In aceste cazuri, transferurile de date cu caracter personal catre tara terta sau organizatia internationala respectiva pot avea loc fara a fi necesar sa se obtina autorizari suplimentare. De asemenea, Comisia poate sa decida, dupa trimiterea unei notificari si a unei justificari complete tarii terte sau organizatiei internationale, sa anuleze o astfel de decizie.

(104) In conformitate cu valorile fundamentale pe care se intemeiaza Uniunea, in special protectia drepturilor omului, Comisia ar trebui, in evaluarea sa referitoare la tara terta sau la un teritoriu sau la un sector specificat dintr-o tara terta, sa ia in considerare modul in care aceasta respecta statul de drept, accesul la justitie, precum si normele si standardele internationale in materie de drepturi ale omului si legislatia sa generala si sectoriala, inclusiv legislatia privind securitatea publica, apararea si securitatea nationala, precum si ordinea publica si dreptul penal. Adoptarea unei decizii privind caracterul adecvat al nivelului de protectie pentru un teritoriu sau un sector specificat dintr-o tara terta ar trebui sa tina seama de criterii clare si obiective, cum ar fi activitatile specifice de prelucrare si domeniul de aplicare al standardelor legale aplicabile si legislatia in vigoare in tara terta respectiva. Tara terta ar trebui sa ofere garantii care sa asigure un nivel adecvat de protectie, echivalent in esenta cu cel asigurat in cadrul Uniunii, in special atunci cand datele cu caracter personal sunt prelucrate in unul sau mai multe sectoare specifice. In special, tara terta ar trebui sa asigure o supraveghere efectiva independenta in materie de protectie a datelor si sa prevada mecanisme de cooperare cu autoritatile statelor membre de

protectie a datelor, iar persoanele vizate ar trebui sa beneficieze de drepturi efective si opozabile si de reparatii efective pe cale administrativa si judiciara.

(105) Pe langa angajamentele internationale asumate de tara terta sau de organizatia internationala, Comisia ar trebui sa tina seama de obligatiile care decurg din participarea tarii terte sau a organizatiei internationale la sistemele multilaterale sau regionale, in special in ceea ce priveste protectia datelor cu caracter personal, precum si de punerea in aplicare a unor astfel de obligatii. In special, ar trebui sa fie luata in considerare aderarea tarii terte la Conventia Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor fata de prelucrarea automatizata a datelor cu caracter personal si protocolul aditional la aceasta. Comisia ar trebui sa consulte comitetul atunci cand evalueaza nivelul de protectie din tarile terte sau din organizatiile internationale.

(106) Comisia ar trebui sa monitorizeze functionarea deciziilor privind nivelul de protectie dintr-o tara terta sau un teritoriu sau un anumit sector dintr-o tara terta sau dintr-o organizatie internationala si sa monitorizeze functionarea deciziilor adoptate in temeiul articolului 25 alineatul (6) sau al articolului 26 alineatul (4) din Directiva 95/46/CE. In deciziile sale privind caracterul adecvat al nivelului de protectie, Comisia ar trebui sa prevada un mecanism de revizuire periodica a modului lor de functionare. Aceasta revizuire periodica ar trebui sa fie efectuata in consultare cu tara terta sau organizatia internationala in cauza si ar trebui sa ia in considerare toate evolutiile relevante din tara terta sau organizatia internationala. In scopul monitorizarii si al efectuarii revizuirilor periodice, Comisia ar trebui sa ia in considerare opiniile si constatarile Parlamentului European si ale Consiliului, precum si ale altor organisme si surse relevante. Comisia ar trebui sa evalueze, intr-un termen rezonabil, functionarea deciziilor din urma si sa raporteze toate constatarile relevante comitetului, in sensul Regulamentului (UE) nr. 182/2011 al Parlamentului European si al Consiliului, dupa cum s-a stabilit in temeiul prezentului regulament, Parlamentului European si Consiliului.

(107) Comisia poate sa recunoasca faptul ca o tara terta,un teritoriu sau un sector specificat dintr-o tara terta sau o organizatie internationala nu mai asigura un nivel adecvat de protectie a datelor. In consecinta, transferul de date cu caracter personal catre tara terta sau organizatia internationala respectiva ar trebui sa fie interzis, cu exceptia cazului in care sunt indeplinite cerintele prevazute in prezentul regulament privind transferurile in baza unor garantii adecvate, inclusiv regulile corporatiste obligatorii si derogarile de la situatiile specifice. In acest caz, ar trebui sa se prevada dispozitii pentru consultari intre Comisie si astfel de tari terte sau organizatii internationale. Comisia ar trebui ca, in timp util, sa informeze tara terta sau organizatia internationala cu privire la aceste motive si sa initieze consultari cu aceasta pentru remedierea situatiei.

(108) In absenta unei decizii privind caracterul adecvat al nivelului de protectie, operatorul sau persoana imputernicita de operator ar trebui sa adopte masuri pentru a compensa lipsa protectiei datelor intr-o tara terta prin intermediul unor garantii adecvate pentru persoana vizata. Astfel de garantii adecvate pot consta in utilizarea regulilor corporatiste obligatorii, a clauzelor standard de protectie a datelor adoptate de Comisie, a clauzelor standard de protectie a datelor adoptate de o autoritate de supraveghere sau a clauzelor contractuale autorizate de o autoritate de supraveghere. Respectivele garantii ar trebui sa asigure respectarea cerintelor in materie de protectie a datelor si drepturi ale persoanelor vizate corespunzatoare prelucrarii in interiorul Uniunii, inclusiv disponibilitatea unor drepturi opozabile ale persoanelor vizate si a unor cai de atac eficiente, printre care dreptul de acces la reparatii efective pe cale administrativa sau judiciara si dreptul de a solicita despagubiri, in Uniune sau intr-o tara terta. Acestea ar trebui sa se refere in special la respectarea principiilor generale privind prelucrarea datelor cu caracter personal: principiul protectiei datelor incepand cu momentul conceperii si principiul protectiei implicite a datelor. Transferurile pot fi efectuate si de catre autoritatile sau organismele publice cu autoritati sau organisme publice in tari terte sau cu organizatii internationale cu atributii si functii corespunzatoare, inclusiv pe baza dispozitiilor care prevad drepturi opozabile si efective pentru persoanele vizate, care trebuie introduse in acordurile administrative, cum ar fi un memorandum de intelegere. Autorizatia din partea autoritatii de supraveghere competente ar trebui obtinuta atunci cand garantiile sunt oferite in cadrul unor acorduri administrative fara caracter juridic obligatoriu.

(109) Posibilitatea ca operatorul sau persoana imputernicita de operator sa utilizeze clauze standard in materie de protectie a datelor, adoptate de Comisie sau de o autoritate de supraveghere, nu ar trebui sa impiedice operatorii sau persoanele imputernicite de acestia sa includa clauzele standard in materie de protectie a datelor intr-un contract mai amplu, precum un contract intre persoana imputernicita de operator si o alta persoana imputernicita de operator, si nici sa adauge alte clauze sau garantii suplimentare, atat timp cat acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de o autoritate de supraveghere sau nu prejudiciaza drepturile sau libertatile fundamentale ale persoanelor vizate. Operatorii si persoanele imputernicite de operatori ar trebui sa fie incurajati sa ofere garantii suplimentare prin intermediul unor angajamente contractuale care sa completeze clauzele standard in materie de protectie.

(110) Un grup de intreprinderi sau un grup de intreprinderi implicat intr-o activitate economica comuna ar trebui sa poata utiliza regulile corporatiste obligatorii aprobate pentru transferurile sale internationale dinspre Uniune catre organizatii din cadrul aceluiasi grup de intreprinderi sau grup de intreprinderi implicate intr-o activitate economica comuna, cu conditia ca astfel de reguli corporatiste sa includa toate principiile esentiale si drepturile opozabile in scopul asigurarii unor garantii adecvate pentru transferurile sau categoriile de transferuri de date cu caracter personal.

(111) Ar trebui sa se prevada posibilitatea de a se efectua transferuri in anumite circumstante in care persoana vizata si-a dat consimtamantul explicit, in care transferul este ocazional si necesar in legatura cu un contract sau cu o actiune in justitie, indiferent daca este in contextul unei proceduri judiciare sau in contextul unei proceduri administrative sau extrajudiciare, inclusiv in cadrul procedurilor inaintate organismelor de reglementare. De asemenea, ar trebui sa se prevada posibilitatea de a se efectua transferuri in cazul in care motive importante de interes public stabilite de dreptul Uniunii sau de dreptul intern impun acest lucru sau in cazul in care transferul se efectueaza dintr-un registru instituit prin lege si destinat sa fie consultat de catre public sau de catre persoane care au un interes legitim. In acest ultim caz, un astfel de transfer nu ar trebui sa implice totalitatea datelor cu caracter personal sau ansamblul categoriilor de date continute in registru, iar atunci cand registrul este destinat sa fie consultat de persoane care au un interes legitim, transferul ar trebui sa fie efectuat doar la cererea persoanelor respective sau daca acestea sunt destinatarii, luand pe deplin in considerare interesele si drepturile fundamentale ale persoanei vizate.

(112) Aceste derogari ar trebui sa se aplice, in special, transferurilor de date solicitate si necesare din considerente importante de interes public, de exemplu in cazul schimbului international de date intre autoritatile din domeniul concurentei, administratiile fiscale sau vamale, intre autoritatile de supraveghere financiara, intre serviciile competente in materie de securitate sociala sau de sanatate publica, de exemplu in cazul depistarii punctelor de contact pentru bolile contagioase sau pentru reducerea si/sau eliminarea dopajului in sport. Un transfer de date cu caracter personal ar trebui, de asemenea, sa fie considerat legal in cazul in care este necesar in scopul protejarii unui interes care este esential in interesele vitale ale persoanei vizate sau ale unei alte persoane, inclusiv pentru integritatea fizica sau pentru viata acesteia, in cazul in care persona vizata nu are capacitatea sa isi dea consimtamantul. In absenta unei decizii privind caracterul adecvat al nivelului de protectie, dreptul Uniunii sau dreptul intern poate, din considerente importante de interes public, stabili in mod expres limite asupra transferului unor categorii specifice de date catre o tara terta sau o organizatie internationala. Statele membre ar trebui sa notifice Comisiei aceste dispozitii. Orice transfer catre o organizatie umanitara internationala al datelor cu caracter personal ale unei persoane vizate care se afla in incapacitate fizica sau juridica de a isi da consimtamantul, in vederea indeplinirii unei sarcini care decurge din Conventiile de la Geneva sau in vederea conformarii cu dreptul international umanitar aplicabil in conflictele armate, ar putea fi considerat necesar pentru un motiv important de interes public sau pentru ca este in interesul vital al persoanei vizate.

(113) Transferurile care pot fi considerate ca nefiind repetitive si care se refera doar la un numar limitat de persoane vizate, ar putea, de asemenea, sa fie efectuate in scopul realizarii intereselor legitime urmarite de operator, atunci cand asupra respectivelor interese nu prevaleaza interesele sau drepturile si libertatile persoanei vizate si atunci cand operatorul a evaluat toate circumstantele aferente transferului de date. Operatorul ar trebui sa acorde o atentie deosebita naturii datelor cu caracter personal, scopului si duratei operatiunii sau operatiunilor propuse de prelucrare, precum si situatiei din tara de origine, din tara terta si din tara de destinatie finala si ar trebui sa ofere garantii adecvate pentru protectia drepturilor si libertatilor fundamentale ale persoanelor fizice in ceea ce priveste prelucrarea datelor lor cu caracter personal. Astfel de transferuri ar trebui sa fie posibile numai in cazurile reziduale in care nu se poate aplica niciunul dintre celelalte motive de transfer. In ceea ce priveste scopurile de cercetare stiintifica sau istorica sau scopurile statistice, ar trebui sa se ia in considerare asteptarile legitime ale societatii cu privire la cresterea nivelului de cunostinte. Operatorul ar trebui sa informeze autoritatea de supraveghere si persoana vizata cu privire la transfer.

(114) In orice caz, atunci cand Comisia nu a luat o decizie cu privire la nivelul adecvat de protectie a datelor dintr-o tara terta, operatorul sau persoana imputernicita de operator ar trebui sa utilizeze solutii care sa ofere persoanelor vizate drepturi opozabile si efective in ceea ce priveste prelucrarea datelor lor in Uniune odata ce aceste date au fost transferate, astfel incat persoanele vizate sa beneficieze in continuare de drepturi fundamentale si garantii.

(115) Unele tari terte au adoptat legi, reglementari si alte acte juridice care au drept obiectiv sa reglementeze in mod direct activitatile de prelucrare a datelor ale persoanelor fizice si juridice aflate sub jurisdictia statelor membre. Aceasta poate include hotarari ale instantelor judecatoresti sau decizii ale autoritatilor administrative

din tari terte care solicita unui operator sau unei persoane imputernicite de operator sa transfere sau sa divulge date cu caracter personal si care nu se bazeaza pe un acord international, cum ar fi un tratat de asistenta juridica reciproca, in vigoare intre tara terta solicitanta si Uniune sau un stat membru. Aplicarea extrateritoriala a acestor legi, reglementari si alte acte juridice poate incalca dreptul international si poate impiedica asigurarea protectiei persoanelor fizice asigurata in Uniune prin prezentul regulament. Transferurile ar trebui sa fie permise numai in cazul indeplinirii conditiilor prevazute de prezentul regulament pentru un transfer catre tari terte. Acesta ar putea fi cazul, inter alia, atunci cand divulgarea este necesara dintr-un motiv important de interes public recunoscut in dreptul Uniunii sau in dreptul intern care se aplica operatorului.

(116) Fluxul transfrontalier de date cu caracter personal in afara Uniunii poate expune unui risc sporit capacitatea persoanelor fizice de a-si exercita drepturile in materie de protectie a datelor, in special pentru a-si asigura protectia impotriva utilizarii sau a divulgarii ilegale a acestor informatii. In acelasi timp, autoritatile de supraveghere pot constata ca se afla in imposibilitatea de a trata plangeri sau de a efectua investigatii referitoare la activitatile desfasurate in afara frontierelor lor. Eforturile acestora de a conlucra in context transfrontalier pot fi, de asemenea, ingreunate de insuficienta competentelor de prevenire sau remediere, de caracterul eterogen al regimurilor juridice si de existenta unor obstacole de ordin practic, cum ar fi constrangerile in materie de resurse. Prin urmare, este necesar sa se promoveze o cooperare mai stransa intre autoritatile de supraveghere a protectiei datelor pentru a putea face schimb de informatii si a desfasura investigatii impreuna cu omologii lor internationali. In scopul elaborarii de mecanisme de cooperare internationala pentru a facilita si a oferi asistenta internationala reciproca in asigurarea aplicarii legislatiei din domeniul protectiei datelor cu caracter personal, Comisia si autoritatile de supraveghere ar trebui sa faca schimb de informatii si sa coopereze in cadrul activitatilor legate de exercitarea competentelor lor cu autoritatile competente din tari terte, pe baza de reciprocitate si in conformitate cu prezentul regulament.

(117) Instituirea in statele membre a unor autoritati de supraveghere, imputernicite sa isi indeplineasca sarcinile si sa isi exercite competentele in deplina independenta, este un element esential al protectiei persoanelor fizice in ceea ce priveste prelucrarea datelor lor cu caracter personal. Statele membre ar trebui sa poata institui mai multe autoritati de supraveghere, pentru a reflecta structura lor constitutionala, organizatorica si administrativa.

(118) Independenta autoritatilor de supraveghere nu ar trebui sa insemne ca autoritatile de supraveghere nu pot face obiectul unor mecanisme de control sau de monitorizare in ceea ce priveste cheltuielile acestora sau unui control jurisdictional.

(119) In cazul in care un stat membru instituie mai multe autoritati de supraveghere, acesta ar trebui sa stabileasca prin lege mecanisme care sa asigure participarea efectiva a autoritatilor de supraveghere respective la mecanismul pentru asigurarea coerentei. Statul membru respectiv ar trebui, in special, sa desemneze autoritatea de supraveghere care indeplineste functia de punct unic de contact pentru participarea efectiva a acestor autoritati la mecanism, in scopul asigurarii unei cooperari rapide si armonioase cu alte autoritati de supraveghere, cu comitetul si cu Comisia.

(120) Fiecare autoritate de supraveghere ar trebui sa beneficieze de resurse financiare si umane, de spatiile si de infrastructura necesare pentru indeplinirea cu eficacitate a sarcinilor lor, inclusiv a celor legate de asistenta reciproca si cooperarea cu alte autoritati de supraveghere in intreaga Uniune. Fiecare autoritate de supraveghere ar trebui sa aiba un buget public anual separat, care poate face parte din bugetul general de stat sau national.

(121) Conditiile generale pentru membrul sau membrii autoritatii de supraveghere ar trebui stabilite de lege in fiecare stat membru si ar trebui, in special, sa prevada ca respectivii membri sunt numiti printr-o procedura transparenta fie de parlamentul, de guvernul ori seful 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 catre un organism independent imputernicit prin dreptul intern. In vederea asigurarii independentei autoritatii de supraveghere, membrul sau membrii acesteia ar trebui sa actioneze cu integritate, sa nu intreprinda actiuni incompatibile cu indatoririle lor, iar, pe durata mandatului, ar trebui sa nu desfasoare activitati incompatibile, remunerate sau nu. Autoritatea de supraveghere ar trebui sa aiba personal propriu, ales de autoritatea de supraveghere sau de un organism independent infiintat in temeiul dreptului intern, care ar trebui sa fie subordonat exclusiv membrului sau membrilor autoritatii de supraveghere.

(122) Fiecare autoritate de supraveghere ar trebui sa aiba, pe teritoriul statului membru de care apartine, atributia de a exercita competentele si de a indeplini sarcinile cu care este investita in conformitate cu prezentul regulament. Aceasta ar trebui sa includa in special prelucrarea in contextul activitatilor unui sediu al operatorului sau al persoanei imputernicite de operator pe teritoriul propriului stat membru, prelucrarea datelor cu caracter personal efectuata de autoritatile publice sau de organisme private care actioneaza in interes public,

prelucrarea care afecteaza persoanele vizate de pe teritoriul sau sau prelucrarea efectuata de catre un operator sau o persoana imputernicita de operator care nu isi are sediul in Uniune in cazul in care aceasta priveste persoane vizate care isi au resedinta pe teritoriul sau. Aceasta ar trebui sa includa tratarea plangerilor depuse de o persoana vizata, efectuarea de investigatii privind aplicarea prezentului regulament si promovarea informarii publicului cu privire la riscurile, normele, garantiile si drepturile in materie de prelucrare a datelor cu caracter personal.

(123) Autoritatile de supraveghere ar trebui sa monitorizeze aplicarea dispozitiilor prevazute de prezentul regulament si sa contribuie la aplicarea coerenta a acestuia in intreaga Uniune, in scopul asigurarii protectiei persoanelor fizice in ceea ce priveste prelucrarea datelor lor cu caracter personal si al facilitarii liberei circulatii a datelor cu caracter personal in interiorul pietei interne. In acest sens, autoritatile de supraveghere ar trebui sa coopereze reciproc, precum si cu Comisia, fara sa fie necesar niciun acord intre statele membre cu privire la acordarea de asistenta reciproca sau cu privire la respectiva cooperare.

(124) In cazul in care prelucrarea datelor cu caracter personal se desfasoara in cadrul activitatilor unui sediu al unui operator sau al unei persoane imputernicite de operator din Uniune, iar operatorul sau persoana imputernicita de operator are sedii in mai multe state membre, sau in cazul in care prelucrarea care se desfasoara in contextul activitatilor unui singur sediu al unui operator sau al unei persoane imputernicite de operator din Uniune afecteaza sau este susceptibila sa afecteze semnificativ persoane vizate din mai multe state membre, autoritatea de supraveghere a sediului principal al operatorului sau al persoanei imputernicite de operator ori a sediului unic al operatorului sau al persoanei imputernicite de operator ar trebui sa actioneze in calitate de autoritate principala. Aceasta ar trebui sa coopereze cu celelalte autoritati vizate, pentru ca operatorul sau persoana imputernicita de operator are un sediu pe teritoriul statului lor membru, pentru ca persoanele vizate care isi au resedinta pe teritoriul lor sunt afectate in mod semnificativ sau pentru ca le-a fost inaintata o plangere. De asemenea, in cazul in care o persoana vizata care nu isi are resedinta in statul membru respectiv a depus o plangere, autoritatea de supraveghere la care a fost depusa plangerea ar trebui, de asemenea, sa fie o autoritate de supraveghere vizata. In cadrul sarcinilor sale de a emite orientari cu privire la orice chestiune referitoare la punerea in aplicare a prezentului regulament, comitetul ar trebui sa poata emite orientari privind, in special, criteriile care trebuie luate in considerare pentru a se stabili daca prelucrarea in cauza afecteaza in mod semnificativ persoane vizate din mai multe state membre si privind continutul unei obiectii relevante si motivate.

(125) Autoritatea principala ar trebui sa aiba competenta de a adopta decizii obligatorii privind masurile de aplicare a competentelor care ii sunt conferite in conformitate cu prezentul regulament. In calitatea sa de autoritate principala, autoritatea de supraveghere ar trebui sa implice indeaproape si sa coordoneze activitatile autoritatilor de supraveghere vizate in procesul decizional. In cazurile in care decizia este de respingere partiala sau totala a plangerii din partea persoanei vizate, o asemenea decizie ar trebui adoptata de catre autoritatea de supraveghere la care s-a depus plangerea.

(126) Decizia ar trebui convenita in comun de autoritatea de supraveghere principala si de autoritatile de supraveghere vizate si ar trebui sa vizeze sediul principal sau sediul unic al operatorului sau al persoanei imputernicite de operator si sa fie obligatorie pentru operator si pentru persoana imputernicita de operator. Operatorul sau persoana imputernicita de operator ar trebui sa ia masurile necesare pentru a asigura conformitatea cu prezentul regulament si punerea in aplicare a deciziei notificate de autoritatea de supraveghere principala sediului principal al operatorului sau al persoanei imputernicite de operator in ceea ce priveste activitatile de prelucrare in Uniune.

(127) Fiecare autoritate de supraveghere care nu actioneaza ca autoritate de supraveghere principala ar trebui sa aiba competenta de a trata cazuri locale, in care operatorul sau persoana imputernicita de operator are sedii in mai multe state membre, dar obiectul respectivei prelucrari priveste doar prelucrarea efectuata intr-un singur stat membru si implicand doar persoane vizate din acel unic stat membru, de exemplu in cazul in care obiectul il constituie prelucrarea datelor cu caracter personal ale angajatilor in contextul specific legat de forta de munca dintr-un stat membru. In astfel de cazuri, autoritatea de supraveghere ar trebui sa informeze fara intarziere autoritatea de supraveghere principala cu privire la aceasta chestiune. Dupa ce a fost informata, autoritatea de supraveghere principala ar trebui sa decida daca va trata ea insasi cazul in temeiul dispozitiei privind cooperarea intre autoritatea de supraveghere principala si alte autoritati de supraveghere vizate ("mecanismul ghiseului unic"), sau daca autoritatea de supraveghere care a informat-o ar trebui sa se ocupe de caz la nivel local. Atunci cand decide daca va trata cazul, autoritatea de supraveghere principala ar trebui sa ia in considerare daca exista un sediu al operatorului sau al persoanei imputernicite de operator in statul membru al autoritatii de supraveghere care a informat-o, in vederea garantarii respectarii efective a unei decizii in ceea ce priveste

operatorul sau persoana imputernicita de operator. In cazul in care autoritatea de supraveghere principala decide sa trateze cazul, autoritatea de supraveghere care a informat-o ar trebui sa beneficieze de posibilitatea de a prezenta un proiect de decizie, de care autoritatea de supraveghere principala ar trebui sa tina seama in cea mai mare masura atunci cand pregateste proiectul sau de decizie in cadrul respectivului mecanism al ghiseului unic.

(128) Normele privind autoritatea de supraveghere principala si mecanismul ghiseului unic nu ar trebui sa se aplice in cazul in care prelucrarea este efectuata de autoritati publice sau organisme private in interes public. In asemenea cazuri, singura autoritate de supraveghere competenta sa isi exercite competentele care i-au fost atribuite in conformitate cu prezentul regulament ar trebui sa fie autoritatea de supraveghere a statului membru in care autoritatea publica sau organismul privat isi are sediul.

(129) Pentru a se asigura consecventa monitorizarii si a aplicarii prezentului regulament in intreaga Uniune, autoritatile de supraveghere ar trebui sa aiba in fiecare stat membru aceleasi sarcini si competente efective, inclusiv competente de investigare, competente corective si sanctiuni, precum si competente de autorizare si de consiliere, in special in cazul plangerilor depuse de persoane fizice, precum si, fara a aduce atingere competentelor autoritatilor de urmarire penala in temeiul dreptului intern, de a aduce in atentia autoritatilor judiciare cazurile de incalcare a prezentului regulament si de a se implica in proceduri judiciare. Aceste competente ar trebui sa includa si competenta de a impune o limitare temporara sau definitiva, inclusiv o interdictie, asupra prelucrarii. Statele membre pot stabili alte sarcini legate de protectia datelor cu caracter personal in temeiul prezentului regulament. Competentele autoritatilor de supraveghere ar trebui exercitate in conformitate cu garantii procedurale adecvate prevazute in dreptul Uniunii si in dreptul intern, in mod impartial, echitabil si intr-un termen rezonabil. In special, fiecare masura ar trebui sa fie adecvata, necesara si proportionala in scopul de a asigura conformitatea cu dispozitiile prezentului regulament, luand in considerare circumstantele fiecarui caz in parte, sa respecte dreptul oricarei persoane de a fi ascultata inainte de luarea oricarei masuri individuale care ar putea sa ii aduca atingere si sa evite costurile inutile si inconvenientele excesive pentru persoanele in cauza. Competentele de investigare in ceea ce priveste accesul in incinte ar trebui exercitate in conformitate cu cerintele specifice din dreptul procedural national, cum ar fi obligatia de a obtine in prealabil o autorizare judiciara. Fiecare masura obligatorie din punct de vedere juridic luata de autoritatea de supraveghere ar trebui sa fie prezentata in scris, sa fie clara si lipsita de ambiguitate, sa indice autoritatea de supraveghere care a emis masura, data emiterii masurii, sa poarte semnatura sefului sau a unui membru al autoritatii de supraveghere autorizat de acesta, sa furnizeze motivele pentru care s-a luat masura si sa faca trimitere la dreptul la o cale de atac eficienta. Acest lucru nu ar trebui sa excluda cerinte suplimentare in conformitate cu dreptul procedural national. Adoptarea unor astfel de decizii obligatorii din punct de vedere juridic implica faptul ca se poate da nastere unui control jurisdictional in statul membru al autoritatii de supraveghere care a adoptat decizia.

(130) In cazul in care autoritatea de supraveghere la care s-a depus plangerea nu este autoritatea de supraveghere principala, autoritatea de supraveghere principala ar trebui sa coopereze indeaproape cu autoritatea de supraveghere la care s-a depus plangerea, in conformitate cu dispozitiile privind cooperarea si consecventa prevazute in prezentul regulament. In astfel de cazuri, autoritatea de supraveghere principala ar trebui, atunci cand ia masuri destinate sa produca efecte juridice, inclusiv impunerea de amenzi administrative, sa tina seama cat mai mult posibil de opinia autoritatii de supraveghere la care a fost depusa plangerea si care ar trebui sa isi mentina competenta de a desfasura orice investigatie pe teritoriul propriului stat membru, in colaborare cu autoritatea de supraveghere principala.

(131) In cazurile in care o alta autoritate de supraveghere ar trebui sa actioneze in calitate de autoritate de supraveghere principala pentru activitatile de prelucrare ale operatorului sau ale persoanei imputernicite de operator, dar obiectul concret al unei plangeri sau posibila incalcare vizeaza numai activitatile de prelucrare ale operatorului sau ale persoanei imputernicite de operator in statul membru in care a fost depusa plangerea sau a fost depistata posibila incalcare, iar chestiunea nu afecteaza in mod substantial sau nu este susceptibila sa afecteze in mod substantial persoane vizate din alte state membre, autoritatea de supraveghere care a primit o plangere sau a depistat ori a fost informata in alt mod asupra unor situatii de posibile incalcari ale prezentului regulament ar trebui sa incerce o solutionare pe cale amiabila cu operatorul si, in cazul in care aceasta esueaza, sa isi exercite plenitudinea competentelor. Aceasta ar trebui sa includa activitati specifice de prelucrare efectuate pe teritoriul statului membru al autoritatii de supraveghere ori cu privire la persoane vizate de pe teritoriul acelui stat membru, activitati de prelucrare care au loc in contextul unei oferte de bunuri sau servicii destinate in mod special persoanelor vizate pe teritoriul statului membru al autoritatii de supraveghere sau activitati de prelucrare care trebuie evaluate tinand seama de obligatiile juridice relevante in temeiul dreptului intern.

(132) Activitatile de crestere a gradului de constientizare organizate pentru public de autoritatile de supraveghere ar trebui sa includa masuri specifice care sa vizeze operatorii si persoanele imputernicite de operatori, inclusiv microintreprinderile si intreprinderile mici si mijlocii, precum si persoanele fizice, in special in context educational.

(133) Autoritatile de supraveghere ar trebui sa isi acorde reciproc asistenta in indeplinirea sarcinilor care le revin, pentru a se asigura coerenta aplicarii prezentului regulament pe piata interna. O autoritate de supraveghere care solicita asistenta reciproca poate adopta o masura provizorie in cazul in care nu primeste un raspuns la o solicitare de asistenta reciproca in termen de o luna de la primirea solicitarii de catre cealalta autoritate de supraveghere.

(134) Fiecare autoritate de supraveghere ar trebui sa participe, dupa caz, la operatiuni comune intre autoritatile de supraveghere. Autoritatea de supraveghere careia i s-a adresat solicitarea ar trebui sa aiba obligatia de a raspunde cererii intr-un anumit termen.

(135) Pentru a se asigura aplicarea coerenta a prezentului regulament in intreaga Uniune, ar trebui sa se instituie un mecanism pentru asigurarea coerentei in cadrul caruia autoritatile de supraveghere sa coopereze. Acest mecanism ar trebui sa se aplice, in special, in cazul in care o autoritate de supraveghere intentioneaza sa adopte o masura prevazuta a produce efecte juridice in ceea ce priveste operatiunile de prelucrare care afecteaza in mod substantial un numar semnificativ de persoane vizate din mai multe state membre. Mecanismul ar trebui sa se aplice, de asemenea, in cazul in care o autoritate de supraveghere vizata sau Comisia solicita ca aspectul respectiv sa fie tratat in cadrul mecanismului pentru asigurarea coerentei. Acest mecanism nu ar trebui sa aduca atingere masurilor pe care Comisia le poate adopta in exercitarea competentelor care ii revin in temeiul tratatelor.

(136) In aplicarea mecanismului pentru asigurarea coerentei, comitetul ar trebui, intr-un anumit termen, sa emita un aviz in cazul in care o majoritate a membrilor sai decide astfel sau in cazul in care orice autoritate de supraveghere vizata sau Comisia solicita acest lucru. Comitetul ar trebui, de asemenea, sa fie imputernicit sa adopte decizii obligatorii din punct de vedere juridic in cazul unor litigii intre autoritatile de supraveghere. In acest scop, acesta ar trebui sa emita, in principiu cu o majoritate de doua treimi din membrii sai, decizii obligatorii din punct de vedere juridic, in cazuri bine definite, in cazul in care exista opinii divergente intre autoritatile de supraveghere, in special in cadrul mecanismului de cooperare intre autoritatea de supraveghere principala si autoritatile de supraveghere vizate privind fondul cauzei, in special existenta sau nu a unei incalcari a prezentului regulament.

(137) Este posibil sa existe o necesitate urgenta de a se actiona pentru asigurarea protectiei drepturilor si libertatilor persoanelor vizate, in special in cazul in care exista pericolul ca exercitarea unui drept al unei persoane vizate sa fie impiedicata in mod considerabil. Prin urmare, o autoritate de supraveghere ar trebui sa poata adopta masuri provizorii pe teritoriul sau, justificate in mod corespunzator, avand o perioada de valabilitate determinata care nu ar trebui sa depaseasca trei luni.

(138) Aplicarea unui astfel de mecanism ar trebui sa constituie o conditie pentru legalitatea unei masuri destinate sa produca efecte juridice, luate de o autoritate de supraveghere, in cazurile in care aplicarea acesteia este obligatorie. In alte cazuri cu relevanta transfrontaliera, ar trebui pus in aplicare mecanismul de cooperare intre autoritatea de supraveghere principala si autoritatile de supraveghere vizate, iar intre autoritatile de supraveghere vizate s-ar putea acorda asistenta reciproca si s-ar putea desfasura operatiuni comune pe baza bilaterala sau multilaterala, fara declansarea mecanismului pentru asigurarea coerentei.

(139) Cu scopul de a promova aplicarea coerenta a prezentului regulament, comitetul ar trebui instituit ca organ independent al Uniunii. Pentru a-si indeplini obiectivele, comitetul ar trebui sa aiba personalitate juridica. Comitetul ar trebui sa fie reprezentat de presedintele sau. Acesta ar trebui sa inlocuiasca Grupul de lucru pentru protectia persoanelor in ceea ce priveste prelucrarea datelor cu caracter personal, instituit prin Directiva 95/46/CE. Acesta ar trebui sa fie alcatuit din sefii autoritatilor de supraveghere din fiecare stat membru si din Autoritatea Europeana pentru Protectia Datelor sau reprezentantii acestora. Comisia ar trebui sa participe la activitatile comitetului fara a avea drept de vot, iar Autoritatea Europeana pentru Protectia Datelor ar trebui sa aiba drepturi de vot speciale. Comitetul ar trebui sa contribuie la aplicarea coerenta a prezentului regulament in intreaga Uniune, inclusiv prin oferirea de consiliere Comisiei, in special cu privire la nivelul de protectie in tarile terte si in cadrul organizatiilor internationale, si prin promovarea cooperarii autoritatilor de supraveghere in intreaga Uniune. Comitetul ar trebui sa actioneze in mod independent in indeplinirea sarcinilor sale.

(140) Comitetul ar trebui sa fie asistat de un secretariat asigurat de Autoritatea Europeana pentru Protectia Datelor. Personalul Autoritatii Europene pentru Protectia Datelor implicat in indeplinirea sarcinilor conferite

comitetului in temeiul prezentului regulament ar trebui sa isi indeplineasca sarcinile exclusiv conform instructiunilor presedintelui comitetului si sa raporteze acestuia.

(141) Orice persoana vizata ar trebui sa aiba dreptul de a depune o plangere la o singura autoritate de supraveghere, in special in statul membru in care isi are resedinta obisnuita, precum si dreptul la o cale de atac eficienta in conformitate cu articolul 47 din carta, in cazul in care persoana vizata considera ca drepturile sale in temeiul prezentului regulament sunt incalcate sau in cazul in care autoritatea de supraveghere nu reactioneaza la o plangere, respinge sau refuza partial sau total o plangere sau nu actioneaza atunci cand o astfel de actiune este necesara pentru asigurarea protectiei drepturilor persoanei vizate. Investigatia in urma unei plangeri ar trebui sa fie efectuata, sub control judiciar, in masura in care este necesar, in functie de caz. Autoritatea de supraveghere ar trebui sa informeze persoana vizata cu privire la evolutia si solutionarea plangerii intr-un termen rezonabil. In eventualitatea in care cazul necesita o investigare suplimentara sau coordonarea cu o alta autoritate de supraveghere, ar trebui sa se furnizeze informatii intermediare persoanei vizate. In vederea facilitarii depunerii plangerilor, fiecare autoritate de supraveghere ar trebui sa ia masuri precum punerea la dispozitie a unui formular de depunere a plangerii, care sa poata fi completat inclusiv in format electronic, fara a exclude alte mijloace de comunicare.

(142) In cazul in care persoana vizata considera ca drepturile sale in temeiul prezentului regulament sunt incalcate, aceasta ar trebui sa aiba dreptul de a mandata un organism, o organizatie sau o asociatie fara scop lucrativ care este infiintat(a) in conformitate cu dreptul intern, ale carui (carei) obiective statutare sunt in interesul public si care isi desfasoara activitatea in domeniul asigurarii protectiei datelor cu caracter personal, sa depuna o plangere in numele sau la o autoritate de supraveghere, sa exercite dreptul la o cale de atac in numele persoanelor vizate sau, in cazul in care se prevede in dreptul intern, sa exercite dreptul de a primi despagubiri in numele persoanelor vizate. Un stat membru poate prevedea ca un astfel de organism, organizatie sau asociatie sa aiba dreptul de a depune o plangere in statul membru respectiv, independent de mandatul acordat de o persoana vizata, si sa aiba dreptul la o cale de atac eficienta in cazul in care are motive sa considere ca drepturile unei persoane vizate au fost incalcate ca rezultat al unei prelucrari a datelor cu caracter personal care incalca prezentul regulament. Organismul, organizatia sau asociatia in cauza nu poate pretinde despagubiri in numele unei persoane vizate, independent de mandatul acordat de persoana vizata.

(143) Orice persoana fizica sau juridica are dreptul de a introduce o actiune in anulare impotriva deciziilor comitetului in fata Curtii de Justitie, in conformitate cu conditiile prevazute la articolul 263 din TFUE. In calitate de destinatare ale acestor decizii, autoritatile de supraveghere vizate care doresc sa le conteste trebuie sa introduca o actiune impotriva deciziilor respective in termen de doua luni de la data la care le-au fost notificate, in conformitate cu articolul 263 din TFUE. In cazul in care deciziile comitetului vizeaza in mod direct si individual un operator, o persoana imputernicita de operator sau reclamantul, acestia din urma pot introduce o actiune in anularea respectivelor decizii in termen de doua luni de la publicarea acestora pe site-ul comitetului, in conformitate cu articolul 263 din TFUE. Fara a aduce atingere acestui drept in temeiul articolului 263 din TFUE, orice persoana fizica sau juridica ar trebui sa aiba dreptul la o cale de atac judiciara eficienta in fata instantei nationale competente impotriva unei decizii a unei autoritati de supraveghere care produce efecte juridice privind respectiva persoana. O astfel de decizie se refera in special la exercitarea competentelor de investigare, corective si de autorizare de catre autoritatea de supraveghere sau la refuzul sau respingerea plangerilor. Cu toate acestea, dreptul la o cale de atac judiciara eficienta nu include masuri ale autoritatilor de supraveghere care nu sunt obligatorii din punct de vedere juridic, cum ar fi avizele emise de autoritatea de supraveghere sau consiliere furnizata de aceasta. Actiunile impotriva unei autoritati de supraveghere ar trebui sa fie aduse in fata instantelor statului membru in care este stabilita autoritatea de supraveghere si ar trebui sa se desfasoare in conformitate cu dreptul procesual al statului membru respectiv. Respectivele instante ar trebui sa isi exercite competenta judiciara deplina, care ar trebui sa includa competenta de a examina toate aspectele de fapt sau de drept care au relevanta pentru litigiul cu care acestea sunt sesizate.

In cazul in care o plangere a fost respinsa sau refuzata de o autoritate de supraveghere, reclamantul poate introduce o actiune la instantele din acelasi stat membru. In contextul cailor de atac judiciare privind aplicarea prezentului regulament, instantele nationale care considera necesara o decizie privind chestiunea respectiva pentru a le permite sa ia o hotarare pot sau, in cazul prevazut la articolul 267 din TFUE, trebuie sa solicite Curtii de Justitie sa pronunte o decizie preliminara privind interpretarea dreptului Uniunii, inclusiv a prezentului regulament. In plus, in cazul in care o decizie a unei autoritati de supraveghere care pune in aplicare o decizie a comitetului este contestata in fata unei instante nationale si este in discutie validitatea deciziei comitetului, respectiva instanta nationala nu are competenta de a declara nula decizia comitetului, ci trebuie sa aduca chestiunea validitatii in fata Curtii de Justitie, in conformitate cu articolul 267 din TFUE, astfel cum a fost

interpretat de Curtea de Justitie, ori de cate ori instanta nationala considera decizia nula. Cu toate acestea, o instanta nationala nu poate sa transmita o chestiune cu privire la validitatea deciziei comitetului la cererea unei persoane fizice sau juridice care a avut posibilitatea de a introduce o actiune in anulare impotriva respectivei decizii, in special daca aceasta era vizata in mod direct si individual de decizia in cauza, dar nu a facut acest lucru in termenul prevazut la articolul 263 din TFUE.

(144) Atunci cand o instanta sesizata cu o procedura impotriva unei decizii a unei autoritati de supraveghere are motive sa creada ca in fata unei instante competente dintr-un alt stat membru au fost introduse proceduri cu privire la aceeasi prelucrare, cum ar fi acelasi obiect al prelucrarii, de catre acelasi operator sau aceleeasi persoana imputernicita de operator, sau aceeasi cauza, instanta respectiva ar trebui sa contacteze cea de a doua instanta pentru a confirma existenta unor astfel de proceduri conexe. In cazul in care aceste proceduri conexe se afla pe rolul unei instante dintr-un alt stat membru, orice instanta, cu exceptia celei sesizate initial, poate sa isi suspende procedurile sau, la cererea uneia dintre parti, isi poate declina competenta in favoarea instantei sesizate initial, cu conditia ca aceasta din urma sa aiba competenta de a solutiona procedurile in cauza si ca dreptul care i se aplica sa ii permita consolidarea acestor proceduri conexe. Procedurile sunt considerate conexe atunci cand sunt atat de strans legate intre ele incat este oportuna instrumentarea si judecarea lor in acelasi timp pentru a se evita riscul pronuntarii unor hotarari ireconciliabile in cazul judecarii lor in mod separat.

(145) In ceea ce priveste actiunile initiate impotriva unui operator sau unei persoane imputernicite de operator, reclamantul ar trebui sa aiba posibilitatea de a introduce actiunea in fata instantelor din statele membre in care operatorul sau persoana imputernicita de operator are un sediu sau in care persoana vizata isi are resedinta, cu exceptia cazului in care operatorul este o autoritate publica dintr-un stat membru ce actioneaza in exercitarea competentelor sale publice.

(146) Operatorul sau persoana imputernicita de operator ar trebui sa plateasca despagubiri pentru orice prejudiciu pe care o persoana il poate suferi ca urmare a unei prelucrari care incalca prezentul regulament. Operatorul sau persoana imputernicita de operator ar trebui sa fie exonerati de raspundere daca dovedesc ca nu sunt in niciun fel raspunzatori pentru prejudiciu. Conceptul de prejudiciu ar trebui interpretat in sens larg, din perspectiva jurisprudentei Curtii de Justitie, intr-un mod care sa reflecte pe deplin obiectivele prezentului regulament. Aceasta dispozitie nu aduce atingere niciunei cereri de despagubire care rezulta din incalcarea altor norme din dreptul Uniunii sau din dreptul intern. O prelucrare care incalca prezentul regulament include si prelucrarea care incalca actele delegate si de punere in aplicare adoptate in conformitate cu prezentul regulament si cu dreptul intern care specifica norme din prezentul regulament. Persoanele vizate ar trebui sa primeasca despagubiri integrale si eficace pentru prejudiciul pe care le-au suferit. In cazul in care operatorii sau persoanele imputernicite de operatori sunt implicate in aceeasi prelucrare, fiecare operator sau fiecare persoana imputernicita de operator ar trebui sa fie considerata raspunzatoare pentru intregul prejudiciu. Cu toate acestea, atunci cand procedurile juridice care le vizeaza sunt conexate, in conformitate cu dreptul intern, despagubirile pot fi impartite in functie de raspunderea fiecarui operator sau a fiecarei persoane imputernicite de operator, cu conditia sa se asigure despagubirea integrala si efectiva a persoanei vizate care a suferit prejudiciul. Orice operator sau persoana imputernicita de operator care a platit despagubiri integrale poate formula ulterior o actiune in regres impotriva altor operatori sau persoane imputernicite de operatori implicate in aceeasi prelucrare.

(147) In cazul in care prezentul regulament cuprinde norme specifice privind competenta judiciara, in special in ceea ce priveste caile de atac judiciare, inclusiv actiunile in despagubiri, impotriva unui operator sau a unei persoane imputernicite de operator, normele generale privind competenta judiciara precum cele din Regulamentul (UE) nr. 1215/2012 al Parlamentului European si al Consiliului nu ar trebui sa aduca atingere aplicarii unor astfel de norme specifice.

(148) Pentru a consolida respectarea aplicarii normelor prevazute in prezentul regulament, ar trebui impuse sanctiuni, inclusiv amenzi administrative, pentru orice incalcare a prezentului regulament, pe langa sau in locul masurilor adecvate impuse de autoritatea de supraveghere in temeiul prezentului regulament. In cazul unei incalcari minore sau in cazul in care amenda susceptibila de a fi impusa ar constitui o sarcina disproportionata pentru o persoana fizica, poate fi emis un avertisment in locul unei amenzi. Cu toate acestea, ar trebui sa se ia in considerare in mod corespunzator natura, gravitatea si durata incalcarii, caracterul deliberat al incalcarii, actiunile intreprinse pentru a reduce prejudiciul cauzat, gradul de raspundere sau orice incalcari anterioare relevante, modul in care incalcarea a fost adusa la cunostinta autoritatii de supraveghere, conformitatea cu masurile adoptate impotriva operatorului sau a persoanei imputernicite de operator, aderarea la un cod de conduita si orice alt factor agravant sau atenuant. Impunerea de sanctiuni, inclusiv de amenzi administrative, ar

trebui sa faca obiectul unor garantii procedurale adecvate, in conformitate cu principiile generale ale dreptului Uniunii si cu carta, inclusiv o protectie judiciara eficienta si un proces echitabil.

(149) Statele membre ar trebui sa poata stabili normele privind sanctiunile penale pentru incalcarile prezentului regulament, inclusiv pentru incalcarea normelor de drept intern adoptate in temeiul si in limitele prezentului regulament. Respectivele sanctiuni penale pot, de asemenea, permite privarea de profiturile obtinute prin incalcarea prezentului regulament. Cu toate acestea, impunerea de sanctiuni penale pentru incalcari ale unor asemenea norme de drept intern si de sanctiuni administrative nu ar trebui sa duca la incalcarea principiului ne bis in idem, astfel cum a fost interpretat de Curtea de Justitie.

(150) Pentru consolidarea si armonizarea sanctiunilor administrative in cazul incalcarii prezentului regulament, fiecare autoritate de supraveghere ar trebui sa aiba competenta de a impune amenzi administrative. Prezentul regulament ar trebui sa indice incalcarile, si limita maxima si criteriile pentru stabilirea amenzilor administrative aferente, care ar trebui sa fie stabilite de autoritatea de supraveghere competenta in fiecare caz in parte, tinand seama de toate circumstantele relevante ale situatiei specifice, luandu-se in considerare in mod corespunzator, in special, natura, gravitatea si durata incalcarii, precum si consecintele acesteia si masurile luate pentru a se asigura respectarea obligatiilor in temeiul prezentului regulament si pentru a se preveni sau atenua consecintele incalcarii. In cazul in care amenzile administrative sunt impuse unei intreprinderi, o intreprindere ar trebui inteleasa ca fiind o intreprindere in conformitate cu articolele 101 si 102 din TFUE in aceste scopuri. In cazul in care se impun amenzi administrative unor persoane care nu sunt intreprinderi, autoritatea de supraveghere ar trebui sa tina seama de nivelul general al veniturilor din statul membru respectiv, precum si de situatia economica a persoanei atunci cand estimeaza cuantumul adecvat al amenzii. Mecanismul pentru asigurarea coerentei poate fi, de asemenea, utilizat pentru a promova aplicarea consecventa a amenzilor administrative. Competenta de a stabili daca si in ce masura autoritatile publice ar trebui sa faca obiectul unor amenzi administrative ar trebui sa revina statelor membre. Impunerea unei amenzi administrative sau transmiterea unei avertizari nu afecteaza aplicarea altor competente ale autoritatilor de supraveghere sau a altor sanctiuni in temeiul prezentului regulament.

(151) Sistemele juridice ale Danemarcei si Estoniei nu permit amenzi administrative astfel cum sunt prevazute in prezentul regulament. Normele privind amenzile administrative pot fi aplicate astfel incat, in Danemarca, amenda sa fie impusa de instantele nationale competente ca sanctiune penala, iar in Estonia amenda sa fie impusa de autoritatea de supraveghere in cadrul unei proceduri privind delictele, cu conditia ca o astfel de aplicare a normelor in statele membre respective sa aiba un efect echivalent cu cel al amenzilor administrative impuse de autoritatile de supraveghere. Prin urmare, instantele nationale competente ar trebui sa tina seama de recomandarea autoritatii de supraveghere care a initiat amenda. In orice caz, amenzile impuse ar trebui sa fie eficace, proportionale si disuasive.

(152) In cazul in care prezentul regulament nu armonizeaza sanctiunile administrative sau in alte cazuri, acolo unde este necesar, de exemplu in cazul unor incalcari grave ale prezentului regulament, statele membre ar trebui sa puna in aplicare un sistem care sa prevada sanctiuni eficace, proportionale si disuasive. Natura unor astfel de sanctiuni, penale sau administrative, ar trebui stabilita in dreptul intern.

(153) Dreptul statelor membre ar trebui sa stabileasca un echilibru intre normele care reglementeaza libertatea de exprimare si de informare, inclusiv exprimarea jurnalistica, academica, artistica si/sau literara, si dreptul la protectia datelor cu caracter personal in temeiul prezentului regulament. Prelucrarea datelor cu caracter personal exclusiv in scopuri jurnalistice sau in scopul exprimarii academice, artistice sau literare ar trebui sa faca obiectul unor derogari sau al unor exceptii de la anumite dispozitii ale prezentului regulament in cazul in care este necesara stabilirea unui echilibru intre dreptul la protectia datelor cu caracter personal si dreptul la libertatea de exprimare si de informare, astfel cum este prevazut in articolul 11 din carta. Acest lucru ar trebui sa se aplice in special prelucrarii datelor cu caracter personal in domeniul audiovizualului, precum si in arhivele de stiri si in bibliotecile ziarelor. Prin urmare, statele membre ar trebui sa adopte masuri legislative care sa prevada exceptiile si derogarile necesare in vederea asigurarii echilibrului intre aceste drepturi fundamentale. Statele membre ar trebui sa adopte astfel de exceptii si derogari in ceea ce priveste principiile generale, drepturile persoanelor vizate, operatorul si persoana imputernicita de operator, transferul de date cu caracter personal catre tari terte sau organizatii internationale, autoritatile de supraveghere independente, cooperarea si coerenta, precum si in ceea ce priveste situatii specifice de prelucrare a datelor. In cazul in care aceste exceptii sau derogari difera de la un stat membru la altul, ar trebui sa se aplice dreptul statului membru sub incidenta caruia intra operatorul. Pentru a tine seama de importanta dreptului la libertatea de exprimare in fiecare societate democratica, este necesar ca notiunile legate de aceasta libertate, cum ar fi jurnalismul, sa fie interpretate in sens larg.

(154) Prezentul regulament permite luarea in considerare a principiului accesului public la documente oficiale in aplicarea prezentului regulament. Accesul public la documente oficiale poate fi considerat a fi in interes public. Datele cu caracter personal din documentele detinute de o autoritate publica sau de un organism public ar trebui sa poata fi divulgate de autoritatea respectiva sau de organismul respectiv in cazul in care dreptul Uniunii sau dreptul intern sub incidenta caruia intra autoritatea publica sau organismul public prevede acest lucru. Dreptul Uniunii si dreptul intern ar trebui sa asigure un echilibru intre accesul public la documentele oficiale si reutilizarea informatiilor din sectorul public, pe de o parte, si dreptul la protectia datelor cu caracter personal, pe de alta parte, si ar putea prin urmare sa prevada echilibrul necesar cu dreptul la protectia datelor cu caracter personal in temeiul prezentului regulament. Trimiterea la autoritatile si organismele publice ar trebui, in acest context, sa includa toate autoritatile sau alte organisme reglementate de dreptul intern privind accesul public la documente. Directiva 2003/98/CE a Parlamentului European si a Consiliului lasa intact si nu aduce atingere in niciun fel nivelului de protectie a persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal in conformitate cu dreptul Uniunii si cu cel intern si, in special, nu modifica drepturile si obligatiile prevazute de prezentul regulament. In special, directiva sus-mentionata nu se aplica documentelor la care accesul este exclus sau restrans in temeiul regimurilor de acces din motive legate de protectia datelor cu caracter personal si nici partilor din documente accesibile in temeiul respectivelor regimuri care contin date cu caracter personal a caror reutilizare a fost stabilita prin lege ca fiind incompatibila cu dreptul privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal.

(155) Dreptul intern sau acordurile colective, inclusiv "acordurile de munca", pot prevedea norme specifice care sa reglementeze prelucrarea datelor cu caracter personal ale angajatilor in contextul ocuparii unui loc de munca, in special conditiile in care datele cu caracter personal in contextul ocuparii unui loc de munca pot fi prelucrate pe baza consimtamantului angajatului, in scopul recrutarii, al respectarii clauzelor contractului de munca, inclusiv descarcarea de obligatiile stabilite prin lege sau prin acorduri colective, al gestionarii, planificarii si organizarii muncii, al egalitatii si diversitatii la locul de munca, al asigurarii sanatatii si securitatii la locul de munca, precum si in scopul exercitarii si beneficierii, in mod individual sau colectiv, de drepturile si beneficiile legate de ocuparea unui loc de munca, precum si in scopul incetarii raporturilor de munca.

(156) Prelucrarea datelor cu caracter personal in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice ar trebui sa faca obiectul unor garantii adecvate pentru drepturile si libertatile persoanei vizate in temeiul prezentului regulament. Respectivele garantii ar trebui sa asigure faptul ca au fost instituite masuri tehnice si organizatorice necesare pentru a se asigura, in special, principiul reducerii la minimum a datelor. Prelucrarea ulterioara a datelor cu caracter personal in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice se efectueaza atunci cand operatorul a evaluat fezabilitatea pentru indeplinirea acestor obiective prin prelucrarea unor date cu caracter personal care nu permit sau nu mai permit identificarea persoanelor vizate, cu conditia sa existe garantii adecvate (cum ar fi pseudonimizarea datelor cu caracter personal). Statele membre ar trebui sa prevada garantii adecvate pentru prelucrarea datelor cu caracter personal in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice. Statele membre ar trebui sa fie autorizate sa ofere, in anumite conditii si sub rezerva unor garantii adecvate pentru persoanele vizate, precizari si derogari in ceea ce priveste cererile de informatii si dreptul la rectificare, dreptul la stergere, dreptul de a fi uitat, dreptul la restrictionarea prelucrarii,dreptul la portabilitatea datelor, precum si dreptul la opozitie in cazul prelucrarii datelor cu caracter personal in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice. Conditiile si garantiile in cauza pot genera proceduri specifice astfel incat persoanele vizate sa isi exercite respectivele drepturi daca acest lucru este adecvat in contextul scopurilor vizate de prelucrarea specifica, precum si masuri tehnice si organizationale vizand reducerea la minimum a prelucrarii datelor cu caracter personal, in conformitate cu principiile proportionalitatii si necesitatii. Prelucrarea datelor cu caracter personal in scopuri stiintifice ar trebui sa fie, de asemenea, conforma cu alte acte legislative relevante, cum ar fi cele privind studiile clinice.

(157) Prin combinarea informatiilor din registre, cercetatorii pot obtine noi cunostinte de mare valoare in ceea ce priveste bolile cu larga raspandire, cum ar fi bolile cardiovasculare, cancerul si depresia. Pe baza registrelor, rezultatele cercetarilor pot fi intarite, intrucat acestea se bazeaza pe o populatie mai mare. In domeniul stiintelor sociale, cercetarea pe baza registrelor le permite cercetatorilor sa obtina informatii esentiale despre corelarea pe termen lung a unei serii de conditii sociale, precum somajul sau educatia, cu alte conditii de viata. Rezultatele cercetarilor obtinute pe baza registrelor furnizeaza cunostinte solide, de inalta calitate, care pot constitui baza pentru elaborarea si punerea in aplicare a unor politici bazate pe cunoastere si care pot imbunatati calitatea vietii pentru un numar de persoane, eficienta serviciilor sociale. Pentru a facilita cercetarea stiintifica, datele cu

caracter personal pot fi prelucrate in scopuri de cercetare stiintifica, sub rezerva conditiilor si a garantiilor corespunzatoare stabilite in dreptul Uniunii sau in dreptul intern.

(158) In cazul in care datele cu caracter personal sunt prelucrate in scopuri de arhivare, prezentul regulament ar trebui sa se aplice si prelucrarii respective, tinand seama de faptul ca prezentul regulament nu ar trebui sa se aplice persoanelor decedate. Autoritatile publice sau organismele publice sau private care detin evidente de interes public ar trebui, in temeiul dreptului Uniunii sau al dreptului national, sa aiba o obligatie legala de a dobandi, a pastra, a evalua, a pregati, a descrie, a comunica, a promova, a disemina si a asigura accesul la evidente de valoare durabila de interes public general. Statele membre ar trebui, de asemenea, sa poata sa prevada prelucrarea ulterioara a datelor cu caracter personal in scopuri de arhivare, de exemplu cu scopul de a furniza informatii specifice referitoare la comportamentul politic in perioada fostelor regimuri de stat totalitare, la genociduri, la crime impotriva umanitatii, in special holocaustul, sau la crime de razboi.

(159) In cazul in care datele cu caracter personal sunt prelucrate in scopuri de cercetare stiintifica, prezentul regulament ar trebui sa se aplice si prelucrarii respective. In sensul prezentului regulament, prelucrarea datelor cu caracter personal in scopuri de cercetare stiintifica ar trebui sa fie interpretata in sens larg, incluzand de exemplu dezvoltarea tehnologica si activitatile demonstrative, cercetarea fundamentala, cercetarea aplicata si cercetarea finantata din surse private. Ar trebui, in plus, luat in considerare obiectivul Uniunii de creare a unui Spatiu european de cercetare, astfel cum este mentionat la articolul 179 alineatul (1) din TFUE. Scopurile de cercetare stiintifica ar trebui sa includa, de asemenea, studii efectuate in interes public in domeniul sanatatii publice. Pentru a indeplini caracteristicile specifice ale prelucrarii datelor cu caracter personal in scopuri de cercetare stiintifica, ar trebui sa se aplice conditii specifice, in special in ceea ce priveste publicarea sau divulgarea intr-un alt mod a datelor cu caracter personal in contextul scopurilor de cercetare stiintifica. In cazul in care rezultatul cercetarii stiintifice, in special in contextul sanatatii, constituie un motiv pentru masuri suplimentare in interesul persoanei vizate, normele generale ale prezentului regulament ar trebui sa se aplice avand in vedere aceste masuri.

(160) In cazul in care datele cu caracter personal sunt prelucrate in scopuri de cercetare istorica, prezentul regulament ar trebui sa se aplice si prelucrarii respective. Acest lucru ar trebui sa includa, de asemenea, cercetarea istorica si cercetarea in scopuri genealogice, tinand seama de faptul ca prezentul regulament nu ar trebui sa se aplice persoanelor decedate.

(161) In scopul acordarii consimtamantului de a participa la activitati de cercetare stiintifica in cadrul testelor clinice, ar trebui sa se aplice dispozitiile relevante ale Regulamentului (UE) nr. 536/2014 al Parlamentului European si al Consiliului.

(162) In cazul in care datele cu caracter personal sunt prelucrate in scopuri statistice, prezentul regulament ar trebui sa se aplice prelucrarii respective. Dreptul Uniunii sau dreptul intern ar trebui, in limitele prezentului regulament, sa determine continutul statistic, controlul accesului, specificatiile pentru prelucrarea datelor cu caracter personal in scopuri statistice si masurile adecvate pentru a proteja drepturile si libertatile persoanelor vizate si pentru a asigura confidentialitatea datelor statistice. Aceste rezultate statistice pot fi utilizate ulterior in diferite scopuri, inclusiv in scopuri de cercetare stiintifica. Scopuri statistice inseamna orice operatiune de colectare si prelucrare de date cu caracter personal necesara pentru anchetele statistice sau pentru producerea de rezultate statistice. Scopurile statistice presupun ca rezultatul prelucrarii in scopuri statistice nu constituie date cu caracter personal, ci date agregate si ca acest rezultat sau datele cu caracter personal nu sunt utilizate in sprijinul unor masuri sau decizii privind o anumita persoana fizica.

(163) Informatiile confidentiale pe care autoritatile statistice de la nivelul Uniunii si de la nivel national le colecteaza in vederea elaborarii de statistici europene si nationale oficiale ar trebui sa fie protejate. Statisticile europene ar trebui concepute, elaborate si difuzate in conformitate cu principiile statistice prevazute la articolul 338 alineatul (2) din TFUE, in timp ce statisticile nationale ar trebui, de asemenea, sa fie in conformitate cu dreptul intern. Regulamentul (CE) nr. 223/2009 al Parlamentului European si al Consiliului prevede specificatii suplimentare privind confidentialitatea datelor statistice pentru statisticile europene.

(164) In ceea ce priveste competentele autoritatilor de supraveghere de a obtine de la operator sau de la persoana imputernicita de operator accesul la datele cu caracter personal si accesul in cladirile lor, statele membre pot adopta, pe cale legislativa si in limitele stabilite de prezentul regulament, norme specifice pentru protejarea secretului profesional sau a altor obligatii echivalente, in masura in care acest lucru este necesar pentru a asigura un echilibru intre dreptul la protectia datelor cu caracter personal si obligatia de pastrare a secretului profesional. Aceasta nu aduce atingere obligatiilor existente ale statelor membre de a adopta norme privind secretul profesional in situatiile cerute de dreptul Uniunii.

(165) Prezentul regulament respecta si nu aduce atingere statutului de care beneficiaza, in temeiul dreptului constitutional existent, bisericile si asociatiile sau comunitatile religioase din statele membre, astfel cum este recunoscut in articolul 17 din TFUE.

(166) In vederea indeplinirii obiectivelor prezentului regulament, si anume protejarea drepturilor si libertatilor fundamentale ale persoanelor fizice si, in special, a dreptului acestora la protectia datelor cu caracter personal, si pentru a se garanta libera circulatie a datelor cu caracter personal pe teritoriul Uniunii, competenta de a adopta acte in conformitate cu articolul 290 din TFUE ar trebui sa fie delegata Comisiei. In special, ar trebui adoptate acte delegate in ceea ce priveste criteriile si cerintele privind mecanismele de certificare, informatiile care trebuie prezentate prin pictograme standardizate si procedurile pentru furnizarea unor astfel de pictograme. Este deosebit de important ca, in cadrul activitatii sale pregatitoare, Comisia sa organizeze consultari adecvate, inclusiv la nivel de experti. Atunci cand pregateste si elaboreaza acte delegate, Comisia ar trebui sa asigure transmiterea simultana, la timp si in mod corespunzator a documentelor relevante catre Parlamentul European si catre Consiliu.

(167) In vederea asigurarii unor conditii uniforme de punere in aplicare a prezentului regulament, Comisia ar trebui investita cu competente de executare in situatiile stabilite de prezentul regulament. Competentele respective ar trebui sa fie exercitate in conformitate cu Regulamentul (UE) nr. 182/2011. In acest context, Comisia ar trebui sa ia in considerare masuri specifice pentru microintreprinderi si pentru intreprinderile mici si mijlocii.

(168) Procedura de examinare ar trebui utilizata pentru adoptarea de acte de punere in aplicare privind: clauzele contractuale standard dintre operatori si persoanele imputernicite de operatori, precum si dintre persoanele imputernicite de operatori; codurile de conduita; standardele tehnice si mecanismele de certificare; nivelul adecvat de protectie oferit de o tara terta, de un teritoriu sau de un anumit sector de prelucrare din tara terta respectiva, sau de o organizatie internationala; clauzele standard de protectie a datelor; formatele si procedurile pentru schimbul electronic de informatii intre operatori, persoanele imputernicite de operatori si autoritatile de supraveghere pentru regulile corporatiste obligatorii; asistenta reciproca; precum si modalitatile de realizare a schimbului electronic de informatii intre autoritatile de supraveghere, precum si intre autoritatile de supraveghere si comitetul.

(169) Comisia ar trebui sa adopte acte de punere in aplicare imediat aplicabile atunci cand dovezile disponibile arata ca o tara terta, un teritoriu sau un anumit sector de prelucrare din tara terta respectiva, sau o organizatie internationala nu asigura un nivel de protectie adecvat, precum si din motive imperative de urgenta.

(170) Deoarece obiectivul prezentului regulament, si anume asigurarea unui nivel echivalent de protectie a persoanelor fizice si libera circulatie a datelor cu caracter personal in intreaga Uniune, nu poate fi realizat in mod satisfacator de catre statele membre dar, avand in vedere amploarea sau efectele actiunii, poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta masuri in conformitate cu principiul subsidiaritatii, astfel cum este definit la articolul 5 din Tratatul privind Uniunea Europeana ("Tratatul UE"). In conformitate cu principiul proportionalitatii, astfel cum este definit la articolul respectiv, prezentul regulament nu depaseste ceea ce este necesar pentru realizarea obiectivelor mentionate.

(171) Directiva 95/46/CE ar trebui sa fie abrogata prin prezentul regulament. Prelucrarile in derulare la data aplicarii prezentului regulament ar trebui sa fie aduse in conformitate cu prezentul regulament in termen de doi ani de la data intrarii in vigoare a prezentului regulament. In cazul in care prelucrarile se bazeaza pe consimtamant in temeiul Directivei 95/46/CE, nu este necesar ca persoana vizata sa isi dea inca o data consimtamantul in cazul in care modul in care consimtamantul a fost dat este in conformitate cu conditiile din prezentul regulament, astfel incat operatorului sa i se permita sa continue o astfel de prelucrare dupa data aplicarii prezentului regulament. Deciziile adoptate ale Comisiei si autorizatiile autoritatilor de supraveghere emise pe baza Directivei 95/46/CE raman in vigoare pana cand vor fi modificate, inlocuite sau abrogate.

(172) Autoritatea Europeana pentru Protectia Datelor a fost consultata in conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 si a emis un aviz la 7 martie 2012.

(173) Prezentul regulament ar trebui sa se aplice tuturor aspectelor referitoare la protectia drepturilor si libertatilor fundamentale legate de prelucrarea datelor cu caracter personal, care nu fac obiectul unor obligatii specifice cu acelasi obiectiv ca cel stabilit in Directiva 2002/58/CE a Parlamentului European si a Consiliului, inclusiv obligatiile privind operatorul si drepturile persoanelor fizice. Pentru a se clarifica relatia dintre prezentul regulament si Directiva 2002/58/CE, respectiva directiva ar trebui sa fie modificata in consecinta. Dupa adoptarea prezentului regulament, Directiva 2002/58/CE ar trebui sa fie revizuita in special pentru a se asigura coerenta cu prezentul regulament,

ADOPTA PREZENTUL REGULAMENT:

CAPITOLUL I
Dispozitii generale

Articolul 1
Obiect si obiective

(1) Prezentul regulament stabileste normele referitoare la protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal, precum si normele referitoare la libera circulatie a datelor cu caracter personal.

(2) Prezentul regulament asigura protectia drepturilor si libertatilor fundamentale ale persoanelor fizice si in special a dreptului acestora la protectia datelor cu caracter personal.

(3) Libera circulatie a datelor cu caracter personal in interiorul Uniunii nu poate fi restrictionata sau interzisa din motive legate de protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal.

Articolul 2
Domeniul de aplicare material

(1) Prezentul regulament se aplica prelucrarii datelor cu caracter personal, efectuata total sau partial prin mijloace automatizate, precum si prelucrarii prin alte mijloace decat cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenta a datelor sau care sunt destinate sa faca parte dintr-un sistem de evidenta a datelor.

(2) Prezentul regulament nu se aplica prelucrarii datelor cu caracter personal:

(a) in cadrul unei activitati care nu intra sub incidenta dreptului Uniunii;

(b) de catre statele membre atunci cand desfasoara activitati care intra sub incidenta capitolului 2 al titlului V din Tratatul UE;

(c) de catre o persoana fizica in cadrul unei activitati exclusiv personale sau domestice;

(d) de catre autoritatile competente in scopul prevenirii, investigarii, depistarii sau urmaririi penale a infractiunilor, sau al executarii sanctiunilor penale, inclusiv al protejarii impotriva amenintarilor la adresa sigurantei publice si al prevenirii acestora.

(3) Pentru prelucrarea datelor cu caracter personal de catre institutiile, organele, oficiile si agentiile Uniunii, se aplica Regulamentul (CE) nr. 45/2001. Regulamentul (CE) nr. 45/2001 si alte acte juridice ale Uniunii aplicabile unei asemenea prelucrari a datelor cu caracter personal se adapteaza la principiile si normele din prezentul regulament in conformitate cu articolul 98.

(4) Prezentul regulament nu aduce atingere aplicarii Directivei 2000/31/CE, in special normelor privind raspunderea furnizorilor de servicii intermediari, prevazute la articolele 12-15 din directiva mentionata.

Articolul 3
Domeniul de aplicare teritorial

(1) Prezentul regulament se aplica prelucrarii datelor cu caracter personal in cadrul activitatilor unui sediu al unui operator sau al unei persoane imputernicite de operator pe teritoriul Uniunii, indiferent daca prelucrarea are loc sau nu pe teritoriul Uniunii.

(2) Prezentul regulament se aplica prelucrarii datelor cu caracter personal ale unor persoane vizate care se afla in Uniune de catre un operator sau o persoana imputernicita de operator care nu este stabilit(a) in Uniune, atunci cand activitatile de prelucrare sunt legate de:

(a) oferirea de bunuri sau servicii unor astfel de persoane vizate in Uniune, indiferent daca se solicita sau nu efectuarea unei plati de catre persoana vizata; sau

(b) monitorizarea comportamentului lor daca acesta se manifesta in cadrul Uniunii.

(3) Prezentul regulament se aplica prelucrarii datelor cu caracter personal de catre un operator care nu este stabilit in Uniune, ci intr-un loc in care dreptul intern se aplica in temeiul dreptului international public.

Articolul 4
Definitii

In sensul prezentului regulament:

1. "date cu caracter personal" inseamna orice informatii privind o persoana fizica identificata sau identificabila ("persoana vizata"); o persoana fizica identificabila este o persoana care poate fi identificata, direct sau indirect, in special prin referire la un element de identificare, cum ar fi un nume, un numar de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identitatii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

2. "prelucrare" inseamna orice operatiune sau set de operatiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fara utilizarea de mijloace automatizate, cum ar fi colectarea, inregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispozitie in orice alt mod, alinierea sau combinarea, restrictionarea, stergerea sau distrugerea;

3. "restrictionarea prelucrarii" inseamna marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

4. "creare de profiluri" inseamna orice forma de prelucrare automata a datelor cu caracter personal care consta in utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoana fizica, in special pentru a analiza sau prevedea aspecte privind performanta la locul de munca, situatia economica, sanatatea, preferintele personale, interesele, fiabilitatea, comportamentul, locul in care se afla persoana fizica respectiva sau deplasarile acesteia;

5. "pseudonimizare" inseamna prelucrarea datelor cu caracter personal intr-un asemenea mod incat acestea sa nu mai poata fi atribuite unei anume persoane vizate fara a se utiliza informatii suplimentare, cu conditia ca aceste informatii suplimentare sa fie stocate separat si sa faca obiectul unor masuri de natura tehnica si organizatorica care sa asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

6. "sistem de evidenta a datelor" inseamna orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate dupa criterii functionale sau geografice;

7. "operator" inseamna persoana fizica sau juridica, autoritatea publica, agentia sau alt organism care, singur sau impreuna cu altele, stabileste scopurile si mijloacele de prelucrare a datelor cu caracter personal; atunci cand scopurile si mijloacele prelucrarii sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevazute in dreptul Uniunii sau in dreptul intern;

8. "persoana imputernicita de operator" inseamna persoana fizica sau juridica, autoritatea publica, agentia sau alt organism care prelucreaza datele cu caracter personal in numele operatorului;

9. "destinatar" inseamna persoana fizica sau juridica, autoritatea publica, agentia sau alt organism careia (caruia) ii sunt divulgate datele cu caracter personal, indiferent daca este sau nu o parte terta. Cu toate acestea, autoritatile publice carora li se pot comunica date cu caracter personal in cadrul unei anumite anchete in conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de catre autoritatile publice respective respecta normele aplicabile in materie de protectie a datelor, in conformitate cu scopurile prelucrarii;

10. "parte terta" inseamna o persoana fizica sau juridica, autoritate publica, agentie sau organism altul decat persoana vizata, operatorul, persoana imputernicita de operator si persoanele care, sub directa autoritate a operatorului sau a persoanei imputernicite de operator, sunt autorizate sa prelucreze date cu caracter personal;

11. "consimtamant" al persoanei vizate inseamna orice manifestare de vointa libera, specifica, informata si lipsita de ambiguitate a persoanei vizate prin care aceasta accepta, printr-o declaratie sau printr-o actiune fara echivoc, ca datele cu caracter personal care o privesc sa fie prelucrate;

12. "incalcarea securitatii datelor cu caracter personal" inseamna o incalcare a securitatii care duce, in mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizata a datelor cu caracter personal transmise, stocate sau prelucrate intr-un alt mod, sau la accesul neautorizat la acestea;

13. "date genetice" inseamna datele cu caracter personal referitoare la caracteristicile genetice mostenite sau dobandite ale unei persoane fizice, care ofera informatii unice privind fiziologia sau sanatatea persoanei respective si care rezulta in special in urma unei analize a unei mostre de material biologic recoltate de la persoana in cauza;

14. "date biometrice" inseamna o date cu caracter personal care rezulta in urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirma identificarea unica a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

15. "date privind sanatatea" inseamna date cu caracter personal legate de sanatatea fizica sau mentala a unei persoane fizice, inclusiv prestarea de servicii de asistenta medicala, care dezvaluie informatii despre starea de sanatate a acesteia;

16. "sediu principal" inseamna:

(a) in cazul unui operator cu sedii in cel putin doua state membre, locul in care se afla administratia centrala a acestuia in Uniune, cu exceptia cazului in care deciziile privind scopurile si mijloacele de prelucrare a datelor cu caracter personal se iau intr-un alt sediu al operatorului din Uniune, sediu care are competenta de a dispune punerea in aplicare a acestor decizii, caz in care sediul care a luat deciziile respective este considerat a fi sediul principal;

(b) in cazul unei persoane imputernicite de operator cu sedii in cel putin doua state membre, locul in care se afla administratia centrala a acesteia in Uniune, sau, in cazul in care persoana imputernicita de operator nu are o administratie centrala in Uniune, sediul din Uniune al persoanei imputernicite de operator in care au loc activitatile principale de prelucrare, in contextul activitatilor unui sediu al persoanei imputernicite de operator, in masura in care aceasta este supusa unor obligatii specifice in temeiul prezentului regulament;

17. "reprezentant" inseamna o persoana fizica sau juridica stabilita in Uniune, desemnata in scris de catre operator sau persoana imputernicita de operator in temeiul articolului 27, care reprezinta operatorul sau persoana imputernicita in ceea ce priveste obligatiile lor respective care le revin in temeiul prezentului regulament;

18. "intreprindere" inseamna o persoana fizica sau juridica ce desfasoara o activitate economica, indiferent de forma juridica a acesteia, inclusiv parteneriate sau asociatii care desfasoara in mod regulat o activitate economica;

19. "grup de intreprinderi" inseamna o intreprindere care exercita controlul si intreprinderile controlate de aceasta;

20. "reguli corporatiste obligatorii" inseamna politicile in materie de protectie a datelor cu caracter personal care trebuie respectate de un operator sau de o persoana imputernicita de operator stabilita pe teritoriul unui stat membru, in ceea ce priveste transferurile sau seturile de transferuri de date cu caracter personal catre un operator sau o persoana imputernicita de operator in una sau mai multe tari terte in cadrul unui grup de intreprinderi sau al unui grup de intreprinderi implicate intr-o activitate economica comuna;

21. "autoritate de supraveghere" inseamna o autoritate publica independenta instituita de un stat membru in temeiul articolului 51;

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

(a) operatorul sau persoana imputernicita de operator este stabilita pe teritoriul statului membru al autoritatii de supraveghere respective;

(b) persoanele vizate care isi au resedinta in statul membru in care se afla autoritatea de supraveghere respectiva sunt afectate in mod semnificativ sau sunt susceptibile de a fi afectate in mod semnificativ de prelucrare; sau

(c) la autoritatea de supraveghere respectiva a fost depusa o plangere;

23. "prelucrare transfrontaliera" inseamna:

(a) fie prelucrarea datelor cu caracter personal care are loc in contextul activitatilor sediilor din mai multe state membre ale unui operator sau ale unei persoane imputernicite de operator pe teritoriul Uniunii, daca operatorul sau persoana imputernicita de operator are sedii in cel putin doua state membre; sau

(b) fie prelucrarea datelor cu caracter personal care are loc in contextul activitatilor unui singur sediu al unui operator sau al unei persoane imputernicite de operator pe teritoriul Uniunii, dar care afecteaza in mod semnificativ sau este susceptibila de a afecta in mod semnificativ persoane vizate din cel putin doua state membre;

24. "obiectie relevanta si motivata" inseamna o obiectie la un proiect de decizie in scopul de a stabili daca exista o incalcare a prezentului regulament sau daca masurile preconizate in ceea ce priveste operatorul sau persoana imputernicita de operator respecta prezentul regulament, care demonstreaza in mod clar importanta riscurilor pe care le prezinta proiectul de decizie in ceea ce priveste drepturile si libertatile fundamentale ale persoanelor vizate si, dupa caz, libera circulatie a datelor cu caracter personal in cadrul Uniunii;

25. "serviciile societatii informationale" inseamna un serviciu astfel cum este definit la articolul 1 alineatul (1) litera (b) din Directiva 98/34/CE a Parlamentului European si a Consiliului;

26. "organizatie internationala" inseamna o organizatie si organismele sale subordonate reglementate de dreptul international public sau orice alt organism care este instituit printr-un acord incheiat intre doua sau mai multe tari sau in temeiul unui astfel de acord.

CAPITOLUL II
Principii

Articolul 5
Principii legate de prelucrarea datelor cu caracter personal

(1) Datele cu caracter personal sunt:

(a) prelucrate in mod legal, echitabil si transparent fata de persoana vizata ("legalitate, echitate si transparenta");

(b) colectate in scopuri determinate, explicite si legitime si nu sunt prelucrate ulterior intr-un mod incompatibil cu aceste scopuri; prelucrarea ulterioara in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice nu este considerata incompatibila cu scopurile initiale, in conformitate cu articolul 89 alineatul (1) ("limitari legate de scop");

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

(d) exacte si, in cazul in care este necesar, sa fie actualizate; trebuie sa se ia toate masurile necesare pentru a se asigura ca datele cu caracter personal care sunt inexacte, avand in vedere scopurile pentru care sunt prelucrate, sunt sterse sau rectificate fara intarziere ("exactitate");

(e) pastrate intr-o forma care permite identificarea persoanelor vizate pe o perioada care nu depaseste perioada necesara indeplinirii scopurilor in care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi in masura in care acestea vor fi prelucrate exclusiv in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice, in conformitate cu articolul 89 alineatul (1), sub rezerva punerii in aplicare a masurilor de ordin tehnic si organizatoric adecvate prevazute in prezentul regulament in vederea garantarii drepturilor si libertatilor persoanei vizate ("limitari legate de stocare");

(f) prelucrate intr-un mod care asigura securitatea adecvata a datelor cu caracter personal, inclusiv protectia impotriva prelucrarii neautorizate sau ilegale si impotriva pierderii, a distrugerii sau a deteriorarii accidentale, prin luarea de masuri tehnice sau organizatorice corespunzatoare ("integritate si confidentialitate").

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

Articolul 6
Legalitatea prelucrarii

(1) Prelucrarea este legala numai daca si in masura in care se aplica cel putin una dintre urmatoarele conditii:

(a) persoana vizata si-a dat consimtamantul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

(b) prelucrarea este necesara pentru executarea unui contract la care persoana vizata este parte sau pentru a face demersuri la cererea persoanei vizate inainte de incheierea unui contract;

(c) prelucrarea este necesara in vederea indeplinirii unei obligatii legale care ii revine operatorului;

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

(e) prelucrarea este necesara pentru indeplinirea unei sarcini care serveste unui interes public sau care rezulta din exercitarea autoritatii publice cu care este investit operatorul;

(f) prelucrarea este necesara in scopul intereselor legitime urmarite de operator sau de o parte terta, cu exceptia cazului in care prevaleaza interesele sau drepturile si libertatile fundamentale ale persoanei vizate, care necesita protejarea datelor cu caracter personal, in special atunci cand persoana vizata este un copil.

Litera (f) din primul paragraf nu se aplica in cazul prelucrarii efectuate de autoritati publice in indeplinirea atributiilor lor.

(2) Statele membre pot mentine sau introduce dispozitii mai specifice de adaptare a aplicarii normelor prezentului regulament in ceea ce priveste prelucrarea in vederea respectarii alineatului (1) literele (c) si (e) prin definirea unor cerinte specifice mai precise cu privire la prelucrare si a altor masuri de asigurare a unei

prelucrari legale si echitabile, inclusiv pentru alte situatii concrete de prelucrare, astfel cum este prevazut in capitolul IX.

(3) Temeiul pentru prelucrarea mentionata la alineatul (1) literele (c) si (e) trebuie sa fie prevazut in:

(a) dreptul Uniunii; sau

(b) dreptul intern care se aplica operatorului.

Scopul prelucrarii este stabilit pe baza respectivului temei juridic sau, in ceea ce priveste prelucrarea mentionata la alineatul (1) litera (e), este necesar pentru indeplinirea unei sarcini efectuate in interes public sau in cadrul exercitarii unei functii publice atribuite operatorului. Respectivul temei juridic poate contine dispozitii specifice privind adaptarea aplicarii normelor prezentului regulament, printre altele: conditiile generale care reglementeaza legalitatea prelucrarii de catre operator; tipurile de date care fac obiectul prelucrarii; persoanele vizate; entitatile carora le pot fi divulgate datele si scopul pentru care respectivele date cu caracter personal pot fi divulgate; limitarile legate de scop; perioadele de stocare; si operatiunile si procedurile de prelucrare, inclusiv masurile de asigurare a unei prelucrari legale si echitabile cum sunt cele pentru alte situatii concrete de prelucrare astfel cum sunt prevazute in capitolul IX. Dreptul Uniunii sau dreptul intern urmareste un obiectiv de interes public si este proportional cu obiectivul legitim urmarit.

(4) In cazul in care prelucrarea in alt scop decat cel pentru care datele cu caracter personal au fost colectate nu se bazeaza pe consimtamantul persoanei vizate sau pe dreptul Uniunii sau dreptul intern, care constituie o masura necesara si proportionala intr-o societate democratica pentru a proteja obiectivele mentionate la articolul 23 alineatul (1), operatorul, pentru a stabili daca prelucrarea in alt scop este compatibila cu scopul pentru care datele cu caracter personal au fost colectate initial, ia in considerare, printre altele:

(a) orice legatura dintre scopurile in care datele cu caracter personal au fost colectate si scopurile prelucrarii ulterioare preconizate;

(b) contextul in care datele cu caracter personal au fost colectate, in special in ceea ce priveste relatia dintre persoanele vizate si operator;

(c) natura datelor cu caracter personal, in special in cazul prelucrarii unor categorii speciale de date cu caracter personal, in conformitate cu articolul 9, sau in cazul in care sunt prelucrate date cu caracter personal referitoare la condamnari penale si infractiuni, in conformitate cu articolul 10;

(d) posibilele consecinte asupra persoanelor vizate ale prelucrarii ulterioare preconizate;

(e) existenta unor garantii adecvate, care pot include criptarea sau pseudonimizarea.

Articolul 7
Conditii privind consimtamantul

(1) In cazul in care prelucrarea se bazeaza pe consimtamant, operatorul trebuie sa fie in masura sa demonstreze ca persoana vizata si-a dat consimtamantul pentru prelucrarea datelor sale cu caracter personal.

(2) In cazul in care consimtamantul persoanei vizate este dat in contextul unei declaratii scrise care se refera si la alte aspecte, cererea privind consimtamantul trebuie sa fie prezentata intr-o forma care o diferentiaza in mod clar de celelalte aspecte, intr-o forma inteligibila si usor accesibila, utilizand un limbaj clar si simplu. Nicio parte a respectivei declaratii care constituie o incalcare a prezentului regulament nu este obligatorie.

(3) Persoana vizata are dreptul sa isi retraga in orice moment consimtamantul. Retragerea consimtamantului nu afecteaza legalitatea prelucrarii efectuate pe baza consimtamantului inainte de retragerea acestuia. Inainte de acordarea consimtamantului, persoana vizata este informata cu privire la acest lucru. Retragerea consimtamantului se face la fel de simplu ca acordarea acestuia.

(4) Atunci cand se evalueaza daca consimtamantul este dat in mod liber, se tine seama cat mai mult de faptul ca, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este conditionata sau nu de consimtamantul cu privire la prelucrarea datelor cu caracter personal care nu este necesara pentru executarea acestui contract.

Articolul 8
Conditii aplicabile in ceea ce priveste consimtamantul copiilor in legatura cu serviciile societatii informationale

(1) In cazul in care se aplica articolul 6 alineatul (1) litera (a), in ceea ce priveste oferirea de servicii ale societatii informationale in mod direct unui copil, prelucrarea datelor cu caracter personal ale unui copil este legala daca copilul are cel putin varsta de 16 ani. Daca copilul are sub varsta de 16 ani, respectiva prelucrare

este legala numai daca si in masura in care consimtamantul respectiv este acordat sau autorizat de titularul raspunderii parintesti asupra copilului.

Statele membre pot prevedea prin lege o varsta inferioara in aceste scopuri, cu conditia ca acea varsta inferioara sa nu fie mai mica de 13 ani.

(2) Operatorul depune toate eforturile rezonabile pentru a verifica in astfel de cazuri ca titularul raspunderii parintesti a acordat sau a autorizat consimtamantul, tinand seama de tehnologiile disponibile.

(3) Alineatul (1) nu afecteaza dreptul general al contractelor aplicabil in statele membre, cum ar fi normele privind valabilitatea, incheierea sau efectele unui contract in legatura cu un copil.

Articolul 9

Prelucrarea de categorii speciale de date cu caracter personal

(1) Se interzice prelucrarea de date cu caracter personal care dezvaluie originea rasiala sau etnica, opiniile politice, confesiunea religioasa sau convingerile filozofice sau apartenenta la sindicate si prelucrarea de date genetice, de date biometrice pentru identificarea unica a unei persoane fizice, de date privind sanatatea sau de date privind viata sexuala sau orientarea sexuala ale unei persoane fizice.

(2) Alineatul (1) nu se aplica in urmatoarele situatii:

(a) persoana vizata si-a dat consimtamantul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu exceptia cazului in care dreptul Uniunii sau dreptul intern prevede ca interdictia prevazuta la alineatul (1) sa nu poata fi ridicata prin consimtamantul persoanei vizate;

(b) prelucrarea este necesara in scopul indeplinirii obligatiilor si al exercitarii unor drepturi specifice ale operatorului sau ale persoanei vizate in domeniul ocuparii fortei de munca si al securitatii sociale si protectiei sociale, in masura in care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de munca incheiat in temeiul dreptului intern care prevede garantii adecvate pentru drepturile fundamentale si interesele persoanei vizate;

(c) prelucrarea este necesara pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci cand persoana vizata se afla in incapacitate fizica sau juridica de a-si da consimtamantul;

(d) prelucrarea este efectuata in cadrul activitatilor lor legitime si cu garantii adecvate de catre o fundatie, o asociatie sau orice alt organism fara scop lucrativ si cu specific politic, filozofic, religios sau sindical, cu conditia ca prelucrarea sa se refere numai la membrii sau la fostii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente in legatura cu scopurile sale si ca datele cu caracter personal sa nu fie comunicate tertilor fara consimtamantul persoanelor vizate;

(e) prelucrarea se refera la date cu caracter personal care sunt facute publice in mod manifest de catre persoana vizata;

(f) prelucrarea este necesara pentru constatarea, exercitarea sau apararea unui drept in instanta sau ori de cate ori instantele actioneaza in exercitiul functiei lor judiciare;

(g) prelucrarea este necesara din motive de interes public major, in baza dreptului Uniunii sau a dreptului intern, care este proportional cu obiectivul urmarit, respecta esenta dreptului la protectia datelor si prevede masuri corespunzatoare si specifice pentru protejarea drepturilor fundamentale si a intereselor persoanei vizate;

(h) prelucrarea este necesara in scopuri legate de medicina preventiva sau a muncii, de evaluarea capacitatii de munca a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistenta medicala sau sociala sau a unui tratament medical sau de gestionarea sistemelor si serviciilor de sanatate sau de asistenta sociala, in temeiul dreptului Uniunii sau al dreptului intern sau in temeiul unui contract incheiat cu un cadru medical si sub rezerva respectarii conditiilor si garantiilor prevazute la alineatul (3);

(i) prelucrarea este necesara din motive de interes public in domeniul sanatatii publice, cum ar fi protectia impotriva amenintarilor transfrontaliere grave la adresa sanatatii sau asigurarea de standarde ridicate de calitate si siguranta a asistentei medicale si a medicamentelor sau a dispozitivelor medicale, in temeiul dreptului Uniunii sau al dreptului intern, care prevede masuri adecvate si specifice pentru protejarea drepturilor si libertatilor persoanei vizate, in special a secretului profesional; sau

(j) prelucrarea este necesara in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice, in conformitate cu articolul 89 alineatul (1), in baza dreptului Uniunii sau a dreptului intern, care este proportional cu obiectivul urmarit, respecta esenta dreptului la protectia datelor si prevede masuri corespunzatoare si specifice pentru protejarea drepturilor fundamentale si a intereselor persoanei vizate.

(3) Datele cu caracter personal mentionate la alineatul (1) pot fi prelucrate in scopurile mentionate la alineatul (2) litera (h) in cazul in care datele respective sunt prelucrate de catre un profesionist supus obligatiei de pastrare a secretului profesional sau sub responsabilitatea acestuia, in temeiul dreptului Uniunii sau al dreptului intern sau in temeiul normelor stabilite de organisme nationale competente sau de o alta persoana supusa, de asemenea, unei obligatii de confidentialitate in temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme nationale competente.

(4) Statele membre pot mentine sau introduce conditii suplimentare, inclusiv restrictii, in ceea ce priveste prelucrarea de date genetice, date biometrice sau date privind sanatatea.

Articolul 10

Prelucrarea de date cu caracter personal referitoare la condamnari penale si infractiuni

Prelucrarea de date cu caracter personal referitoare la condamnari penale si infractiuni sau la masuri de securitate conexe in temeiul articolului 6 alineatul (1) se efectueaza numai sub controlul unei autoritati de stat sau atunci cand prelucrarea este autorizata de dreptul Uniunii sau de dreptul intern care prevede garantii adecvate pentru drepturile si libertatile persoanelor vizate. Orice registru cuprinzator al condamnarilor penale se tine numai sub controlul unei autoritati de stat.

Articolul 11

Prelucrarea care nu necesita identificare

(1) In cazul in care scopurile pentru care un operator prelucreaza date cu caracter personal nu necesita sau nu mai necesita identificarea unei persoane vizate de catre operator, operatorul nu are obligatia de a pastra, obtine sau prelucra informatii suplimentare pentru a identifica persoana vizata in scopul unic al respectarii prezentului regulament.

(2) Daca, in cazurile mentionate la alineatul (1) din prezentul articol, operatorul poate demonstra ca nu este in masura sa identifice persoana vizata, operatorul informeaza persoana vizata in mod corespunzator, in cazul in care este posibil. In astfel de cazuri, articolele 15-20 nu se aplica, cu exceptia cazului in care persoana vizata, in scopul exercitarii drepturilor sale in temeiul respectivelor articole, ofera informatii suplimentare care permit identificarea sa.

CAPITOLUL III

Drepturile persoanei vizate

Sectiunea 1

Transparenta si modalitati

Articolul 12

Transparenta informatiilor, a comunicarilor si a modalitatilor de exercitare a drepturilor persoanei vizate

(1) Operatorul ia masuri adecvate pentru a furniza persoanei vizate orice informatii mentionate la articolele 13 si 14 si orice comunicari in temeiul articolelor 15-22 si 34 referitoare la prelucrare, intr-o forma concisa, transparenta, inteligibila si usor accesibila, utilizand un limbaj clar si simplu, in special pentru orice informatii adresate in mod specific unui copil. Informatiile se furnizeaza in scris sau prin alte mijloace, inclusiv, atunci cand este oportun, in format electronic. La solicitarea persoanei vizate, informatiile pot fi furnizate verbal, cu conditia ca identitatea persoanei vizate sa fie dovedita prin alte mijloace.

(2) Operatorul faciliteaza exercitarea drepturilor persoanei vizate in temeiul articolelor 15-22. In cazurile mentionate la articolul 11 alineatul (2), operatorul nu refuza sa dea curs cererii persoanei vizate de a-si exercita drepturile in conformitate cu articolele 15-22, cu exceptia cazului in care operatorul demonstreaza ca nu este in masura sa identifice persoana vizata.

(3) Operatorul furnizeaza persoanei vizate informatii privind actiunile intreprinse in urma unei cereri in temeiul articolelor 15-22, fara intarzieri nejustificate si in orice caz in cel mult o luna de la primirea cererii. Aceasta perioada poate fi prelungita cu doua luni atunci cand este necesar, tinandu-se seama de complexitatea si

numarul cererilor. Operatorul informeaza persoana vizata cu privire la orice astfel de prelungire, in termen de o luna de la primirea cererii, prezentand si motivele intarzierii. In cazul in care persoana vizata introduce o cerere in format electronic, informatiile sunt furnizate in format electronic acolo unde este posibil, cu exceptia cazului in care persoana vizata solicita un alt format.

(4) Daca nu ia masuri cu privire la cererea persoanei vizate, operatorul informeaza persoana vizata, fara intarziere si in termen de cel mult o luna de la primirea cererii, cu privire la motivele pentru care nu ia masuri si la posibilitatea de a depune o plangere in fata unei autoritati de supraveghere si de a introduce o cale de atac judiciara.

(5) Informatiile furnizate in temeiul articolelor 13 si 14 si orice comunicare si orice masuri luate in temeiul articolelor 15-22 si 34 sunt oferite gratuit. In cazul in care cererile din partea unei persoane vizate sunt in mod vadit nefondate sau excesive, in special din cauza caracterului lor repetitiv, operatorul poate:

(a) fie sa perceapa o taxa rezonabila tinand cont de costurile administrative pentru furnizarea informatiilor sau a comunicarii sau pentru luarea masurilor solicitate;

(b) fie sa refuze sa dea curs cererii.

In aceste cazuri, operatorului ii revine sarcina de a demonstra caracterul vadit nefondat sau excesiv al cererii.

(6) Fara a aduce atingere articolului 11, in cazul in care are indoieli intemeiate cu privire la identitatea persoanei fizice care inainteaza cererea mentionata la articolele 15-21, operatorul poate solicita furnizarea de informatii suplimentare necesare pentru a confirma identitatea persoanei vizate.

(7) Informatiile care urmeaza sa fie furnizate persoanelor vizate in temeiul articolelor 13 si 14 pot fi furnizate in combinatie cu pictograme standardizate pentru a oferi intr-un mod usor vizibil, inteligibil si clar lizibil o imagine de ansamblu semnificativa asupra prelucrarii avute in vedere. In cazul in care pictogramele sunt prezentate in format electronic, acestea trebuie sa poata fi citite automat.

(8) Comisia este imputernicita sa adopte acte delegate in conformitate cu articolul 92 in vederea determinarii informatiilor care urmeaza sa fie prezentate de pictograme si a procedurilor pentru furnizarea de pictograme standardizate.

Sectiunea 2
Informare si acces la date cu caracter personal

Articolul 13
Informatii care se furnizeaza in cazul in care datele cu caracter personal sunt colectate de la persoana vizata

(1) In cazul in care datele cu caracter personal referitoare la o persoana vizata sunt colectate de la aceasta, operatorul, in momentul obtinerii acestor date cu caracter personal, furnizeaza persoanei vizate toate informatiile urmatoare:

(a) identitatea si datele de contact ale operatorului si, dupa caz, ale reprezentantului acestuia;

(b) datele de contact ale responsabilului cu protectia datelor, dupa caz;

(c) scopurile in care sunt prelucrate datele cu caracter personal, precum si temeiul juridic al prelucrarii;

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

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

(f) daca este cazul, intentia operatorului de a transfera date cu caracter personal catre o tara terta sau o organizatie internationala si existenta sau absenta unei decizii a Comisiei privind caracterul adecvat sau, in cazul transferurilor mentionate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf, o trimitere la garantiile adecvate sau corespunzatoare si la mijloacele de a obtine o copie a acestora, in cazul in care acestea au fost puse la dispozitie.

(2) In plus fata de informatiile mentionate la alineatul (1), in momentul in care datele cu caracter personal sunt obtinute, operatorul furnizeaza persoanei vizate urmatoarele informatii suplimentare necesare pentru a asigura o prelucrare echitabila si transparenta:

(a) perioada pentru care vor fi stocate datele cu caracter personal sau, daca acest lucru nu este posibil, criteriile utilizate pentru a stabili aceasta perioada;

(b) existenta dreptului de a solicita operatorului, in ceea ce priveste datele cu caracter personal referitoare la persoana vizata, accesul la acestea, rectificarea sau stergerea acestora sau restrictionarea prelucrarii sau a dreptului de a se opune prelucrarii, precum si a dreptului la portabilitatea datelor;

(c) atunci cand prelucrarea se bazeaza pe articolul 6 alineatul (1) litera (a) sau pe articolul 9 alineatul (2) litera (a), existenta dreptului de a retrage consimtamantul in orice moment, fara a afecta legalitatea prelucrarii efectuate pe baza consimtamantului inainte de retragerea acestuia;

(d) dreptul de a depune o plangere in fata unei autoritati de supraveghere;

(e) daca furnizarea de date cu caracter personal reprezinta o obligatie legala sau contractuala sau o obligatie necesara pentru incheierea unui contract, precum si daca persoana vizata este obligata sa furnizeze aceste date cu caracter personal si care sunt eventualele consecinte ale nerespectarii acestei obligatii;

(f) existenta unui proces decizional automatizat incluzand crearea de profiluri, mentionat la articolul 22 alineatele (1) si (4), precum si, cel putin in cazurile respective, informatii pertinente privind logica utilizata si privind importanta si consecintele preconizate ale unei astfel de prelucrari pentru persoana vizata.

(3) In cazul in care operatorul intentioneaza sa prelucreze ulterior datele cu caracter personal intr-un alt scop decat cel pentru care acestea au fost colectate, operatorul furnizeaza persoanei vizate, inainte de aceasta prelucrare ulterioara, informatii privind scopul secundar respectiv si orice informatii suplimentare relevante, in conformitate cu alineatul (2).

(4) Alineatele (1), (2) si (3) nu se aplica daca si in masura in care persoana vizata detine deja informatiile respective.

Articolul 14
Informatii care se furnizeaza in cazul in care datele cu caracter personal nu au fost obtinute de la persoana vizata

(1) In cazul in care datele cu caracter personal nu au fost obtinute de la persoana vizata, operatorul furnizeaza persoanei vizate urmatoarele informatii:

(a) identitatea si datele de contact ale operatorului si, dupa caz, ale reprezentantului acestuia;

(b) datele de contact ale responsabilului cu protectia datelor, dupa caz;

(c) scopurile in care sunt prelucrate datele cu caracter personal, precum si temeiul juridic al prelucrarii;

(d) categoriile de date cu caracter personal vizate;

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

(f) daca este cazul, intentia operatorului de a transfera date cu caracter personal catre un destinatar dintr-o tara terta sau o organizatie internationala si existenta sau absenta unei decizii a Comisiei privind caracterul adecvat sau, in cazul transferurilor mentionate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf, o trimitere la garantiile adecvate sau corespunzatoare si la mijloacele de a obtine o copie a acestora, in cazul in care acestea au fost puse la dispozitie.

(2) Pe langa informatiile mentionate la alineatul (1), operatorul furnizeaza persoanei vizate urmatoarele informatii necesare pentru a asigura o prelucrare echitabila si transparenta in ceea ce priveste persoana vizata:

(a) perioada pentru care vor fi stocate datele cu caracter personal sau, daca acest lucru nu este posibil, criteriile utilizate pentru a stabili aceasta perioada;

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

(c) existenta dreptului de a solicita operatorului, in ceea ce priveste datele cu caracter personal referitoare la persoana vizata, accesul la acestea, rectificarea sau stergerea acestora sau restrictionarea prelucrarii si a dreptului de a se opune prelucrarii, precum si a dreptului la portabilitatea datelor;

(d) atunci cand prelucrarea se bazeaza pe articolul 6 alineatul (1) litera (a) sau pe articolul 9 alineatul (2) litera (a), existenta dreptului de a retrage consimtamantul in orice moment, fara a afecta legalitatea prelucrarii efectuate pe baza consimtamantului inainte de retragerea acestuia;

(e) dreptul de a depune o plangere in fata unei autoritati de supraveghere;

(f) sursa din care provin datele cu caracter personal si, daca este cazul, daca acestea provin din surse disponibile public;

(g) existenta unui proces decizional automatizat incluzand crearea de profiluri, mentionat la articolul 22 alineatele (1) si (4), precum si, cel putin in cazurile respective, informatii pertinente privind logica utilizata si privind importanta si consecintele preconizate ale unei astfel de prelucrari pentru persoana vizata.

(3) Operatorul furnizeaza informatiile mentionate la alineatele (1) si (2):

(a) intr-un termen rezonabil dupa obtinerea datelor cu caracter personal, dar nu mai mare de o luna, tinandu-se seama de circumstantele specifice in care sunt prelucrate datele cu caracter personal;

(b) daca datele cu caracter personal urmeaza sa fie utilizate pentru comunicarea cu persoana vizata, cel tarziu in momentul primei comunicari catre persoana vizata respectiva; sau

(c) daca se intentioneaza divulgarea datelor cu caracter personal catre un alt destinatar, cel mai tarziu la data la care acestea sunt divulgate pentru prima oara.

(4) In cazul in care operatorul intentioneaza sa prelucreze ulterior datele cu caracter personal intr-un alt scop decat cel pentru care acestea au fost obtinute, operatorul furnizeaza persoanei vizate, inainte de aceasta prelucrare ulterioara, informatii privind scopul secundar respectiv si orice informatii suplimentare relevante, in conformitate cu alineatul (2).

(5) Alineatele (1)-(4) nu se aplica daca si in masura in care:

(a) persoana vizata detine deja informatiile;

(b) furnizarea acestor informatii se dovedeste a fi imposibila sau ar implica eforturi disproportionate, in special in cazul prelucrarii in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice, sub rezerva conditiilor si a garantiilor prevazute la articolul 89 alineatul (1), sau in masura in care obligatia mentionata la alineatul (1) din prezentul articol este susceptibil sa faca imposibila sau sa afecteze in mod grav realizarea obiectivelor prelucrarii respective In astfel de cazuri, operatorul ia masuri adecvate pentru a proteja drepturile, libertatile si interesele legitime ale persoanei vizate, inclusiv punerea informatiilor la dispozitia publicului;

(c) obtinerea sau divulgarea datelor este prevazuta in mod expres de dreptul Uniunii sau de dreptul intern sub incidenta caruia intra operatorul si care prevede masuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau

(d) in cazul in care datele cu caracter personal trebuie sa ramana confidentiale in temeiul unei obligatii statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligatii legale de a pastra secretul.

Articolul 15

Dreptul de acces al persoanei vizate

(1) Persoana vizata are dreptul de a obtine din partea operatorului o confirmare ca se prelucreaza sau nu date cu caracter personal care o privesc si, in caz afirmativ, acces la datele respective si la urmatoarele informatii:

(a) scopurile prelucrarii;

(b) categoriile de date cu caracter personal vizate;

(c) destinatarii sau categoriile de destinatari carora datele cu caracter personal le-au fost sau urmeaza sa le fie divulgate, in special destinatari din tari terte sau organizatii internationale;

(d) acolo unde este posibil, perioada pentru care se preconizeaza ca vor fi stocate datele cu caracter personal sau, daca acest lucru nu este posibil, criteriile utilizate pentru a stabili aceasta perioada;

(e) existenta dreptului de a solicita operatorului rectificarea sau stergerea datelor cu caracter personal ori restrictionarea prelucrarii datelor cu caracter personal referitoare la persoana vizata sau a dreptului de a se opune prelucrarii;

(f) dreptul de a depune o plangere in fata unei autoritati de supraveghere;

(g) in cazul in care datele cu caracter personal nu sunt colectate de la persoana vizata, orice informatii disponibile privind sursa acestora;

(h) existenta unui proces decizional automatizat incluzand crearea de profiluri, mentionat la articolul 22 alineatele (1) si (4), precum si, cel putin in cazurile respective, informatii pertinente privind logica utilizata si privind importanta si consecintele preconizate ale unei astfel de prelucrari pentru persoana vizata.

(2) In cazul in care datele cu caracter personal sunt transferate catre o tara terta sau o organizatie internationala, persoana vizata are dreptul sa fie informata cu privire la garantiile adecvate in temeiul articolului 46 referitoare la transfer.

(3) Operatorul furnizeaza o copie a datelor cu caracter personal care fac obiectul prelucrarii. Pentru orice alte copii solicitate de persoana vizata, operatorul poate percepe o taxa rezonabila, bazata pe costurile administrative. In cazul in care persoana vizata introduce cererea in format electronic si cu exceptia cazului in care persoana vizata solicita un alt format, informatiile sunt furnizate intr-un format electronic utilizat in mod curent.

(4) Dreptul de a obtine o copie mentionata la alineatul (3) nu aduce atingere drepturilor si libertatilor altora.

Sectiunea 3
Rectificare si stergere

Articolul 16
Dreptul la rectificare

Persoana vizata are dreptul de a obtine de la operator, fara intarzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Tinandu-se seama de scopurile in care au fost prelucrate datele, persoana vizata are dreptul de a obtine completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declaratii suplimentare.

Articolul 17
Dreptul la stergerea datelor ("dreptul de a fi uitat")

(1) Persoana vizata are dreptul de a obtine din partea operatorului stergerea datelor cu caracter personal care o privesc, fara intarzieri nejustificate, iar operatorul are obligatia de a sterge datele cu caracter personal fara intarzieri nejustificate in cazul in care se aplica unul dintre urmatoarele motive:

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

(b) persoana vizata isi retrage consimtamantul pe baza caruia are loc prelucrarea, in conformitate cu articolul 6 alineatul (1) litera (a) sau cu articolul 9 alineatul (2) litera (a), si nu exista niciun alt temei juridic pentru prelucrarea;

(c) persoana vizata se opune prelucrarii in temeiul articolului 21 alineatul (1) si nu exista motive legitime care sa prevaleze in ceea ce priveste prelucrarea sau persoana vizata se opune prelucrarii in temeiul articolului 21 alineatul (2);

(d) datele cu caracter personal au fost prelucrate ilegal;

(e) datele cu caracter personal trebuie sterse pentru respectarea unei obligatii legale care revine operatorului in temeiul dreptului Uniunii sau al dreptului intern sub incidenta caruia se afla operatorul;

(f) datele cu caracter personal au fost colectate in legatura cu oferirea de servicii ale societatii informationale mentionate la articolul 8 alineatul (1).

(2) In cazul in care operatorul a facut publice datele cu caracter personal si este obligat, in temeiul alineatului (1), sa le stearga, operatorul, tinand seama de tehnologia disponibila si de costul implementarii, ia masuri rezonabile, inclusiv masuri tehnice, pentru a informa operatorii care prelucreaza datele cu caracter personal ca persoana vizata a solicitat stergerea de catre acesti operatori a oricaror linkuri catre datele respective sau a oricaror copii sau reproduceri ale acestor date cu caracter personal.

(3) Alineatele (1) si (2a) nu se aplica in masura in care prelucrarea este necesara:

(a) pentru exercitarea dreptului la libera exprimare si la informare;

(b) pentru respectarea unei obligatii legale care prevede prelucrarea in temeiul dreptului Uniunii sau al dreptului intern care se aplica operatorului sau pentru indeplinirea unei sarcini executate in interes public sau in cadrul exercitarii unei autoritati oficiale cu care este investit operatorul;

(c) din motive de interes public in domeniul sanatatii publice, in conformitate cu articolul 9 alineatul (2) literele (h) si (i) si cu articolul 9 alineatul (3);

(d) in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice, in conformitate cu articolul 89 alineatul (1), in masura in care dreptul mentionat la alineatul (1) este susceptibil sa faca imposibila sau sa afecteze in mod grav realizarea obiectivelor prelucrarii respective; sau

(e) pentru constatarea, exercitarea sau apararea unui drept in instanta.

Articolul 18
Dreptul la restrictionarea prelucrarii

(1) Persoana vizata are dreptul de a obtine din partea operatorului restrictionarea prelucrarii in cazul in care se aplica unul din urmatoarele cazuri:

(a) persoana vizata contesta exactitatea datelor, pentru o perioada care ii permite operatorului sa verifice exactitatea datelor;

(b) prelucrarea este ilegala, iar persoana vizata se opune stergerii datelor cu caracter personal, solicitand in schimb restrictionarea utilizarii lor;

(c) operatorul nu mai are nevoie de datele cu caracter personal in scopul prelucrarii, dar persoana vizata i le solicita pentru constatarea, exercitarea sau apararea unui drept in instanta; sau

(d) persoana vizata s-a opus prelucrarii in conformitate cu articolul 21 alineatul (1), pentru intervalul de timp in care se verifica daca drepturile legitime ale operatorului prevaleaza asupra celor ale persoanei vizate.

(2) In cazul in care prelucrarea a fost restrictionata in temeiul alineatului (1), astfel de date cu caracter personal pot, cu exceptia stocarii, sa fie prelucrate numai cu consimtamantul persoanei vizate sau pentru constatarea, exercitarea sau apararea unui drept in instanta sau pentru protectia drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

(3) O persoana vizata care a obtinut restrictionarea prelucrarii in temeiul alineatului (1) este informata de catre operator inainte de ridicarea restrictiei de prelucrare.

Articolul 19

Obligatia de notificare privind rectificarea sau stergerea datelor cu caracter personal sau restrictionarea prelucrarii

Operatorul comunica fiecarui destinatar caruia i-au fost divulgate datele cu caracter personal orice rectificare sau stergere a datelor cu caracter personal sau restrictionare a prelucrarii efectuate in conformitate cu articolul 16, articolul 17 alineatul (1) si articolul 18, cu exceptia cazului in care acest lucru se dovedeste imposibil sau presupune eforturi disproportionate. Operatorul informeaza persoana vizata cu privire la destinatarii respectivi daca persoana vizata solicita acest lucru.

Articolul 20

Dreptul la portabilitatea datelor

(1) Persoana vizata are dreptul de a primi datele cu caracter personal care o privesc si pe care le-a furnizat operatorului intr-un format structurat, utilizat in mod curent si care poate fi citit automat si are dreptul de a transmite aceste date altui operator, fara obstacole din partea operatorului caruia i-au fost furnizate datele cu caracter personal, in cazul in care:

(a) prelucrarea se bazeaza pe consimtamant in temeiul articolului 6 alineatul (1) litera (a) sau al articolului 9 alineatul (2) litera (a) sau pe un contract in temeiul articolului 6 alineatul (1) litera (b); si

(b) prelucrarea este efectuata prin mijloace automate.

(2) In exercitarea dreptului sau la portabilitatea datelor in temeiul alineatului (1), persoana vizata are dreptul ca datele cu caracter personal sa fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic.

(3) Exercitarea dreptului mentionat la alineatul (1) din prezentul articol nu aduce atingere articolului 17. Respectivul drept nu se aplica prelucrarii necesare pentru indeplinirea unei sarcini executate in interes public sau in cadrul exercitarii unei autoritati oficiale cu care este investit operatorul.

(4) Dreptul mentionat la alineatul (1) nu aduce atingere drepturilor si libertatilor altora.

Sectiunea 4

Dreptul la o pozitie si procesul decizional individual automatizat

Articolul 21

Dreptul la opozitie

(1) In orice moment, persoana vizata are dreptul de a se opune, din motive legate de situatia particulara in care se afla, prelucrarii in temeiul articolului 6 alineatul (1) litera (e) sau (f) sau al articolului 6 alineatul (1) a datelor cu caracter personal care o privesc, inclusiv crearii de profiluri pe baza respectivelor dispozitii. Operatorul nu mai prelucreaza datele cu caracter personal, cu exceptia cazului in care operatorul demonstreaza ca are motive legitime si imperioase care justifica prelucrarea si care prevaleaza asupra intereselor, drepturilor si libertatilor persoanei vizate sau ca scopul este constatarea, exercitarea sau apararea unui drept in instanta.

(2) Atunci cand prelucrarea datelor cu caracter personal are drept scop marketingul direct, persoana vizata are dreptul de a se opune in orice moment prelucrarii in acest scop a datelor cu caracter personal care o privesc, inclusiv crearii de profiluri, in masura in care este legata de marketingul direct respectiv.

(3) In cazul in care persoana vizata se opune prelucrarii in scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate in acest scop.

(4) Cel tarziu in momentul primei comunicari cu persoana vizata, dreptul mentionat la alineatele (1) si (2) este adus in mod explicit in atentia persoanei vizate si este prezentat in mod clar si separat de orice alte informatii.

(5) In contextual utilizarii serviciilor societatii informationale si in pofida Directivei 2002/58/CE, persoana vizata isi poate exercita dreptul de a se opune prin mijloace automate care utilizeaza specificatii tehnice.

(6) In cazul in care datele cu caracter personal sunt prelucrate in scopuri de cercetare stiintifica sau istorica sau in scopuri statistice in conformitate cu articolul 89 alineatul (1), persoana vizata, din motive legate de situatia sa particulara, are dreptul de a se opune prelucrarii datelor cu caracter personal care o privesc, cu exceptia cazului in care prelucrarea este necesara pentru indeplinirea unei sarcini din motive de interes public.

Articolul 22

Procesul decizional individual automatizat, inclusiv crearea de profiluri

(1) Persoana vizata are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automata, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizata sau o afecteaza in mod similar intr-o masura semnificativa.

(2) Alineatul (1) nu se aplica in cazul in care decizia:

(a) este necesara pentru incheierea sau executarea unui contract intre persoana vizata si un operator de date;

(b) este autorizata prin dreptul Uniunii sau dreptul intern care se aplica operatorului si care prevede, de asemenea, masuri corespunzatoare pentru protejarea drepturilor, libertatilor si intereselor legitime ale persoanei vizate; sau

(c) are la baza consimtamantul explicit al persoanei vizate.

(3) In cazurile mentionate la alineatul (2) literele (a) si (c), operatorul de date pune in aplicare masuri corespunzatoare pentru protejarea drepturilor, libertatilor si intereselor legitime ale persoanei vizate, cel putin dreptul acesteia de a obtine interventie umana din partea operatorului, de a-si exprima punctul de vedere si de a contesta decizia.

(4) Deciziile mentionate la alineatul (2) nu au la baza categoriile speciale de date cu caracter personal mentionate la articolul 9 alineatul (1), cu exceptia cazului in care se aplica articolul 9 alineatul (2) litera (a) sau (g) si in care au fost instituite masuri corespunzatoare pentru protejarea drepturilor, libertatilor si intereselor legitime ale persoanei vizate.

Sectiunea 5

Restrictii

Articolul 23

Restrictii

(1) Dreptul Uniunii sau dreptul intern care se aplica operatorului de date sau persoanei imputernicite de operator poate restrictiona printr-o masura legislativa domeniul de aplicare al obligatiilor si al drepturilor prevazute la articolele 12-22 si 34, precum si la articolul 5 in masura in care dispozitiile acestuia corespund drepturilor si obligatiilor prevazute la articolele 12-22, atunci cand o astfel de restrictie respecta esenta drepturilor si libertatilor fundamentale si constituie o masura necesara si proportionala intr-o societate democratica, pentru a asigura:

(a) securitatea nationala;

(b) apararea;

(c) securitatea publica;

(d) prevenirea, investigarea, depistarea sau urmarirea penala a infractiunilor sau executarea sanctiunilor penale, inclusiv protejarea impotriva amenintarilor la adresa securitatii publice si prevenirea acestora;

(e) alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, in special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv in domeniile monetar, bugetar si fiscal si in domeniul sanatatii publice si al securitatii sociale;

(f) protejarea independentei judiciare si a procedurilor judiciare;
(g) prevenirea, investigarea, depistarea si urmarirea penala a incalcarii eticii in cazul profesiilor reglementate;
(h) functia de monitorizare, inspectare sau reglementare legata, chiar si ocazional, de exercitarea autoritatii oficiale in cazurile mentionate la literele (a)-(e) si (g);
(i) protectia persoanei vizate sau a drepturilor si libertatilor altora;
(j) punerea in aplicare a pretentiilor de drept civil.
(2) In special, orice masura legislativa mentionata la alineatul (1) contine dispozitii specifice cel putin, daca este cazul, in ceea ce priveste:
(a) scopurile prelucrarii sau ale categoriilor de prelucrare;
(b) categoriile de date cu caracter personal;
(c) domeniul de aplicare al restrictiilor introduse;
(d) garantiile pentru a preveni abuzurile sau accesul sau transferul ilegal;
(e) mentionarea operatorului sau a categoriilor de operatori;
(f) perioadele de stocare si garantiile aplicabile avand in vedere natura, domeniul de aplicare si scopurile prelucrarii sau ale categoriilor de prelucrare;
(g) riscurile pentru drepturile si libertatilor persoanelor vizate; si
(h) dreptul persoanelor vizate de a fi informate cu privire la restrictie, cu exceptia cazului in care acest lucru poate aduce atingere scopului restrictiei.

CAPITOLUL IV
Operatorul si persoana imputernicita de operator

Sectiunea 1
Obligatii generale

Articolul 24
Responsabilitatea operatorului

(1) Tinand seama de natura, domeniul de aplicare, contextul si scopurile prelucrarii, precum si de riscurile cu grade diferite de probabilitate si gravitate pentru drepturile si libertatile persoanelor fizice, operatorul pune in aplicare masuri tehnice si organizatorice adecvate pentru a garanta si a fi in masura sa demonstreze ca prelucrarea se efectueaza in conformitate cu prezentul regulament. Respectivele masuri se revizuiesc si se actualizeaza daca este necesar.
(2) Atunci cand sunt proportionale in raport cu operatiunile de prelucrare, masurile mentionate la alineatul (1) includ punerea in aplicare de catre operator a unor politici adecvate de protectie a datelor.
(3) Aderarea la coduri de conduita aprobate, mentionate la articolul 40, sau la un mecanism de certificare aprobat, mentionat la articolul 42, poate fi utilizata ca element care sa demonstreze respectarea obligatiilor de catre operator.

Articolul 25
Asigurarea protectiei datelor incepand cu momentul conceperii si in mod implicit

(1) Avand in vedere stadiul actual al tehnologiei, costurile implementarii, si natura, domeniul de aplicare, contextul si scopurile prelucrarii, precum si riscurile cu grade diferite de probabilitate si gravitate pentru drepturile si libertatile persoanelor fizice pe care le prezinta prelucrarea, operatorul, atat in momentul stabilirii mijloacelor de prelucrare, cat si in cel al prelucrarii in sine, pune in aplicare masuri tehnice si organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate sa puna in aplicare in mod eficient principiile de protectie a datelor, precum reducerea la minimum a datelor, si sa integreze garantiile necesare in cadrul prelucrarii, pentru a indeplini cerintele prezentului regulament si a proteja drepturile persoanelor vizate.
(2) Operatorul pune in aplicare masuri tehnice si organizatorice adecvate pentru a asigura ca, in mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrarii. Respectiva obligatie se aplica volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare si accesibilitatii lor. In special, astfel de masuri asigura ca, in mod implicit, datele cu caracter personal nu pot fi accesate, fara interventia persoanei, de un numar nelimitat de persoane.

(3) Un mecanism de certificare aprobat in conformitate cu articolul 42 poate fi utilizat drept element care sa demonstreze indeplinirea cerintelor prevazute la alineatele (1) si (2) ale prezentului articol.

Articolul 26
Operatori asociati

(1) In cazul in care doi sau mai multi operatori stabilesc in comun scopurile si mijloacele de prelucrare, acestia sunt operatori asociati. Ei stabilesc intr-un mod transparent responsabilitatile fiecaruia in ceea ce priveste indeplinirea obligatiilor care le revin in temeiul prezentului regulament, in special in ceea ce priveste exercitarea drepturilor persoanelor vizate si indatoririle fiecaruia de furnizare a informatiilor prevazute la articolele 13 si 14, prin intermediul unui acord intre ei, cu exceptia cazului si in masura in care responsabilitatile operatorilor sunt stabilite in dreptul Uniunii sau in dreptul intern care se aplica acestora. Acordul poate sa desemneze un punct de contact pentru persoanele vizate.

(2) Acordul mentionat la alineatul (1) reflecta in mod adecvat rolurile si raporturile respective ale operatorilor asociati fata de persoanele vizate. Esenta acestui acord este facuta cunoscuta persoanei vizate.

(3) Indiferent de clauzele acordului mentionat la alineatul (1), persoana vizata isi poate exercita drepturile in temeiul prezentului regulament cu privire la si in raport cu fiecare dintre operatori.

Articolul 27
Reprezentantii operatorilor sau ai persoanelor imputernicite de operatori care nu isi au sediul in Uniune

(1) In cazul in care se aplica articolul 3 alineatul (2), operatorul sau persoana imputernicita de operator desemneaza in scris un reprezentant in Uniune.

(2) Obligatia prevazuta la alineatul (1) din prezentul articol nu se aplica:

(a) prelucrarii care are un caracter ocazional, care nu include, pe scara larga, prelucrarea unor categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau prelucrarea unor date cu caracter personal referitoare la condamnari penale si infractiuni mentionata la articolul 10, si care este putin susceptibila de a genera un risc pentru drepturile si libertatile persoanelor, tinand cont de natura, contextul, domeniul de aplicare si scopurile prelucrarii; sau

(b) unei autoritati sau unui organism public.

(3) Reprezentantul isi are sediul in unul dintre statele membre in care se afla persoanele vizate ale caror date cu caracter personal sunt prelucrate in legatura cu furnizarea de bunuri si servicii sau al caror comportament este monitorizat.

(4) Reprezentantul primeste din partea operatorului sau a persoanei imputernicite de operator un mandat prin care autoritatile de supraveghere si persoanele vizate, in special, se pot adresa reprezentantului, in plus fata de operator sau persoana imputernicita de operator sau in locul acestora, cu privire la toate chestiunile legate de prelucrarea, in scopul asigurarii respectarii prezentului regulament.

(5) Desemnarea unui reprezentant de catre operator sau persoana imputernicita de operator nu aduce atingere actiunilor in justitie care ar putea fi introduse impotriva operatorului sau persoanei imputernicite de operator insesi.

Articolul 28
Persoana imputernicita de operator

(1) In cazul in care prelucrarea urmeaza sa fie realizata in numele unui operator, operatorul recurge doar la persoane imputernicite care ofera garantii suficiente pentru punerea in aplicare a unor masuri tehnice si organizatorice adecvate, astfel incat prelucrarea sa respecte cerintele prevazute in prezentul regulament si sa asigure protectia drepturilor persoanei vizate.

(2) Persoana imputernicita de operator nu recruteaza o alta persoana imputernicita de operator fara a primi in prealabil o autorizatie scrisa, specifica sau generala, din partea operatorului. In cazul unei autorizatii generale scrise, persoana imputernicita de operator informeaza operatorul cu privire la orice modificari preconizate privind adaugarea sau inlocuirea altor persoane imputernicite de operator, oferind astfel posibilitatea operatorului de a formula obiectii fata de aceste modificari.

(3) Prelucrarea de catre o persoana imputernicita de un operator este reglementata printr-un contract sau alt act juridic in temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana imputernicita de operator in raport cu operatorul si care stabileste obiectul si durata prelucrarii, natura si scopul prelucrarii, tipul de date cu caracter personal si categoriile de persoane vizate si obligatiile si drepturile operatorului. Respectivul contract sau act juridic prevede in special ca persoana imputernicita de operator:

(a) prelucreaza datele cu caracter personal numai pe baza unor instructiuni documentate din partea operatorului, inclusiv in ceea ce priveste transferurile de date cu caracter personal catre o tara terta sau o organizatie internationala, cu exceptia cazului in care aceasta obligatie ii revine persoanei imputernicite in temeiul dreptului Uniunii sau al dreptului intern care i se aplica; in acest caz, notifica aceasta obligatie juridica operatorului inainte de prelucrare, cu exceptia cazului in care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

(b) se asigura ca persoanele autorizate sa prelucreze datele cu caracter personal s-au angajat sa respecte confidentialitatea sau au o obligatie statutara adecvata de confidentialitate;

(c) adopta toate masurile necesare in conformitate cu articolul 32;

(d) respecta conditiile mentionate la alineatele (2) si (4) privind recrutarea unei alte persoane imputernicite de operator;

(e) tinand seama de natura prelucrarii, ofera asistenta operatorului prin masuri tehnice si organizatorice adecvate, in masura in care acest lucru este posibil, pentru indeplinirea obligatiei operatorului de a raspunde cererilor privind exercitarea de catre persoana vizata a drepturilor prevazute in capitolul III;

(f) ajuta operatorul sa asigure respectarea obligatiilor prevazute la articolele 32-36, tinand seama de caracterul prelucrarii si informatiile aflate la dispozitia persoanei imputernicite de operator;

(g) la alegerea operatorului, sterge sau returneaza operatorului toate datele cu caracter personal dupa incetarea furnizarii serviciilor legate de prelucrare si elimina copiile existente, cu exceptia cazului in care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;

(h) pune la dispozitia operatorului toate informatiile necesare pentru a demonstra respectarea obligatiilor prevazute la prezentul articol, permite desfasurarea auditurilor, inclusiv a inspectiilor, efectuate de operator sau alt auditor mandatat si contribuie la acestea.

In ceea ce priveste primul paragraf litera (h), persoana imputernicita de operator informeaza imediat operatorul in cazul in care, in opinia sa, o instructiune incalca prezentul regulament sau alte dispozitii din dreptul intern sau din dreptul Uniunii referitoare la protectia datelor.

(4) In cazul in care o persoana imputernicita de un operator recruteaza o alta persoana imputernicita pentru efectuarea de activitati de prelucrare specifice in numele operatorului, aceleasi obligatii privind protectia datelor prevazute in contractul sau in alt act juridic incheiat intre operator si persoana imputernicita de operator, astfel cum se prevede la alineatul (3), revin celei de a doua persoane imputernicite, prin intermediul unui contract sau al unui alt act juridic, in temeiul dreptului Uniunii sau al dreptului intern, in special furnizarea de garantii suficiente pentru punerea in aplicare a unor masuri tehnice si organizatorice adecvate, astfel incat prelucrarea sa indeplineasca cerintele prezentului regulament. In cazul in care aceasta a doua persoana imputernicita nu isi respecta obligatiile privind protectia datelor, persoana imputernicita initiala ramane pe deplin raspunzatoare fata de operator in ceea ce priveste indeplinirea obligatiilor acestei a doua persoane imputernicite.

(5) Aderarea persoanei imputernicite de operator la un cod de conduita aprobat, mentionat la articolul 40, sau la un mecanism de certificare aprobat, mentionat la articolul 42, poate fi utilizata ca element prin care sa se demonstreze existenta garantiilor suficiente mentionate la alineatele (1) si (4) din prezentul articol.

(6) Fara a aduce atingere unui contract individual incheiat intre operator si persoana imputernicita de operator, contractul sau celalalt act juridic mentionat la alineatele (3) si (4) din prezentul articol se poate baza, integral sau partial, pe clauze contractuale standard mentionate la alineatele (7) si (8) din prezentul articol, inclusiv atunci cand fac parte dintr-o certificare acordata operatorului sau persoanei imputernicite de operator in temeiul articolelor 42 si 43.

(7) Comisia poate sa prevada clauze contractuale standard pentru aspectele mentionate la alineatele (3) si (4) din prezentul articol si in conformitate cu procedura de examinare mentionata la articolul 93 alineatul (2).

(8) O autoritate de supraveghere poate sa adopte clauze contractuale standard pentru aspectele mentionate la alineatele (3) si (4) din prezentul articol si in conformitate cu mecanismul pentru asigurarea coerentei mentionat la articolul 63.

(9) Contractul sau celalalt act juridic mentionat la alineatele (3) si (4) se formuleaza in scris, inclusiv in format electronic.

(10) Fara a aduce atingere articolelor 82, 83 si 84, in cazul in care o persoana imputernicita de operator incalca prezentul regulament, prin stabilirea scopurilor si mijloacelor de prelucrare a datelor cu caracter personal, persoana imputernicita de operator este considerata a fi un operator in ceea ce priveste prelucrarea respectiva.

Articolul 29
Desfasurarea activitatii de prelucrare sub autoritatea operatorului
sau a persoanei imputernicite de operator

Persoana imputernicita de operator si orice persoana care actioneaza sub autoritatea operatorului sau a persoanei imputernicite de operator care are acces la date cu caracter personal nu le prelucreaza decat la cererea operatorului, cu exceptia cazului in care dreptul Uniunii sau dreptul intern il obliga sa faca acest lucru.

Articolul 30
Evidentele activitatilor de prelucrare

(1) Fiecare operator si, dupa caz, reprezentantul acestuia pastreaza o evidenta a activitatilor de prelucrare desfasurate sub responsabilitatea lor. Respectiva evidenta cuprinde toate urmatoarele informatii:
(a) numele si datele de contact ale operatorului si, dupa caz, ale operatorului asociat, ale reprezentantului operatorului si ale responsabilului cu protectia datelor;
(b) scopurile prelucrarii;
(c) o descriere a categoriilor de persoane vizate si a categoriilor de date cu caracter personal;
(d) categoriile de destinatari carora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din tari terte sau organizatii internationale;
(e) daca este cazul, transferurile de date cu caracter personal catre o tara terta sau o organizatie internationala, inclusiv identificarea tarii terte sau a organizatiei internationale respective si, in cazul transferurilor mentionate la articolul 49 alineatul (1) al doilea paragraf, documentatia care dovedeste existenta unor garantii adecvate;
(f) acolo unde este posibil, termenele-limita preconizate pentru stergerea diferitelor categorii de date;
(g) acolo unde este posibil, o descriere generala a masurilor tehnice si organizatorice de securitate mentionate la articolul 32 alineatul (1).
(2) Fiecare operator si, dupa caz, persoana imputernicita de operator pastreaza o evidenta a tuturor categoriilor de activitati de prelucrare desfasurate in numele operatorului, care cuprind:
(a) numele si datele de contact ale persoanei sau persoanelor imputernicite de operator si ale fiecarui operator in numele caruia actioneaza aceasta persoana (aceste persoane), precum si ale reprezentantului operatorului sau al persoanei imputernicite de operator, dupa caz;
(b) categoriile de activitati de prelucrare desfasurate in numele fiecarui operator;
(c) daca este cazul, transferurile de date cu caracter personal catre o tara terta sau o organizatie internationala, inclusiv identificarea tarii terte sau a organizatiei internationale respective si, in cazul transferurilor prevazute la articolul 49 alineatul (1) al doilea paragraf, documentatia care dovedeste existenta unor garantii adecvate;
(d) acolo unde este posibil, o descriere generala a masurilor tehnice si organizatorice de securitate mentionate la articolul 32 alineatul (1).
(3) Evidentele mentionate la alineatele (1) si (2) se formuleaza in scris, inclusiv in format electronic.
(4) Operatorul sau persoana imputernicita de acesta, precum si, dupa caz, reprezentantul operatorului sau al persoanei imputernicite de operator pun evidentele la dispozitia autoritatii de supraveghere, la cererea acesteia.
(5) Obligatiile mentionate la alineatele 1 si 2 nu se aplica unei intreprinderi sau organizatii cu mai putin de 250 de angajati, cu exceptia cazului in care prelucrarea pe care o efectueaza este susceptibila sa genereze un risc pentru drepturile si libertatile persoanelor vizate, prelucrarea nu este ocazionala sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnari penale si infractiuni, astfel cum se mentioneaza la articolul 10.

Articolul 31
Cooperarea cu autoritatea de supraveghere

Operatorul si persoana imputernicita de operator si, dupa caz, reprezentantul acestora coopereaza, la cerere, cu autoritatea de supraveghere in indeplinirea sarcinilor lor.

Sectiunea 2
Securitatea datelor cu caracter personal

Articolul 32
Securitatea prelucrarii

(1) Avand in vedere stadiul actual al dezvoltarii, costurile implementarii si natura, domeniul de aplicare, contextul si scopurile prelucrarii, precum si riscul cu diferite grade de probabilitate si gravitate pentru drepturile si libertatile persoanelor fizice, operatorul si persoana imputernicita de acesta implementeaza masuri tehnice si organizatorice adecvate in vederea asigurarii unui nivel de securitate corespunzator acestui risc, incluzand printre altele, dupa caz:

(a) pseudonimizarea si criptarea datelor cu caracter personal;

(b) capacitatea de a asigura confidentialitatea, integritatea, disponibilitatea si rezistenta continue ale sistemelor si serviciilor de prelucrare;

(c) capacitatea de a restabili disponibilitatea datelor cu caracter personal si accesul la acestea in timp util in cazul in care are loc un incident de natura fizica sau tehnica;

(d) un proces pentru testarea, evaluarea si aprecierea periodice ale eficacitatii masurilor tehnice si organizatorice pentru a garanta securitatea prelucrarii.

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

(3) Aderarea la un cod de conduita aprobat, mentionat la articolul 40, sau la un mecanism de certificare aprobat, mentionat la articolul 42, poate fi utilizata ca element prin care sa se demonstreze indeplinirea cerintelor prevazute la alineatul (1) din prezentul articol.

(4) Operatorul si persoana imputernicita de acesta iau masuri pentru a asigura faptul ca orice persoana fizica care actioneaza sub autoritatea operatorului sau a persoanei imputernicite de operator si care are acces la date cu caracter personal nu le prelucreaza decat la cererea operatorului, cu exceptia cazului in care aceasta obligatie ii revine in temeiul dreptului Uniunii sau al dreptului intern.

Articolul 33
Notificarea autoritatii de supraveghere in cazul incalcarii securitatii datelor cu caracter personal

(1) In cazul in care are loc o incalcare a securitatii datelor cu caracter personal, operatorul notifica acest lucru autoritatii de supraveghere competente in temeiul articolului 55, fara intarzieri nejustificate si, daca este posibil, in termen de cel mult 72 de ore de la data la care a luat cunostinta de aceasta, cu exceptia cazului in care este susceptibila sa genereze un risc pentru drepturile si libertatile persoanelor fizice. In cazul in care notificarea nu are loc in termen de 72 de ore, aceasta este insotita de o explicatie motivata din partea autoritatii de supraveghere in cazul in care.

(2) Persoana imputernicita de operator instiinteaza operatorul fara intarzieri nejustificate dupa ce ia cunostinta de o incalcare a securitatii datelor cu caracter personal.

(3) Notificarea mentionata la alineatul (1) cel putin:

(a) descrie caracterul incalcarii securitatii datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile si numarul aproximativ al persoanelor vizate in cauza, precum si categoriile si numarul aproximativ al inregistrarilor de date cu caracter personal in cauza;

(b) comunica numele si datele de contact ale responsabilului cu protectia datelor sau un alt punct de contact de unde se pot obtine mai multe informatii;

(c) descrie consecintele probabile ale incalcarii securitatii datelor cu caracter personal;

(d) descrie masurile luate sau propuse spre a fi luate de operator pentru a remedia problema incalcarii securitatii datelor cu caracter personal, inclusiv, dupa caz, masurile pentru atenuarea eventualelor sale efecte negative.

(4) Atunci cand si in masura in care nu este posibil sa se furnizeze informatiile in acelasi timp, acestea pot fi furnizate in mai multe etape, fara intarzieri nejustificate.

(5) Operatorul pastreaza documente referitoare la toate cazurile de incalcare a securitatii datelor cu caracter personal, care cuprind o descriere a situatiei de fapt in care a avut loc incalcarea securitatii datelor cu caracter personal, a efectelor acesteia si a masurilor de remediere intreprinse. Aceasta documentatie permite autoritatii de supraveghere sa verifice conformitatea cu prezentul articol.

Articolul 34

Informarea persoanei vizate cu privire la incalcarea securitatii datelor cu caracter personal

(1) In cazul in care incalcarea securitatii datelor cu caracter personal este susceptibila sa genereze un risc ridicat pentru drepturile si libertatile persoanelor fizice, operatorul informeaza persoana vizata fara intarzieri nejustificate cu privire la aceasta incalcare.

(2) In informarea transmisa persoanei vizate prevazuta la alineatul (1) din prezentul articol se include o descriere intr-un limbaj clar si simplu a caracterului incalcarii securitatii datelor cu caracter personal, precum si cel putin informatiile si masurile mentionate la articolul 33 alineatul (3) literele (b), (c) si (d).

(3) Informarea persoanei vizate mentionata la alineatul (1) nu este necesara in cazul in care oricare dintre urmatoarele conditii este indeplinita:

(a) operatorul a implementat masuri de protectie tehnice si organizatorice adecvate, iar aceste masuri au fost aplicate in cazul datelor cu caracter personal afectate de incalcarea securitatii datelor cu caracter personal, in special masuri prin care se asigura ca datele cu caracter personal devin neinteligibile oricarei persoane care nu este autorizata sa le acceseze, cum ar fi criptarea;

(b) operatorul a luat masuri ulterioare prin care se asigura ca riscul ridicat pentru drepturile si libertatile persoanelor vizate mentionat la alineatul (1) nu mai este susceptibil sa se materializeze;

(c) ar necesita un efort disproportionat. In aceasta situatie, se efectueaza in loc o informare publica sau se ia o masura similara prin care persoanele vizate sunt informate intr-un mod la fel de eficace.

(4) In cazul in care operatorul nu a comunicat deja incalcarea securitatii datelor cu caracter personal catre persoana vizata, autoritatea de supraveghere, dupa ce a luat in considerare probabilitatea ca incalcarea securitatii datelor cu caracter personal sa genereze un risc ridicat, poate sa ii solicite acestuia sa faca acest lucru sau poate decide ca oricare dintre conditiile mentionate la alineatul (3) sunt indeplinite.

Sectiunea 3

Evaluarea impactului asupra protectiei datelor si consultarea prealabila

Articolul 35

Evaluarea impactului asupra protectiei datelor

(1) Avand in vedere natura, domeniul de aplicare, contextul si scopurile prelucrarii, in cazul in care un tip de prelucrare, in special cel bazat pe utilizarea noilor tehnologii, este susceptibil sa genereze un risc ridicat pentru drepturile si libertatile persoanelor fizice, operatorul efectueaza, inaintea prelucrarii, o evaluare a impactului operatiunilor de prelucrare prevazute asupra protectiei datelor cu caracter personal. O evaluare unica poate aborda un set de operatiuni de prelucrare similare care prezinta riscuri ridicate similare.

(2) La realizarea unei evaluari a impactului asupra protectiei datelor, operatorul solicita avizul responsabilului cu protectia datelor, daca acesta a fost desemnat.

(3) Evaluarea impactului asupra protectiei datelor mentionata la alineatul (1) se impune mai ales in cazul:

(a) unei evaluari sistematice si cuprinzatoare a aspectelor personale referitoare la persoane fizice, care se bazeaza pe prelucrarea automata, inclusiv crearea de profiluri, si care sta la baza unor decizii care produc efecte juridice privind persoana fizica sau care o afecteaza in mod similar intr-o masura semnificativa;

(b) prelucrarii pe scara larga a unor categorii speciale de date, mentionata la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnari penale si infractiuni, mentionata la articolul 10; sau

(c) unei monitorizari sistematice pe scara larga a unei zone accesibile publicului.

(4) Autoritatea de supraveghere intocmeste si publica o lista a tipurilor de operatiuni de prelucrare care fac obiectul cerintei de efectuare a unei evaluari a impactului asupra protectiei datelor, in conformitate cu alineatul (1). Autoritatea de supraveghere comunica aceste liste comitetului mentionat la articolul 68.

(5) Autoritatea de supraveghere poate, de asemenea, sa stabileasca si sa puna la dispozitia publicului o lista a tipurilor de operatiuni de prelucrare pentru care nu este necesara o evaluare a impactului asupra protectiei datelor. Autoritatea de supraveghere comunica aceste liste comitetului.

(6) Inainte de adoptarea listelor mentionate la alineatele (4) si (5), autoritatea de supraveghere competenta aplica mecanismul pentru asigurarea coerentei mentionat la articolul 63 in cazul in care aceste liste implica activitati de prelucrare care presupun furnizarea de bunuri sau prestarea de servicii catre persoane vizate sau monitorizarea comportamentului acestora in mai multe state membre ori care pot afecta in mod substantial libera circulatie a datelor cu caracter personal in cadrul Uniunii.

(7) Evaluarea contine cel putin:

(a) o descriere sistematica a operatiunilor de prelucrare preconizate si a scopurilor prelucrarii, inclusiv, dupa caz, interesul legitim urmarit de operator;

(b) o evaluare a necesitatii si proportionalitatii operatiunilor de prelucrare in legatura cu aceste scopuri;

(c) o evaluare a riscurilor pentru drepturile si libertatile persoanelor vizate mentionate la alineatul (1); si

(d) masurile preconizate in vederea abordarii riscurilor, inclusiv garantiile, masurile de securitate si mecanismele menite sa asigure protectia datelor cu caracter personal si sa demonstreze conformitatea cu dispozitiile prezentului regulament, luand in considerare drepturile si interesele legitime ale persoanelor vizate si ale altor persoane interesate.

(8) La evaluarea impactului operatiunilor de prelucrare efectuate de operatorii sau de persoanele imputernicite de operatori relevante, se are in vedere in mod corespunzator respectarea de catre operatorii sau persoanele imputernicite respective a codurilor de conduita aprobate mentionate la articolul 40, in special in vederea unei evaluari a impactului asupra protectiei datelor.

(9) Operatorul solicita, acolo unde este cazul, avizul persoanelor vizate sau al reprezentantilor acestora privind prelucrarea prevazuta, fara a aduce atingere protectiei intereselor comerciale sau publice ori securitatii operatiunilor de prelucrare.

(10) Atunci cand prelucrarea in temeiul articolului 6 alineatul (1) litera (c) sau (e) are un temei juridic in dreptul Uniunii sau al unui stat membru sub incidenta caruia intra operatorul, iar dreptul respectiv reglementeaza operatiunea de prelucrare specifica sau setul de operatiuni specifice in cauza si deja s-a efectuat o evaluare a impactului asupra protectiei datelor ca parte a unei evaluari a impactului generale in contextul adoptarii respectivului temei juridic, alineatele (1)-(7) nu se aplica, cu exceptia cazului in care statele membre considera ca este necesara efectuarea unei astfel de evaluari inaintea desfasurarii activitatilor de prelucrare.

(11) Acolo unde este necesar, operatorul efectueaza o analiza pentru a evalua daca prelucrarea are loc in conformitate cu evaluarea impactului asupra protectiei datelor, cel putin atunci cand are loc o modificare a riscului reprezentat de operatiunile de prelucrare.

Articolul 36
Consultarea prealabila

(1) Operatorul consulta autoritatea de supraveghere inainte de prelucrarea atunci cand evaluarea impactului asupra protectiei datelor prevazuta la articolul 35 indica faptul ca prelucrarea ar genera un risc ridicat in absenta unor masuri luate de operator pentru atenuarea riscului.

(2) Atunci cand considera ca prelucrarea prevazuta mentionata la alineatul (1) ar incalca prezentul regulament, in special atunci cand riscul nu a fost identificat sau atenuat intr-o masura suficienta de catre operator, autoritatea de supraveghere ofera consiliere in scris operatorului si, dupa caz, persoanei imputernicite de operator, in cel mult opt saptamani de la primirea cererii de consultare, si isi poate utiliza oricare dintre competentele mentionate la articolul 58. Aceasta perioada poate fi prelungita cu sase saptamani, tinandu-se seama de complexitatea prelucrarii prevazute. Autoritatea de supraveghere informeaza operatorul si, dupa caz, persoana imputernicita de operator, in termen de o luna de la primirea cererii, cu privire la orice astfel de prelungire, prezentand motivele intarzierii. Aceste perioade pot fi suspendate pana cand autoritatea de supraveghere a obtinut informatiile pe care le-a solicitat in scopul consultarii.

(3) Atunci cand consulta autoritatea de supraveghere in conformitate cu alineatul (1), operatorul ii furnizeaza acesteia:

(a) daca este cazul, responsabilitatile respective ale operatorului, ale operatorilor asociati si ale persoanelor imputernicite de operator implicate in activitatile de prelucrare, in special pentru prelucrarea in cadrul unui grup de intreprinderi;

(b) scopurile si mijloacele prelucrarii preconizate;

(c) masurile si garantiile prevazute pentru protectia drepturilor si libertatilor persoanelor vizate, in conformitate cu prezentul regulament;

(d) daca este cazul, datele de contact ale responsabilului cu protectia datelor;

(e) evaluarea impactului asupra protectiei datelor prevazuta la articolul 35; si

(f) orice alte informatii solicitate de autoritatea de supraveghere.

(4) Statele membre consulta autoritatea de supraveghere in cadrul procesului de pregatire a unei propuneri de masura legislativa care urmeaza sa fie adoptata de un parlament national sau a unei masuri de reglementare intemeiate pe o astfel de masura legislativa, care se refera la prelucrarea.

(5) In pofida alineatului (1), dreptul intern poate impune operatorilor sa se consulte cu autoritatea de supraveghere si sa obtina in prealabil autorizarea din partea acesteia in legatura cu prelucrarea de catre un operator in vederea indeplinirii unei sarcini exercitate de acesta in interes public, inclusiv prelucrarea in legatura cu protectia sociala si sanatatea publica.

Sectiunea 4
Responsabilul cu protectia datelor

Articolul 37
Desemnarea responsabilului cu protectia datelor

(1) Operatorul si persoana imputernicita de operator desemneaza un responsabil cu protectia datelor ori de cate ori:

(a) prelucrarea este efectuata de o autoritate sau un organism public, cu exceptia instantelor care actioneaza in exercitiul functiei lor jurisdictionale;

(b) activitatile principale ale operatorului sau ale persoanei imputernicite de operator constau in operatiuni de prelucrare care, prin natura, domeniul de aplicare si/sau scopurile lor, necesita o monitorizare periodica si sistematica a persoanelor vizate pe scara larga; sau

(c) activitatile principale ale operatorului sau ale persoanei imputernicite de operator constau in prelucrarea pe scara larga a unor categorii speciale de date, mentionata la articolul 9, sau a unor date cu caracter personal privind condamnari penale si infractiuni, mentionata la articolul 10.

(2) Un grup de intreprinderi poate numi un responsabil cu protectia datelor unic, cu conditia ca responsabilul cu protectia datelor sa fie usor accesibil din fiecare intreprindere.

(3) In cazul in care operatorul sau persoana imputernicita de operator este o autoritate publica sau un organism public, poate fi desemnat un responsabil cu protectia datelor unic pentru mai multe dintre aceste autoritati sau organisme, luand in considerare structura organizatorica si dimensiunea acestora.

(4) In alte cazuri decat cele mentionate la alineatul (1), operatorul sau persoana imputernicita de operator ori asociatiile si alte organisme care reprezinta categorii de operatori sau de persoane imputernicite de operatori pot desemna sau, acolo unde dreptul Uniunii sau dreptul intern solicita acest lucru, desemneaza un responsabil cu protectia datelor. Responsabilul cu protectia datelor poate sa actioneze in favoarea unor astfel de asociatii si alte organisme care reprezinta operatori sau persoane imputernicite de operatori.

(5) Responsabilul cu protectia datelor este desemnat pe baza calitatilor profesionale si, in special, a cunostintelor de specialitate in dreptul si practicile din domeniul protectiei datelor, precum si pe baza capacitatii de a indeplini sarcinile prevazute la articolul 39.

(6) Responsabilul cu protectia datelor poate fi un membru al personalului operatorului sau persoanei imputernicite de operator sau poate sa isi indeplineasca sarcinile in baza unui contract de servicii.

(7) Operatorul sau persoana imputernicita de operator publica datele de contact ale responsabilului cu protectia datelor si le comunica autoritatii de supraveghere.

Articolul 38
Functia responsabilului cu protectia datelor

(1) Operatorul si persoana imputernicita de operator se asigura ca responsabilul cu protectia datelor este implicat in mod corespunzator si in timp util in toate aspectele legate de protectia datelor cu caracter personal.

(2) Operatorul si persoana imputernicita de operator sprijina responsabilul cu protectia datelor in indeplinirea sarcinilor mentionate la articolul 39, asigurandu-i resursele necesare pentru executarea acestor sarcini, precum

si accesarea datelor cu caracter personal si a operatiunilor de prelucrare, si pentru mentinerea cunostintelor sale de specialitate.

(3) Operatorul si persoana imputernicita de operator se asigura ca responsabilul cu protectia datelor nu primeste niciun fel de instructiuni in ceea ce priveste indeplinirea acestor sarcini. Acesta nu este demis sau sanctionat de catre operator sau de persoana imputernicita de operator pentru indeplinirea sarcinilor sale. Responsabilul cu protectia datelor raspunde direct in fata celui mai inalt nivel al conducerii operatorului sau persoanei imputernicite de operator.

(4) Persoanele vizate pot contacta responsabilul cu protectia datelor cu privire la toate chestiunile legate de prelucrarea datelor lor si la exercitarea drepturilor lor in temeiul prezentului regulament.

(5) Responsabilul cu protectia datelor are obligatia de a respecta secretul sau confidentialitatea in ceea ce priveste indeplinirea sarcinilor sale, in conformitate cu dreptul Uniunii sau cu dreptul intern.

(6) Responsabilul cu protectia datelor poate indeplini si alte sarcini si atributii. Operatorul sau persoana imputernicita de operator se asigura ca niciuna dintre aceste sarcini si atributii nu genereaza un conflict de interese.

Articolul 39

Sarcinile responsabilului cu protectia datelor

(1) Responsabilul cu protectia datelor are cel putin urmatoarele sarcini:

(a) informarea si consilierea operatorului, sau a persoanei imputernicite de operator, precum si a angajatilor care se ocupa de prelucrare cu privire la obligatiile care le revin in temeiul prezentului regulament si al altor dispozitii de drept al Uniunii sau drept intern referitoare la protectia datelor;

(b) monitorizarea respectarii prezentului regulament, a altor dispozitii de drept al Uniunii sau de drept intern referitoare la protectia datelor si a politicilor operatorului sau ale persoanei imputernicite de operator in ceea ce priveste protectia datelor cu caracter personal, inclusiv alocarea responsabilitatilor si actiunile de sensibilizare si de formare a personalului implicat in operatiunile de prelucrare, precum si auditurile aferente;

(c) furnizarea de consiliere la cerere in ceea ce priveste evaluarea impactului asupra protectiei datelor si monitorizarea functionarii acesteia, in 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 prealabila mentionata la articolul 36, precum si, daca este cazul, consultarea cu privire la orice alta chestiune.

(2) In indeplinirea sarcinilor sale, responsabilul cu protectia datelor tine seama in mod corespunzator de riscul asociat operatiunilor de prelucrare, luand in considerare natura, domeniul de aplicare, contextul si scopurile prelucrarii.

Sectiunea 5

Coduri de conduita si certificare

Articolul 40

Coduri de conduita

(1) Statele membre, autoritatile de supraveghere, comitetul si Comisia incurajeaza elaborarea de coduri de conduita menite sa contribuie la buna aplicare a prezentului regulament, tinand seama de caracteristicile specifice ale diverselor sectoare de prelucrare si de nevoile specifice ale microintreprinderilor si ale intreprinderilor mici si mijlocii.

(2) Asociatiile si alte organisme care reprezinta categorii de operatori sau de persoane imputernicite de operatori pot pregati coduri de conduita sau le pot modifica sau extinde pe cele existente, in scopul de a specifica modul de aplicare a prezentului regulament, cum ar fi in ceea ce priveste:

(a) prelucrarea in mod echitabil si transparent;

(b) interesele legitime urmarite de operatori in contexte specifice;

(c) colectarea datelor cu caracter personal;

(d) pseudonimizarea datelor cu caracter personal;

(e) informarea publicului si a persoanelor vizate;

(f) exercitarea drepturilor persoanelor vizate;

(g) informarea si protejarea copiilor si modalitatea in care trebuie obtinut consimtamantul titularilor raspunderii parintesti asupra copiilor;

(h) masurile si procedurile mentionate la articolele 24 si 25 si masurile de asigurare a securitatii prelucrarii, mentionate la articolul 32;

(i) notificarea autoritatilor de supraveghere cu privire la incalcarile securitatii datelor cu caracter personal si informarea persoanelor vizate cu privire la aceste incalcari;

(j) transferul de date cu caracter personal catre tari terte sau organizatii internationale; sau

(k) proceduri extrajudiciare si alte proceduri de solutionare a litigiilor pentru solutionarea litigiilor intre operatori si persoanele vizate in ceea ce priveste prelucrarea, fara a aduce atingere drepturilor persoanelor vizate, in temeiul articolelor 77 si 79.

(3) La codurile de conduita aprobate in temeiul alineatului (5) din prezentul articol si care au o valabilitate generala in temeiul alineatului (9) din prezentul articol pot adera nu numai operatorii sau persoanele imputernicite de operatori care fac obiectul prezentului regulament, ci si operatorii sau persoanele imputernicite de operatori care nu fac obiectul prezentului regulament in temeiul articolului 3, in scopul de a oferi garantii adecvate in cadrul transferurilor de date cu caracter personal catre tari terte sau organizatii internationale in conditiile mentionate la articolul 46 alineatul (2) litera (e). Acesti operatori sau persoane imputernicite de operatori isi asuma angajamente cu caracter obligatoriu si executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, in scopul aplicarii garantiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.

(4) Codul de conduita prevazut la alineatul (2) din prezentul articol cuprinde mecanisme care permit organismului mentionat la articolul 41 alineatul (1) sa efectueze monitorizarea obligatorie a respectarii dispozitiilor acestuia de catre operatorii sau persoanele imputernicite de operatori care se angajeaza sa il aplice, fara a aduce atingere sarcinilor si competentelor autoritatilor de supraveghere care sunt competente in temeiul articolului 55 sau 56.

(5) Asociatiile si alte organisme mentionate la alineatul (2) din prezentul articol care intentioneaza sa pregateasca un cod de conduita sau sa modifice sau sa extinda un cod existent transmit proiectul de cod, de modificare sau de extindere autoritatii de supraveghere care este competenta in 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 si il aproba in cazul in care se constata ca acesta ofera garantii adecvate suficiente.

(6) In cazul in care proiectul de cod, de modificare sau de extindere este aprobat in conformitate cu alineatul (5), iar codul de conduita in cauza nu are legatura cu activitatile de prelucrare din mai multe state membre, autoritatea de supraveghere inregistreaza si publica codul.

(7) In cazul in care un proiect de cod de conduita, de modificare sau de extindere are legatura cu activitatile de prelucrare din mai multe state membre, inainte de aprobare, autoritatea de supraveghere competenta in temeiul articolului 55 il transmite, prin procedura mentionata la articolul 63, comitetului, care emite un aviz cu privire la conformitatea cu prezentul regulament a proiectului respectiv, sau, in situatia mentionata la alineatul (3) din prezentul articol, ofera garantii adecvate.

(8) In cazul in care avizul mentionat la alineatul (7) confirma conformitatea cu prezentul regulament a proiectului de cod, de modificare sau de extindere sau in cazul in care, in situatia mentionata la alineatul (3), ofera garantii adecvate, comitetul transmite avizul sau Comisiei.

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

(10) Comisia asigura publicitatea adecvata pentru codurile aprobate asupra carora s-a decis ca au valabilitate generala in conformitate cu alineatul (9).

(11) Comitetul regrupeaza toate codurile de conduita, modificarile si extinderile aprobate intr-un registru si le pune la dispozitia publicului prin mijloace corespunzatoare.

Articolul 41

Monitorizarea codurilor de conduita aprobate

(1) Fara a aduce atingere sarcinilor si competentelor autoritatii de supraveghere competente in temeiul articolelor 57 si 58, monitorizarea respectarii unui cod de conduita in temeiul articolului 40 poate fi realizata de

un organism care dispune de un nivel adecvat de expertiza in legatura cu obiectul codului si care este acreditat in acest scop de autoritatea de supraveghere competenta.

(2) Un organism mentionat la alineatul (1) poate fi acreditat pentru monitorizarea respectarii unui cod de conduita daca:

(a) a demonstrat autoritatii de supraveghere competente, intr-un mod satisfacator, independenta si expertiza sa in legatura cu obiectul codului;

(b) a instituit proceduri care ii permit sa evalueze eligibilitatea operatorilor si a persoanelor imputernicite de operatori in vederea aplicarii codului, sa monitorizeze respectarea de catre acestia a dispozitiilor codului si sa revizuiasca periodic functionarea acestuia;

(c) a instituit proceduri si structuri pentru tratarea plangerilor privind incalcari ale codului sau privind modul in care codul a fost sau este pus in aplicare de un operator sau o persoana imputernicita de operator, precum si pentru asigurarea transparentei acestor proceduri si structuri pentru persoanele vizate si pentru public; si

(d) a demonstrat autoritatii de supraveghere competente, intr-un mod satisfacator, ca sarcinile si atributiile sale nu creeaza conflicte de interese.

(3) Autoritatea de supraveghere competenta transmite proiectul de criterii pentru acreditarea unui organism mentionat la alineatul (1) din prezentul articol comitetului, in conformitate cu mecanismul pentru asigurarea coerentei mentionat la articolul 63.

(4) Fara a aduce atingere sarcinilor si competentelor autoritatii de supraveghere competente si dispozitiilor capitolului VIII, un organism mentionat la alineatul (1) din prezentul articol ia masuri corespunzatoare, sub rezerva unor garantii adecvate, in cazul incalcarii codului de catre un operator sau o persoana imputernicita de operator, inclusiv prin suspendarea sau excluderea respectivului operator sau a respectivei persoane din cadrul codului. Organismul in cauza informeaza autoritatea de supraveghere competenta cu privire la aceste masuri si la motivele care le-au determinat.

(5) Autoritatea de supraveghere competenta revoca acreditarea unui organism mentionat la alineatul (1) in cazul in care nu mai sunt indeplinite conditiile pentru acreditare sau masurile luate de organismul in cauza incalca prezentul regulament.

(6) Prezentul articol nu se aplica prelucrarii efectuate de autoritati si organisme publice.

Articolul 42
Certificare

(1) Statele membre, autoritatile de supraveghere, comitetul si Comisia incurajeaza, in special la nivelul Uniunii, instituirea de mecanisme de certificare in domeniul protectiei datelor, precum si de sigilii si marci in acest domeniu, care sa permita demonstrarea faptului ca operatiunile de prelucrare efectuate de operatori si de persoanele imputernicite de operatori respecta prezentul regulament. Sunt luate in considerare necesitatile specifice ale microintreprinderilor si ale intreprinderilor mici si mijlocii.

(2) Mecanismele de certificare din domeniul protectiei datelor, sigiliile sau marcile aprobate in temeiul alineatului (5) din prezentul articol sunt instituite nu numai pentru a fi respectate de operatorii sau de persoanele imputernicite de operatori care fac obiectul prezentului regulament, ci si pentru a demonstra existenta unor garantii adecvate oferite de operatorii sau de persoanele imputernicite de operatori care nu fac obiectul prezentului regulament, in temeiul articolului 3, in cadrul transferurilor de date cu caracter personal catre tari terte sau organizatii internationale in conditiile mentionate la articolul 46 alineatul (2) litera (f). Acesti operatori sau persoane imputernicite de operatori isi asuma angajamente cu caracter obligatoriu si executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, in scopul aplicarii garantiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.

(3) Certificarea este voluntara si disponibila prin intermediul unui proces transparent.

(4) Certificarea in conformitate cu prezentul articol nu reduce responsabilitatea operatorului sau a persoanei imputernicite de operator de a respecta prezentul regulament si nu aduce atingere sarcinilor si competentelor autoritatilor de supraveghere care sunt competente in temeiul articolului 55 sau 56.

(5) Organismele de certificare mentionate la articolul 43 sau autoritatea de supraveghere competenta emit o certificare in temeiul prezentului articol, pe baza criteriilor aprobate de catre autoritatea de supraveghere competenta respectiva in temeiul articolului 58 alineatul (3), sau de catre comitet in temeiul articolului 63. In cazul in care criteriile sunt aprobate de comitet, aceasta poate duce la o certificare comuna, si anume sigiliul european privind protectia datelor.

(6) Operatorul sau persoana imputernicita de operator care supune activitatile sale de prelucrare mecanismului de certificare ofera organismului de certificare mentionat la articolul 43 sau, dupa caz, autoritatii de supraveghere competente, toate informatiile necesare pentru desfasurarea procedurii de certificare, precum si accesul la activitatile de prelucrare respective.

(7) Certificarea este eliberata unui operator sau unei persoane imputernicite de operator pentru o perioada maxima de trei ani si poate fi reinnoita in aceleasi conditii, cu conditia ca cerintele relevante sa fie indeplinite in continuare. Certificarea este retrasa, dupa caz, de catre organismele de certificare mentionate la articolul 43 sau de catre autoritatea de supraveghere competenta in cazul in care nu mai sunt indeplinite cerintele pentru certificare.

(8) Comitetul regrupeaza toate mecanismele de certificare si sigiliile si marcile de protectie a datelor intr-un registru si le pune la dispozitia publicului prin orice mijloc corespunzator.

Articolul 43

Organisme de certificare

(1) Fara a aduce atingere sarcinilor si competentelor autoritatii de supraveghere competente, prevazute la articolele 57 si 58, organismele de certificare care dispun de un nivel adecvat de competenta in domeniul protectiei datelor, dupa ce informeaza autoritatea de supraveghere pentru a-i permite sa isi exercite competentele in temeiul articolului 58 alineatul (2) litera (h), emit si reinnoiesc certificarea. Statele membre se asigura ca aceste organisme de certificare sunt acreditate de catre una sau amandoua dintre urmatoarele entitati:

(a) autoritatea de supraveghere care este competenta in temeiul articolului 55 sau 56;

(b) organismul national de acreditare desemnat in conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European si al Consiliului in conformitate cu standardul EN-ISO/IEC 17065/2012 si cu cerintele suplimentare stabilite de autoritatea de supraveghere care este competenta in temeiul articolului 55 sau 56.

(2) Un organism de certificare mentionat la alineatul (1) este acreditat in conformitate cu alineatul respectiv numai daca:

(a) a demonstrat autoritatii de supraveghere competente, intr-un mod satisfacator, independenta si expertiza sa in legatura cu obiectul certificarii;

(b) s-a angajat sa respecte criteriile mentionate la articolul 42 alineatul (5) si aprobate de autoritatea de supraveghere care este competenta in temeiul articolului 55 sau 56, sau de catre comitet in temeiul articolului 63;

(c) a instituit proceduri pentru emiterea, revizuirea periodica si retragerea certificarii, a sigiliilor si marcilor din domeniul protectiei datelor;

(d) a instituit proceduri si structuri pentru tratarea plangerilor privind incalcari ale certificarii sau privind modul in care certificarea a fost sau este pusa in aplicare de un operator sau o persoana imputernicita de operator, precum si pentru asigurarea transparentei acestor proceduri si structuri pentru persoanele vizate si pentru public; si

(e) a demonstrat autoritatii de supraveghere competente, intr-un mod satisfacator, ca sarcinile si atributiile sale nu creeaza conflicte de interese.

(3) Acreditarea organismelor de certificare mentionate la alineatele (1) si (2) din prezentul articol se realizeaza pe baza criteriilor aprobate de catre autoritatea de supraveghere care este competenta in temeiul articolului 55 sau 56, sau de catre comitet in temeiul articolului 63. In cazul unei acreditari in conformitate cu alineatul (1) litera (b) din prezentul articol, aceste cerinte le completeaza pe cele prevazute in Regulamentul (CE) nr. 765/2008 si normele tehnice care descriu metodele si procedurile organismelor de certificare.

(4) Organismele de certificare mentionate la alineatul (1) sunt responsabile cu realizarea unei evaluari adecvate in vederea certificarii sau retragerii acestei certificari, fara a aduce atingere responsabilitatii operatorului sau a persoanei imputernicite de operator de a respecta prezentul regulament. Acreditarea se elibereaza pentru o perioada maxima de cinci ani si poate fi reinnoita in aceleasi conditii, cu conditia ca organismul de certificare sa indeplineasca cerintele prevazute in prezentul articol.

(5) Organismele de certificare mentionate la alineatul (1) transmite autoritatilor de supraveghere competente motivele acordarii sau retragerii certificarii solicitate.

(6) Cerintele mentionate la alineatul (3) din prezentul articol si criteriile mentionate la articolul 42 alineatul (5) se publica de catre autoritatea de supraveghere intr-o forma usor de accesat. Autoritatile de supraveghere transmit, de asemenea, aceste cerinte si criterii comitetului. Comitetul regrupeaza toate mecanismele de

certificare si sigiliile de protectie a datelor intr-un registru si le pune la dispozitia publicului prin orice mijloc corespunzator.

(7) Fara a aduce atingere dispozitiilor capitolului VIII, autoritatea de supraveghere competenta sau organismul national de acreditare revoca acreditarea acordata unui organism de certificare in temeiul alineatului (1) din prezentul articol in cazul in care nu sunt sau nu mai sunt indeplinite conditiile pentru acreditare sau masurile luate de organismul de acreditare incalca prezentul regulament.

(8) Comisia este imputernicita sa adopte acte delegate in conformitate cu articolul 92, in scopul specificarii cerintelor care trebuie luate in considerare pentru mecanismele de certificare din domeniul protectiei datelor, mentionate la articolul 42 alineatul (1).

(9) Comisia poate adopta acte de punere in aplicare pentru a stabili standarde tehnice pentru mecanismele de certificare si pentru sigiliile si marcile din domeniul protectiei datelor, precum si mecanisme de promovare si recunoastere a acelor mecanisme de certificare, sigilii si marci. Actele de punere in aplicare respective se adopta in conformitate cu procedura de examinare mentionata la articolul 93 alineatul (2).

CAPITOLUL V
Transferurile de date cu caracter personal catre tari terte sau organizatii internationale

Articolul 44
Principiul general al transferurilor

Orice date cu caracter personal care fac obiectul prelucrarii sau care urmeaza a fi prelucrate dupa ce sunt transferate intr-o tara terta sau catre o organizatie internationala pot fi transferate doar daca, sub rezerva celorlalte dispozitii ale prezentului regulament, conditiile prevazute in prezentul capitol sunt respectate de operator si de persoana imputernicita de operator, inclusiv in ceea ce priveste transferurile ulterioare de date cu caracter personal din tara terta sau de la organizatia internationala catre o alta tara terta sau catre o alta organizatie internationala. Toate dispozitiile din prezentul capitol se aplica pentru a se asigura ca nivelul de protectie a persoanelor fizice garantat prin prezentul regulament nu este subminat.

Articolul 45
Transferuri in temeiul unei decizii privind caracterul adecvat al nivelului de protectie

(1) Transferul de date cu caracter personal catre o tara terta sau o organizatie internationala se poate realiza atunci cand Comisia a decis ca tara terta, un teritoriu ori unul sau mai multe sectoare specificate din acea tara terta sau organizatia internationala in cauza asigura un nivel de protectie adecvat. Transferurile realizate in aceste conditii nu necesita autorizari speciale.

(2) Atunci cand evalueaza caracterul adecvat al nivelului de protectie, Comisia tine seama, in special, de urmatoarele elemente:

(a) statul de drept, respectarea drepturilor omului si a libertatilor fundamentale, legislatia relevanta, atat generala, cat si sectoriala, inclusiv privind securitatea publica, apararea, securitatea nationala si dreptul penal, precum si accesul autoritatilor publice la datele cu caracter personal, precum si punerea in aplicare a acestei legislatii, normele de protectie a datelor, normele profesionale si masurile de securitate, inclusiv normele privind transferul ulterior de date cu caracter personal catre o alta tara terta sau organizatie internationala, care sunt respectate in tara terta respectiva sau in organizatia internationala respectiva, jurisprudenta, precum si existenta unor drepturi efective si opozabile ale persoanelor vizate si a unor reparatii efective pe cale administrativa si judiciara pentru persoanele vizate ale caror date cu caracter personal sunt transferate;

(b) existenta si functionarea eficienta a uneia sau mai multor autoritati de supraveghere independente in tara terta sau sub jurisdictia carora intra o organizatie internationala, cu responsabilitate pentru asigurarea si impunerea respectarii normelor de protectie a datelor, incluzand competente adecvate de asigurare a respectarii aplicarii, pentru acordarea de asistenta si consiliere persoanelor vizate cu privire la exercitarea drepturilor acestora si pentru cooperarea cu autoritatile de supraveghere din statele membre; si

(c) angajamentele internationale la care a aderat tara terta sau organizatia internationala in cauza sau alte obligatii care decurg din conventii sau instrumente obligatorii din punct de vedere juridic, precum si din

participarea acesteia la sisteme multilaterale sau regionale, mai ales in domeniul protectiei datelor cu caracter personal.

(3) Comisia, dupa ce evalueaza caracterul adecvat al nivelului de protectie, poate decide, printr-un act de punere in aplicare, ca o tara terta, un teritoriu sau unul sau mai multe sectoare specificate dintr-o tara terta sau o organizatie internationala asigura un nivel de protectie adecvat in sensul alineatului (2) din prezentul articol. Actul de punere in aplicare prevede un mecanism de revizuire periodica, cel putin o data la patru ani, care ia in considerare toate evolutiile relevante din tara terta sau organizatia internationala. Actul de punere in aplicare mentioneaza aplicarea geografica si sectoriala, si, dupa caz, identifica autoritatea sau autoritatile de supraveghere mentionate la alineatul (2) litera (b) din prezentul articol. Actul de punere in aplicare se adopta in conformitate cu procedura de examinare mentionata la articolul 93 alineatul (2).

(4) Comisia monitorizeaza continuu evolutiile din tarile terte si de la nivelul organizatiilor internationale care ar putea afecta functionarea deciziilor adoptate in temeiul alineatului (3) din prezentul articol si a deciziilor adoptate in temeiul articolului 25 alineatul (6) din Directiva 95/46/CE.

(5) In cazul in care informatiile disponibile dezvaluie, in special in urma revizuirii mentionate la alineatul (3) din prezentul articol, ca o tara terta, un teritoriu sau un sector specificat din acea tara terta sau o organizatie internationala nu mai asigura un nivel de protectie adecvat in sensul alineatului (2) din prezentul articol, Comisia, daca este necesar, abroga, modifica sau suspenda, prin intermediul unui act de punere in aplicare, decizia mentionata la alineatul (3) din prezentul articol fara efect retroactiv. Actele de punere in aplicare respective se adopta in conformitate cu procedura de examinare mentionata la articolul 93 alineatul (2).

Din motive imperioase de urgenta, Comisia adopta acte de punere in aplicare imediat aplicabile in conformitate cu procedura mentionata la articolul 93 alineatul (3).

(6) Comisia initiaza consultari cu tara terta sau organizatia internationala in vederea remedierii situatiei care a stat la baza deciziei luate in conformitate cu alineatul (5).

(7) O decizie luata in temeiul alineatului (5) din prezentul articol nu aduce atingere transferurilor de date cu caracter personal catre tara terta, un teritoriu sau unul sau mai multe sectoare specificate din acea tara terta sau catre organizatia internationala in cauza in conformitate cu articolele 46-49.

(8) Comisia publica in Jurnalul Oficial al Uniunii Europene si pe site-ul sau o lista a tarilor terte, a teritoriilor si sectoarelor specificate dintr-o tara terta si a organizatiilor internationale in cazul carora a decis ca nivelul de protectie adecvat este asigurat sau nu mai este asigurat.

(9) Deciziile adoptate de Comisie in temeiul articolului 25 alineatul (6) din Directiva 95/46/CE raman in vigoare pana cand sunt modificate, inlocuite sau abrogate de o decizie a Comisiei adoptata in conformitate cu alineatul (3) sau (5) din prezentul articol.

Articolul 46

Transferuri in baza unor garantii adecvate

(1) In absenta unei decizii in temeiul articolului 45 alineatul (3), operatorul sau persoana imputernicita de operator poate transfera date cu caracter personal catre o tara terta sau o organizatie internationala numai daca operatorul sau persoana imputernicita de operator a oferit garantii adecvate si cu conditia sa existe drepturi opozabile si cai de atac eficiente pentru persoanele vizate.

(2) Garantiile adecvate mentionate la alineatul 1 pot fi furnizate fara sa fie nevoie de nicio autorizatie specifica din partea unei autoritati de supraveghere, prin:

(a) un instrument obligatoriu din punct de vedere juridic si executoriu intre autoritatile sau organismele publice;

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

(c) clauze standard de protectie a datelor adoptate de Comisie in conformitate cu procedura de examinare mentionata la articolul 93 alineatul (2);

(d) clauze standard de protectie a datelor adoptate de o autoritate de supraveghere si aprobate de Comisie in conformitate cu procedura de examinare mentionata la articolul 93 alineatul (2);

(e) un cod de conduita aprobat in conformitate cu articolul 40, insotit de un angajament obligatoriu si executoriu din partea operatorului sau a persoanei imputernicite de operator din tara terta de a aplica garantii adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

(f) un mecanism de certificare aprobat in conformitate cu articolul 42, insotit de un angajament obligatoriu si executoriu din partea operatorului sau a persoanei imputernicite de operator din tara terta de a aplica garantii adecvate, inclusiv cu privire la drepturile persoanelor vizate.

(3) Sub rezerva autorizarii din partea autoritatii de supraveghere competente, garantiile adecvate mentionate la alineatul (1) pot fi furnizate de asemenea, in special, prin:

(a) clauze contractuale intre operator sau persoana imputernicita de operator si operatorul, persoana imputernicita de operator sau destinatarul datelor cu caracter personal din tara terta sau organizatia internationala; sau

(b) dispozitii care urmeaza sa fie incluse in acordurile administrative dintre autoritatile sau organismele publice, care includ drepturi opozabile si efective pentru persoanele vizate.

(4) Autoritatea de supraveghere aplica mecanismul pentru asigurarea coerentei mentionat la articolul 63, in cazurile mentionate la alineatul (3) din prezentul articol.

(5) Autorizatiile acordate de un stat membru sau de o autoritate de supraveghere in temeiul articolului 26 alineatul (2) din Directiva 95/46/CE sunt valabile pana la data la care sunt modificate, inlocuite sau abrogate, daca este necesar, de respectiva autoritate de supraveghere. Deciziile adoptate de Comisie in temeiul articolului 26 alineatul (4) din Directiva 95/46/CE raman in vigoare pana cand sunt modificate, inlocuite sau abrogate, daca este necesar, de o decizie a Comisiei adoptata in conformitate cu alineatul (2) din prezentul articol.

Articolul 47
Reguli corporatiste obligatorii

(1) In conformitate cu mecanismul pentru asigurarea coerentei prevazut la articolul 63, autoritatea de supraveghere competenta aproba reguli corporatiste obligatorii, cu conditia ca acestea:

(a) sa fie obligatorii din punct de vedere juridic si sa se aplice fiecarui membru vizat al grupului de intreprinderi sau al grupului de intreprinderi implicate intr-o activitate economica comuna, inclusiv angajatilor acestuia, precum si sa fie puse in aplicare de membrii in cauza;

(b) sa confere, in mod expres, drepturi opozabile persoanelor vizate in ceea ce priveste prelucrarea datelor lor cu caracter personal; si

(c) sa indeplineasca cerintele prevazute la alineatul (2).

(2) Regulile corporatiste obligatorii mentionate la alineatul (1) precizeaza cel putin:

(a) structura si datele de contact ale grupului de intreprinderi sau ale grupului de intreprinderi implicate intr-o activitate economica comuna si ale fiecaruia dintre membrii sai;

(b) transferurile de date sau setul de transferuri, inclusiv categoriile de date cu caracter personal, tipul prelucrarii si scopurile prelucrarii, tipurile de persoane vizate afectate si identificarea tarii terte sau a tarilor terte in cauza;

(c) caracterul lor juridic obligatoriu, atat pe plan intern, cat si extern;

(d) aplicarea principiilor generale in materie de protectie a datelor, in special limitarea scopului, reducerea la minimum a datelor, perioadele de stocare limitate, calitatea datelor, protectia datelor incepand cu momentul conceperii si protectia implicita, temeiul juridic pentru prelucrare, prelucrarea categoriilor speciale de date cu caracter personal, masurile de asigurare a securitatii datelor, precum si cerintele referitoare la transferurile ulterioare catre organisme care nu fac obiectul regulilor corporatiste obligatorii;

(e) drepturile persoanelor vizate in ceea ce priveste prelucrarea si mijloacele de exercitare a acestor drepturi, inclusiv dreptul de a nu face obiectul unor decizii bazate exclusiv pe prelucrarea automata, inclusiv crearea de profiluri, in conformitate cu articolul 22, dreptul de a depune o plangere in fata autoritatii de supraveghere competente si in fata instantelor competente ale statelor membre, in conformitate cu articolul 79, precum si dreptul de a obtine reparatii si, dupa caz, despagubiri pentru incalcarea regulilor corporatiste obligatorii;

(f) acceptarea de catre operator sau de persoana imputernicita de operator, care isi are sediul pe teritoriul unui stat membru, a raspunderii pentru orice incalcare a regulilor corporatiste obligatorii de catre orice membru in cauza care nu isi are sediul in Uniune; operatorul sau persoana imputernicita de operator este exonerat(a) de aceasta raspundere, integral sau partial, numai daca dovedeste ca membrul respectiv nu a fost raspunzator de evenimentul care a cauzat prejudiciul;

(g) modul in care informatiile privind regulile corporatiste obligatorii, in special privind dispozitiile mentionate la literele (d), (e) si (f) de la prezentul alineat, sunt furnizate persoanelor vizate in completarea informatiilor mentionate la articolele 13 si 14;

(h) sarcinile oricarui responsabil cu protectia datelor desemnat in conformitate cu articolul 37 sau ale oricarei alte persoane sau entitati insarcinate cu monitorizarea respectarii regulilor corporatiste obligatorii in cadrul grupului de intreprinderi sau al grupului de intreprinderi implicate intr-o activitate economica comuna, a activitatilor de formare si a gestionarii plangerilor;

(i) procedurile de formulare a plangerilor;

(j) mecanismele din cadrul grupului de intreprinderi sau al grupului de intreprinderi implicate intr-o activitate economica comuna, menite sa asigure verificarea conformitatii cu regulile corporatiste obligatorii. Aceste mecanisme includ auditurile privind protectia datelor si metodele de asigurare a actiunilor corective menite sa protejeze drepturile persoanei vizate. Rezultatele acestor verificari ar trebui sa fie comunicate persoanei sau entitatii mentionate la litera (h) si consiliului de administratie al intreprinderii care exercita controlul grupului de intreprinderi sau al grupului de intreprinderi implicate intr-o activitate economica comuna si ar trebui sa fie puse la dispozitia autoritatii de supraveghere competente, la cerere;

(k) mecanismele de raportare si inregistrare a modificarilor aduse regulilor si de raportare a acestor modificari autoritatii de supraveghere;

(l) mecanismul de cooperare cu autoritatea de supraveghere in vederea asigurarii respectarii regulilor de catre orice membru al grupului de intreprinderi sau al grupului de intreprinderi implicate intr-o activitate economica comuna, in special prin punerea la dispozitia autoritatii de supraveghere a rezultatelor verificarilor cu privire la masurile mentionate la punctul (j);

(m) mecanismele de raportare catre autoritatea de supraveghere competenta a oricaror cerinte legale impuse unui membru al grupului de intreprinderi sau al grupului de intreprinderi implicate intr-o activitate economica comuna intr-o tara terta care pot avea un efect advers considerabil asupra garantiilor furnizate prin regulile corporatiste obligatorii; si

(n) formarea corespunzatoare in domeniul protectiei datelor a personalului care are un acces permanent sau periodic la date cu caracter personal.

(3) Comisia poate preciza formatul si procedurile pentru schimbul de informatii intre operatori, persoanele imputernicite de operatori si autoritatile de supraveghere pentru regulile corporatiste obligatorii in sensul prezentului articol. Actele de punere in aplicare respective se adopta in conformitate cu procedura de examinare prevazuta la articolul 93 alineatul (2).

Articolul 48

Transferurile sau divulgarile de informatii neautorizate de dreptul Uniunii

Orice hotarare a unei instante sau a unui tribunal si orice decizie a unei autoritati administrative a unei tari terte care impun unui operator sau persoanei imputernicite de operator sa transfere sau sa divulge date cu caracter personal poate fi recunoscuta sau executata in orice fel numai daca se bazeaza pe un acord international, cum ar fi un tratat de asistenta judiciara reciproca in vigoare intre tara terta solicitanta si Uniune sau un stat membru, fara a se aduce atingere altor motive de transfer in temeiul prezentului capitol.

Articolul 49

Derogari pentru situatii specifice

(1) In absenta unei decizii privind caracterul adecvat al nivelului de protectie in conformitate cu articolul 45 alineatul (3) sau a unor garantii adecvate in conformitate cu articolul 46, inclusiv a regulilor corporatiste obligatorii, un transfer sau un set de transferuri de date cu caracter personal catre o tara terta sau o organizatie internationala poate avea loc numai in una dintre conditiile urmatoare:

(a) persoana vizata si-a exprimat in mod explicit acordul cu privire la transferul propus, dupa ce a fost informata asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizata ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protectie si a unor garantii adecvate;

(b) transferul este necesar pentru executarea unui contract intre persoana vizata si operator sau pentru aplicarea unor masuri precontractuale adoptate la cererea persoanei vizate;

(c) transferul este necesar pentru incheierea unui contract sau pentru executarea unui contract incheiat in interesul persoanei vizate intre operator si o alta persoana fizica sau juridica;

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

(e) transferul este necesar pentru stabilirea, exercitarea sau apararea unui drept in instanta;

(f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci cand persoana vizata nu are capacitatea fizica sau juridica de a-si exprima acordul;

(g) transferul se realizeaza dintr-un registru care, potrivit dreptului Uniunii sau al dreptului intern, are scopul de a furniza informatii publicului si care poate fi consultat fie de public in general, fie de orice persoana care

poate face dovada unui interes legitim, dar numai in masura in care sunt indeplinite conditiile cu privire la consultare prevazute de dreptul Uniunii sau de dreptul intern in acel caz specific.

In cazul in care un transfer nu ar putea sa se intemeieze pe o dispozitie prevazuta la articolul 45 sau 46, inclusiv dispozitii privind reguli corporatiste obligatorii, si nu este aplicabila niciuna dintre derogarile pentru situatii specifice prevazute la primul paragraf din prezentul alineat, un transfer catre o tara terta sau o organizatie internationala poate avea loc numai in cazul in care transferul nu este repetitiv, se refera doar la un numar limitat de persoane vizate, este necesar in scopul realizarii intereselor legitime majore urmarite de operator asupra caruia nu prevaleaza interesele sau drepturile si libertatile persoanei vizate si operatorul a evaluat toate circumstantele aferente transferului de date si, pe baza acestei evaluari, a prezentat garantii corespunzatoare in ceea ce priveste protectia datelor cu caracter personal. Operatorul informeaza autoritatea de supraveghere cu privire la transfer. Operatorul, in plus fata de furnizarea informatiilor mentionate la articolele 13 si 14, informeaza persoana vizata cu privire la transfer si la interesele legitime majore pe care le urmareste.

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

(3) Alineatul (1) primul paragraf literele (a), (b) si (c) si paragraful al doilea nu se aplica in cazul activitatilor desfasurate de autoritatile publice in exercitarea competentelor lor publice.

(4) Interesul public prevazut la alineatul (1) primul paragraf litera (d) este recunoscut in dreptul Uniunii sau in dreptul statului membru sub incidenta caruia intra operatorul.

(5) In absenta unei decizii privind caracterul adecvat al nivelului de protectie, dreptul Uniunii sau dreptul intern poate, din considerente importante de interes public, sa stabileasca in mod expres limite asupra transferului unor categorii specifice de date cu caracter personal catre o tara terta sau o organizatie internationala. Statele membre notifica aceste dispozitii Comisiei.

(6) Operatorul sau persoana imputernicita de operator consemneaza evaluarea, precum si garantiile adecvate prevazute la paragraful al doilea al alineatului (1) din prezentul articol, in evidentele mentionate la articolul 30.

Articolul 50
Cooperarea internationala in domeniul protectiei datelor cu caracter personal

In ceea ce priveste tarile terte si organizatiile internationale, Comisia si autoritatile de supraveghere iau masurile corespunzatoare pentru:

(a) elaborarea de mecanisme de cooperare internationala pentru a facilita asigurarea aplicarii efective a legislatiei privind protectia datelor cu caracter personal;

(b) acordarea de asistenta internationala reciproca in asigurarea aplicarii legislatiei din domeniul protectiei datelor cu caracter personal, inclusiv prin notificare, transferul plangerilor, asistenta in investigatii si schimb de informatii, sub rezerva unor garantii adecvate pentru protectia datelor cu caracter personal si a altor drepturi si libertati fundamentale;

(c) implicarea partilor interesate relevante in discutiile si activitatile care au ca scop intensificarea cooperarii internationale in domeniul aplicarii legislatiei privind protectia datelor cu caracter personal;

(d) promovarea schimbului reciproc si a documentatiei cu privire la legislatia si practicile in materie de protectie a datelor cu caracter personal, inclusiv in ceea ce priveste conflictele jurisdictionale cu tarile terte.

CAPITOLUL VI
Autoritati de supraveghere independente

Sectiunea 1
Statutul independent

Articolul 51
Autoritatea de supraveghere

(1) Fiecare stat membru se asigura ca una sau mai multe autoritati publice independente sunt responsabile de monitorizarea aplicarii prezentului regulament, in vederea protejarii drepturilor si libertatilor fundamentale ale

persoanelor fizice in ceea ce priveste prelucrarea si in vederea facilitarii liberei circulatii a datelor cu caracter personal in cadrul Uniunii ("autoritatea de supraveghere").

(2) Fiecare autoritate de supraveghere contribuie la aplicarea coerenta a prezentului regulament in intreaga Uniune. In acest scop, autoritatile de supraveghere coopereaza atat intre ele, cat si cu Comisia, in conformitate cu capitolul VII.

(3) In cazul in care mai multe autoritati de supraveghere sunt instituite intr-un stat membru, acesta desemneaza autoritatea de supraveghere care reprezinta autoritatile respective in cadrul comitetului si instituie un mecanism prin care sa asigure respectarea de catre celelalte autoritati a normelor privind mecanismul pentru asigurarea coerentei prevazut la articolul 63.

(4) Fiecare stat membru notifica Comisiei dispozitiile de drept pe care le adopta in temeiul prezentului capitol pana la 25 mai 2018 si, fara intarziere, orice modificare ulterioara pe care o aduce acestor dispozitii.

Articolul 52
Independenta

(1) Fiecare autoritate de supraveghere beneficiaza de independenta deplina in indeplinirea sarcinilor sale si exercitarea competentelor sale in conformitate cu prezentul regulament.

(2) Membrul sau membrii fiecarei autoritati de supraveghere, in cadrul indeplinirii sarcinilor si al exercitarii competentelor sale (lor) in conformitate cu prezentul regulament, ramane (raman) independent (independenti) de orice influenta externa directa sau indirecta si nici nu solicita, nici nu accepta instructiuni de la o parte externa.

(3) Membrul sau membrii fiecarei autoritati de supraveghere se abtin de la a intreprinde actiuni incompatibile cu atributiile lor, iar pe durata mandatului, nu desfasoara activitati incompatibile, remunerate sau nu.

(4) Fiecare stat membru se asigura ca fiecare autoritate de supraveghere beneficiaza de resurse umane, tehnice si financiare, de un sediu si de infrastructura necesara pentru indeplinirea sarcinilor si exercitarea efectiva a competentelor sale, inclusiv a celor care urmeaza sa fie aplicate in contextul asistentei reciproce, al cooperarii si al participarii in cadrul comitetului.

(5) Fiecare stat membru se asigura ca fiecare autoritate de supraveghere isi selecteaza personalul propriu si detine personal propriu aflat sub conducerea exclusiva a membrului sau membrilor autoritatii de supraveghere respective.

(6) Fiecare stat membru se asigura ca fiecare autoritate de supraveghere face obiectul unui control financiar care nu aduce atingere independentei sale si ca dispune de bugete anuale distincte, publice, care pot face parte din bugetul general de stat sau national.

Articolul 53
Conditii generale aplicabile membrilor autoritatii de supraveghere

(1) Statele membre se asigura ca fiecare membru al autoritatii lor de supraveghere este numit prin intermediul unei proceduri transparente:

- de parlament;
- de guvern;
- de seful statului; sau
- de un organism independent imputernicit sa faca numiri in temeiul dreptului intern.

(2) Fiecare membru in cauza are calificarile, experienta si competentele necesare, in special in domeniul protectiei datelor cu caracter personal, pentru a-si putea indeplini atributiile si exercita competentele.

(3) Atributiile unui membru inceteaza in cazul expirarii mandatului, in cazul demisiei sau pensionarii din oficiu in conformitate cu dreptul intern relevant.

(4) Un membru poate fi demis doar in cazuri de abateri grave sau daca nu mai indeplineste conditiile necesare pentru indeplinirea atributiilor sale.

Articolul 54
Norme privind instituirea autoritatii de supraveghere

(1) Fiecare stat membru prevede, pe cale legislativa, urmatoarele:

(a) instituirea fiecarei autoritati de supraveghere;

(b) calificarile si conditiile de eligibilitate necesare pentru a fi numit in calitate de membru al fiecarei autoritati de supraveghere;

(c) normele si procedurile pentru numirea membrului sau a membrilor fiecarei autoritati de supraveghere;

(d) durata mandatului membrului sau membrilor fiecarei autoritati de supraveghere, de minimum patru ani, cu exceptia primei numiri dupa 24 mai 2016, din care o parte poate fi pe o perioada mai scurta in cazul in care acest lucru este necesar pentru a proteja independenta autoritatii de supraveghere printr-o procedura de numiri esalonate;

(e) daca si de cate ori este eligibil pentru reinnoire mandatul membrului sau membrilor fiecarei autoritati de supraveghere;

(f) conditiile care reglementeaza obligatiile membrului sau membrilor si ale personalului fiecarei autoritati de supraveghere, interdictii privind actiunile, ocupatiile si beneficiile incompatibile cu acestea in cursul mandatului si dupa incetarea acestuia, precum si normele care reglementeaza incetarea contractului de angajare.

(2) Membrul sau membrii si personalul fiecarei autoritati de supraveghere au obligatia, in conformitate cu dreptul Uniunii sau cu dreptul intern, de a respecta atat pe parcursul mandatului, cat si dupa incetarea acestuia, secretul profesional in ceea ce priveste informatiile confidentiale de care au luat cunostinta in cursul indeplinirii sarcinilor sau al exercitarii competentelor lor. Pe durata mandatului lor, aceasta obligatie de pastrare a secretului profesional se aplica in special in ceea ce priveste raportarea de catre persoane fizice a incalcarilor prezentului regulament.

Sectiunea 2
Abilitari, sarcini si competente

Articolul 55
Competenta

(1) Fiecare autoritate de supraveghere are competenta sa indeplineasca sarcinile si sa exercite competentele care ii sunt conferite in conformitate cu prezentul regulament pe teritoriul statului membru de care apartine.

(2) In cazul in care prelucrarea este efectuata de autoritati publice sau de organisme private care actioneaza pe baza literei (c) sau (e) de la articolul 6 alineatul (1), este autoritatea de supraveghere din statul membru respectiv. In astfel de cazuri, nu se aplica articolul 56.

(3) Autoritatile de supraveghere nu sunt competente sa supravegheze operatiunile de prelucrare ale instantelor care actioneaza in exercitiul functiei lor judiciare.

Articolul 56
Competenta autoritatii de supraveghere principale

(1) Fara a aduce atingere articolului 55, autoritatea de supraveghere a sediului principal sau a sediului unic al operatorului sau al persoanei imputernicite de operator este competenta sa actioneze in calitate de autoritate de supraveghere principala pentru prelucrarea transfrontaliera efectuata de respectivul operator sau respectiva persoana imputernicita in cauza in conformitate cu procedura prevazuta la articolul 60.

(2) Prin derogare de la alineatul (1), fiecare autoritate de supraveghere este competenta sa trateze o plangere depusa in atentia sa sau o eventuala incalcare a prezentului regulament, in cazul in care obiectul acesteia se refera numai la un sediu aflat in statul sau membru sau afecteaza in mod semnificativ persoane vizate numai in statul sau membru.

(3) In cazurile mentionate la alineatul (2) din prezentul articol, autoritatea de supraveghere informeaza fara intarziere autoritatea de supraveghere principala cu privire la aceasta chestiune. In termen de trei saptamani de la momentul informarii, autoritatea de supraveghere principala decide daca trateaza sau nu cazul respectiv in conformitate cu procedura prevazuta la articolul 60, luand in considerare daca exista sau nu un sediu al operatorului sau al persoanei imputernicite de operator pe teritoriul statului membru a carui autoritate de supraveghere a informat-o.

(4) In cazul in care autoritatea de supraveghere principala decide sa trateze cazul, se aplica procedura prevazuta la articolul 60. Autoritatea de supraveghere care a informat autoritatea de supraveghere principala poate inainta un proiect de decizie acesteia din urma. Autoritatea de supraveghere principala tine seama in cea mai mare masura posibila de proiectul respectiv atunci cand pregateste proiectul de decizie prevazut la articolul 60 alineatul (3).

(5) In cazul in care autoritatea de supraveghere principala decide sa nu trateze cazul, autoritatea de supraveghere care a informat autoritatea de supraveghere principala trateaza cazul in conformitate cu articolele 61 si 62.

(6) Autoritatea de supraveghere principala este singurul interlocutor al operatorului sau al persoanei imputernicite de operator in ceea ce priveste prelucrarea transfrontaliera efectuata de respectivul operator sau de respectiva persoana imputernicita de operator.

Articolul 57
Sarcini

(1) Fara a aduce atingere altor sarcini stabilite in temeiul prezentului regulament, fiecare autoritate de supraveghere, pe teritoriul sau:

(a) monitorizeaza si asigura aplicarea prezentului regulament;

(b) promoveaza actiuni de sensibilizare si de intelegere in randul publicului a riscurilor, normelor, garantiilor si drepturilor in materie de prelucrare. Se acorda atentie speciala activitatilor care se adreseaza in mod specific copiilor;

(c) ofera consiliere, in conformitate cu dreptul intern, parlamentului national, guvernului si altor institutii si organisme cu privire la masurile legislative si administrative referitoare la protectia drepturilor si libertatilor persoanelor fizice in ceea ce priveste prelucrarea;

(d) promoveaza actiuni de sensibilizare a operatorilor si a persoanelor imputernicite de acestia cu privire la obligatiile care le revin in temeiul prezentului regulament;

(e) la cerere, furnizeaza informatii oricarei persoane vizate in legatura cu exercitarea drepturilor sale in conformitate cu prezentul regulament si, daca este cazul, coopereaza cu autoritatile de supraveghere din alte state membre in acest scop;

(f) trateaza plangerile depuse de o persoana vizata, un organism, o organizatie sau o asociatie in conformitate cu articolul 80 si investigheaza intr-o masura adecvata obiectul plangerii si informeaza reclamantul cu privire la evolutia si rezultatul investigatiei, intr-un termen rezonabil, in special daca este necesara efectuarea unei investigatii mai amanuntite sau coordonarea cu o alta autoritate de supraveghere;

(g) coopereaza, inclusiv prin schimb de informatii, cu alte autoritati de supraveghere si isi ofera asistenta reciproca pentru a asigura coerenta aplicarii si respectarii prezentului regulament;

(h) desfasoara investigatii privind aplicarea prezentului regulament, inclusiv pe baza unor informatii primite de la o alta autoritate de supraveghere sau de la o alta autoritate publica;

(i) monitorizeaza evolutiile relevante, in masura in care acestea au impact asupra protectiei datelor cu caracter personal, in special evolutia tehnologiilor informatiei si comunicatiilor si a practicilor comerciale;

(j) adopta clauze contractuale standard mentionate la articolul 28 alineatul (8) si la articolul 46 alineatul (2) litera (d);

(k) intocmeste si mentine la zi o lista in legatura cu cerinta privind evaluarea impactului asupra protectiei datelor, in conformitate cu articolul 35 alineatul (4);

(l) ofera consiliere cu privire la operatiunile de prelucrare mentionate la articolul 36 alineatul (2);

(m) incurajeaza elaborarea de coduri de conduita in conformitate cu articolul 40 alineatul (1), isi da avizul cu privire la acestea si le aproba pe cele care ofera suficiente garantii, in conformitate cu articolul 40 alineatul (5);

(n) incurajeaza stabilirea unor mecanisme de certificare, precum si a unor sigilii si marci in domeniul protectiei datelor in conformitate cu articolul 42 alineatul (1) si aproba criteriile de certificare in conformitate cu articolul 42 alineatul (5);

(o) acolo unde este cazul, efectueaza o revizuire periodica a certificarilor acordate, in conformitate cu articolul 42 alineatul (7);

(p) elaboreaza si publica criteriile de acreditare a unui organism de monitorizare a codurilor de conduita in conformitate cu articolul 41 si a unui organism de certificare in conformitate cu articolul 43;

(q) coordoneaza procedura de acreditare a unui organism de monitorizare a codurilor de conduita in conformitate cu articolul 41 si a unui organism de certificare in conformitate cu articolul 43;

(r) autorizeaza clauzele si dispozitiile contractuale mentionate la articolul 46 alineatul (3);

(s) aproba regulile corporatiste obligatorii in conformitate cu articolul 47;

(t) contribuie la activitatile comitetului;

(u) mentine la zi evidente interne privind incalcarile prezentului regulament si masurile luate, in special avertismentele emise si sanctiunile impuse in conformitate cu articolul 58 alineatul (2); si

(v) indeplineste orice alte sarcini legate de protectia datelor cu caracter personal.

(2) Fiecare autoritate de supraveghere faciliteaza depunerea plangerilor mentionate la alineatul (1) litera (f) prin masuri precum punerea la dispozitie a unui formular de depunere a plangerii care sa poata fi completat inclusiv in format electronic, fara a exclude alte mijloace de comunicare.

(3) Indeplinirea sarcinilor fiecarei autoritati de supraveghere este gratuita pentru persoana vizata si, dupa caz, pentru responsabilul cu protectia datelor.

(4) In cazul in care cererile sunt in mod vadit nefondate sau excesive, in special din cauza caracterului lor repetitiv, autoritatea de supraveghere poate percepe o taxa rezonabila, bazata pe costurile administrative, sau poate refuza sa le trateze. Sarcina de a demonstra caracterul evident nefondat sau excesiv al cererii revine autoritatii de supraveghere.

Articolul 58
Competente

(1) Fiecare autoritate de supraveghere are toate urmatoarele competente de investigare:

(a) de a da dispozitii operatorului si persoanei imputernicite de operator si, dupa caz, reprezentantului operatorului sau al persoanei imputernicite de operator sa furnizeze orice informatii pe care autoritatea de supraveghere le solicita in vederea indeplinirii sarcinilor sale;

(b) de a efectua investigatii sub forma de audituri privind protectia datelor;

(c) de a efectua o revizuire a certificarilor acordate in temeiul articolului 42 alineatul (7);

(d) de a notifica operatorul sau persoana imputernicita de operator cu privire la presupusa incalcare a prezentului regulament;

(e) de a obtine, din partea operatorului si a persoanei imputernicite de operator, accesul la toate datele cu caracter personal si la toate informatiile necesare pentru indeplinirea sarcinilor sale;

(f) de a obtine accesul la oricare dintre incintele operatorului si ale persoanei imputernicite de operator, inclusiv la orice echipamente si mijloace de prelucrare a datelor, in conformitate cu dreptul Uniunii sau cu dreptul procesual intern.

(2) Fiecare autoritate de supraveghere are toate urmatoarele competente corective:

(a) de a emite avertizari in atentia unui operator sau a unei persoane imputernicite de operator cu privire la posibilitatea ca operatiunile de prelucrare prevazute sa incalce dispozitiile prezentului regulament;

(b) de a emite mustrari adresate unui operator sau unei persoane imputernicite de operator in cazul in care operatiunile de prelucrare au incalcat dispozitiile prezentului regulament;

(c) de a da dispozitii operatorului sau persoanei imputernicite de operator sa respecte cererile persoanei vizate de a-si exercita drepturile in temeiul prezentului regulament;

(d) de a da dispozitii operatorului sau persoanei imputernicite de operator sa asigure conformitatea operatiunilor de prelucrare cu dispozitiile prezentului regulament, specificand, dupa caz, modalitatea si termenul-limita pentru aceasta;

(e) de a obliga operatorul sa informeze persoana vizata cu privire la o incalcare a protectiei datelor cu caracter personal;

(f) de a impune o limitare temporara sau definitiva, inclusiv o interdictie asupra prelucrarii;

(g) de a dispune rectificarea sau stergerea datelor cu caracter personal sau restrictionarea prelucrarii, in temeiul articolelor 16, 17 si 18, precum si notificarea acestor actiuni destinatarilor carora le-au fost divulgate datele cu caracter personal, in conformitate cu articolul 17 alineatul (2) si cu articolul 19;

(h) de a retrage o certificare sau de a obliga organismul de certificare sa retraga o certificare eliberata in temeiul articolul 42 si 43 sau de a obliga organismul de certificare sa nu elibereze o certificare in cazul in care cerintele de certificare nu sunt sau nu mai sunt indeplinite;

(i) de a impune amenzi administrative in conformitate cu articolul 83, in completarea sau in locul masurilor mentionate la prezentul alineat, in functie de circumstantele fiecarui caz in parte;

(j) de a dispune suspendarea fluxurilor de date catre un destinatar dintr-o tara terta sau catre o organizatie internationala.

(3) Fiecare autoritate de supraveghere are toate urmatoarele competente de autorizare si de consiliere:

(a) de a oferi consiliere operatorului in conformitate cu procedura de consultare prealabila mentionata la articolul 36;

(b) de a emite avize, din proprie initiativa sau la cerere, parlamentului national, guvernului statului membru sau, in conformitate cu dreptul intern, altor institutii si organisme, precum si publicului, cu privire la orice aspect legat de protectia datelor cu caracter personal;

(c) de a autoriza prelucrarea mentionata la articolul 36 alineatul (5), in cazul in care dreptul statului membru prevede o astfel de autorizare prealabila;

(d) de a emite un aviz si de a aproba proiectele de coduri de conduita, in conformitate cu articolul 40 alineatul (5);

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

(f) de a emite certificari si de a aproba criterii de certificare in conformitate cu articolul 42 alineatul (5);

(g) de a adopta clauzele standard in materie de protectie a datelor mentionate la articolul 28 alineatul (8) si la articolul 46 alineatul (2) litera (d);

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

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

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

(4) Exercitarea competentelor conferite autoritatii de supraveghere in temeiul prezentului articol face obiectul unor garantii adecvate, inclusiv cai de atac judiciare eficiente si procese echitabile, prevazute in dreptul Uniunii si in dreptul intern in conformitate cu carta.

(5) Fiecare stat membru prevede, pe cale legislativa, faptul ca autoritatea sa de supraveghere are competenta de a aduce in fata autoritatilor judiciare cazurile de incalcare a prezentului regulament si, dupa caz, de a initia sau de a se implica intr-un alt mod in proceduri judiciare, in scopul de a asigura aplicarea dispozitiilor prezentului regulament.

(6) Fiecare stat membru poate sa prevada in dreptul sau faptul ca autoritatea sa de supraveghere are competente suplimentare, in afara celor mentionate la alineatele (1), (2) si (3). Exercitarea acestor competente nu afecteaza modul de operare eficienta a capitolului VII.

Articolul 59
Rapoarte de activitate

Fiecare autoritate de supraveghere intocmeste un raport anual cu privire la activitatile sale, care poate include o lista a tipurilor de incalcari notificate si a tipurilor de masuri luate in conformitate cu articolul 58 alineatul (2). Rapoartele se transmit parlamentului national, guvernului si altor autoritati desemnate prin dreptul intern. Acestea se pun la dispozitia publicului, a Comisiei si a comitetului.

CAPITOLUL VII
Cooperare si coerenta

Sectiunea 1
Cooperare

Articolul 60
Cooperarea dintre autoritatea de supraveghere principala si celelalte autoritati de supraveghere vizate

(1) Autoritatea de supraveghere principala coopereaza cu celelalte autoritati de supraveghere vizate, in conformitate cu prezentul articol, in incercarea de a ajunge la un consens. Autoritatea de supraveghere principala si autoritatile de supraveghere vizate isi comunica reciproc toate informatiile relevante.

(2) Autoritatea de supraveghere principala poate solicita in orice moment altor autoritati de supraveghere vizate sa ofere asistenta reciproca in temeiul articolului 61 si poate desfasura operatiuni comune in temeiul articolului 62, in special in vederea efectuarii de investigatii sau a monitorizarii punerii in aplicare a unei masuri referitoare la un operator sau o persoana imputernicita de operator, stabilit(a) in alt stat membru.

(3) Autoritatea de supraveghere principala comunica fara intarziere informatiile relevante referitoare la aceasta chestiune celorlalte autoritati de supraveghere vizate. Autoritatea de supraveghere principala transmite fara intarziere un proiect de decizie celorlalte autoritati de supraveghere vizate, pentru a obtine avizul lor, si tine seama in mod corespunzator de opiniile acestora.

(4) In cazul in care oricare dintre celelalte autoritati de supraveghere vizate exprima, in termen de patru saptamani dupa ce a fost consultata in conformitate cu alineatul (3) din prezentul articol, o obiectie relevanta si motivata la proiectul de decizie, autoritatea de supraveghere principala, in cazul in care nu da curs obiectiei relevante si motivate sau considera ca obiectia nu este relevanta sau motivata, sesizeaza mecanismul pentru asigurarea coerentei mentionat la articolul 63.

(5) In cazul in care intentioneaza sa dea curs obiectiei relevante si motivate formulate, autoritatea de supraveghere principala transmite celorlalte autoritati de supraveghere vizate un proiect revizuit de decizie pentru a obtine avizul acestora. Acest proiect revizuit de decizie face obiectul procedurii mentionate la alineatul (4) pe parcursul unei perioade de doua saptamani.

(6) In cazul in care niciuna dintre celelalte autoritati de supraveghere vizate nu a formulat obiectii la proiectul de decizie transmis de autoritatea de supraveghere principala in termenul mentionat la alineatele (4) si (5), se considera ca autoritatea de supraveghere principala si autoritatile de supraveghere vizate sunt de acord cu proiectul de decizie respectiv, care devine obligatoriu pentru acestea.

(7) Autoritatea de supraveghere principala adopta decizia si o notifica sediului principal sau sediului unic al operatorului sau al persoanei imputernicite de operator, dupa caz, si informeaza celelalte autoritati de supraveghere vizate si comitetul cu privire la decizia in cauza, incluzand un rezumat al elementelor si motivelor relevante. Autoritatea de supraveghere la care a fost depusa plangerea informeaza reclamantul cu privire la decizie.

(8) Prin derogare de la alineatul (7), in cazul in care o plangere este refuzata sau respinsa, autoritatea de supraveghere la care s-a depus plangerea adopta decizia, o notifica reclamantului si informeaza operatorul cu privire la acest lucru.

(9) In cazul in care autoritatea de supraveghere principala si autoritatile de supraveghere vizate sunt de acord sa refuze sau sa respinga anumite parti ale unei plangeri si sa dea curs altor parti ale plangerii respective, se adopta o decizie separata pentru fiecare dintre aceste parti. Autoritatea de supraveghere principala adopta decizia pentru partea care vizeaza actiunile referitoare la operator, o notifica sediului principal sau sediului unic al operatorului sau al persoanei imputernicite de operator de pe teritoriul statului membru in cauza si informeaza reclamantul cu privire la acest lucru, in timp ce autoritatea de supraveghere a reclamantului adopta decizia pentru partea care vizeaza refuzarea sau respingerea plangerii respective, o notifica reclamantului si informeaza operatorul sau persoana imputernicita de operator cu privire la acest lucru.

(10) In urma notificarii deciziei autoritatii de supraveghere principale in temeiul alineatelor (7) si (9), operatorul sau persoana imputernicita de operator ia masurile necesare pentru a se asigura ca activitatile de prelucrare sunt in conformitate cu decizia in toate sediile sale din Uniune. Operatorul sau persoana imputernicita de operator notifica masurile luate in vederea respectarii deciziei autoritatii de supraveghere principale, care informeaza celelalte autoritati de supraveghere vizate.

(11) In cazul in care, in circumstante exceptionale, o autoritate de supraveghere vizata are motive sa considere ca exista o nevoie urgenta de a actiona in vederea protejarii intereselor persoanelor vizate, se aplica procedura de urgenta prevazuta la articolul 66.

(12) Autoritatea de supraveghere principala si celelalte autoritati de supraveghere vizate isi furnizeaza reciproc informatiile solicitate in temeiul prezentului articol, pe cale electronica, utilizand un formular standard.

Articolul 61
Asistenta reciproca

(1) Autoritatile de supraveghere isi furnizeaza reciproc informatii relevante si asistenta pentru a pune in aplicare prezentul regulament in mod coerent si instituie masuri de cooperare eficace intre ele. Asistenta reciproca se refera, in special, la cereri de informatii si masuri de supraveghere, cum ar fi cereri privind autorizari si consultari prealabile, inspectii si investigatii.

(2) Fiecare autoritate de supraveghere ia toate masurile corespunzatoare necesare pentru a raspunde unei cererii a unei alte autoritati de supraveghere, fara intarzieri nejustificate si cel tarziu in termen de o luna de la data primirii cererii. Aceste masuri pot include, in special, transmiterea informatiilor relevante privind desfasurarea unei investigatii.

(3) Cererile de asistenta cuprind toate informatiile necesare, inclusiv scopul cererii si motivele care stau la baza acesteia. Informatiile care fac obiectul schimbului se utilizeaza numai in scopul in care au fost solicitate.

(4) Autoritatea de supraveghere solicitata nu poate refuza sa dea curs cererii, cu exceptia cazului in care:

(a) nu are competenta privind obiectul cererii sau masurile pe care este solicitata sa le execute; sau

(b) a da curs cererii ar incalca prezentul regulament sau dreptul Uniunii sau dreptului intern sub incidenta caruia intra autoritatea de supraveghere care a primit cererea.

(5) Autoritatea de supraveghere careia i s-a adresat cererea informeaza autoritatea de supraveghere care a transmis cererea cu privire la rezultate sau, dupa caz, la progresele inregistrate ori masurile intreprinse pentru a raspunde cererii. Autoritatea de supraveghere solicitata isi motiveaza fiecare refuz de a da curs cererii in temeiul alineatului (4).

(6) Ca regula, autoritatile de supraveghere solicitate furnizeaza informatiile solicitate de alte autoritati de supraveghere pe cale electronica, utilizand un formular standard.

(7) Autoritatile de supraveghere solicitate nu percep nicio taxa pentru actiunile intreprinse de acestea in temeiul unei cereri de asistenta reciproca. Autoritatile de supraveghere pot conveni asupra unor norme privind retributiile reciproce in cazul unor cheltuieli specifice rezultate in urma acordarii de asistenta reciproca in situatii exceptionale.

(8) In cazul in care o autoritate de supraveghere nu furnizeaza informatiile mentionate la alineatul (5) din prezentul articol in termen de o luna de la primirea cererii din partea altei autoritati de supraveghere, aceasta din urma poate adopta o masura provizorie pe teritoriul propriului stat membru, in conformitate cu articolul 55 alineatul (1). In acest caz, necesitatea urgenta de a actiona in temeiul articolului 66 alineatul (1) este considerata a fi indeplinita si necesita o decizie obligatorie urgenta din partea comitetului, in conformitate cu articolul 66 alineatul (2).

(9) Comisia, printr-un act de punere in aplicare, poate specifica forma si procedurile pentru asistenta reciproca mentionata in prezentul articol, precum si modalitatile de schimb de informatii pe cale electronica intre autoritatile de supraveghere si intre autoritatile de supraveghere si comitet, in special formularul standard mentionat la alineatul (6) din prezentul articol. Actele de punere in aplicare respective sunt adoptate in conformitate cu procedura de examinare mentionata la articolul 93 alineatul (2).

Articolul 62

Operatiuni comune ale autoritatilor de supraveghere

(1) Dupa caz, autoritatile de supraveghere desfasoara operatiuni comune, inclusiv investigatii comune si masuri comune de aplicare a legii, in care sunt implicati membri sau personal din autoritatile de supraveghere ale altor state membre.

(2) In cazul in care operatorul sau persoana imputernicita de operator detine sedii in mai multe state membre sau daca un numar semnificativ de persoane vizate din mai multe state membre sunt susceptibile de a fi afectate in mod semnificativ de operatiuni de prelucrare, o autoritate de supraveghere din fiecare dintre statele membre respective are dreptul de a participa la operatiunile comune. Autoritatea de supraveghere care este competenta in conformitate cu articolul 56 alineatul (1) sau alineatul (4) invita autoritatile de supraveghere din fiecare dintre aceste state membre sa ia parte la operatiunile comune respective si raspunde fara intarziere la cererea de participare a unei autoritati de supraveghere.

(3) O autoritate de supraveghere poate, in conformitate cu dreptul intern si cu acordul autoritatii de supraveghere din statul membru de origine, sa acorde competente, inclusiv competente de investigare, membrilor sau personalului autoritatii de supraveghere din statul membru de origine implicati in operatiuni comune sau, in masura in care dreptul statului membru al autoritatii de supraveghere din statul membru de primire permite acest lucru, poate autoriza membrii sau personalul autoritatii de supraveghere din statul membru de origine sa isi exercite competentele de investigare in conformitate cu dreptul statului membru al acestei din urma autoritati. Astfel de competente de investigare pot fi exercitate doar sub coordonarea si in prezenta membrilor sau personalului autoritatii de supraveghere din statul membru de primire. Membrii sau personalul autoritatii de supraveghere din statul membru de origine sunt supusi dreptului intern sub incidenta caruia intra autoritatea de supraveghere din statul membru de primire.

(4) In cazul in care, in conformitate cu alineatul (1), personalul unei autoritati de supraveghere din statul membru de origine isi desfasoara activitatea intr-un alt stat membru, statul membru de primire isi asuma responsabilitatea pentru actiunile personalului respectiv, inclusiv raspunderea pentru eventualele prejudicii cauzate de membrii personalului respectiv in cursul operatiunilor acestora, in conformitate cu dreptul statului membru pe teritoriul caruia isi desfasoara operatiunile.

(5) Statul membru pe teritoriul caruia s-au produs prejudiciile repara aceste prejudicii in conditiile aplicabile prejudiciilor cauzate de propriul sau personal. Statul membru de origine al autoritatii de supraveghere al carei

personal a cauzat prejudicii unei persoane de pe teritoriul unui alt stat membru ramburseaza acestui alt stat membru totalitatea sumelor pe care le-a platit persoanelor indreptatite in numele acestora.

(6) Fara a aduce atingere exercitarii drepturilor sale fata de terte parti si cu exceptia alineatului (5), fiecare stat membru se abtine, in cazul prevazut la alineatul (1), de la a pretinde de la un alt stat membru rambursarea despagubirilor pentru prejudiciile mentionate la alineatul (4).

(7) In cazul in care este planificata o operatiune comuna, iar o autoritate de supraveghere nu se conformeaza, in termen de o luna, obligatiei prevazute in a doua teza a alineatului (2) din prezentul articol, celelalte autoritati de supraveghere pot adopta o masura provizorie pe teritoriul statului membru al respectivei autoritati, in conformitate cu articolul 55. In acest caz, necesitatea urgenta de a actiona in temeiul articolului 66 alineatul (1) este considerata a fi indeplinita si necesita un aviz de urgenta sau o decizie obligatorie urgenta din partea comitetului, in conformitate cu articolul 66 alineatul (2).

Sectiunea 2
Asigurarea coerentei

Articolul 63
Mecanismul pentru asigurarea coerentei

Pentru a contribui la aplicarea coerenta a prezentului regulament in intreaga Uniune, autoritatile de supraveghere coopereaza intre ele si, dupa caz, cu Comisia prin mecanismul pentru asigurarea coerentei, astfel cum se prevede in prezenta sectiune.

Articolul 64
Avizul comitetului

(1) Comitetul emite un aviz de fiecare data cand o autoritate de supraveghere competenta intentioneaza sa adopte oricare dintre masurile de mai jos. In acest scop, autoritatea de supraveghere competenta comunica proiectul de decizie comitetului, atunci cand:

(a) vizeaza adoptarea unei liste de operatiuni de prelucrare care fac obiectul cerintei de efectuare a unei evaluari a impactului asupra protectiei datelor, in conformitate cu articolul 35 alineatul (4);

(b) in conformitate cu articolul 40 alineatul (7), se refera la conformitatea cu prezentul regulament a unui proiect de cod de conduita sau a unei modificari sau extinderi a unui cod de conduita;

(c) vizeaza aprobarea criteriilor pentru acreditarea unui organism in conformitate cu articolul 41 alineatul (3) sau a unui organism de certificare in conformitate cu articolul 43 alineatul (3);

(d) vizeaza determinarea clauzelor standard in materie de protectie a datelor mentionate la articolul 46 alineatul (2) litera (d) sau la articolul 28 alineatul (8);

(e) vizeaza autorizarea clauzelor contractuale mentionate la articolul 46 alineatul (3) litera (a); sau

(f) vizeaza aprobarea regulilor corporatiste obligatorii in sensul articolului 47.

(2) Orice autoritate de supraveghere, presedintele comitetului sau Comisia poate solicita ca orice chestiune de aplicare generala sau care produce efecte in mai mult de un stat membru sa fie examinata de comitet in vederea obtinerii unui aviz, in special in cazul in care o autoritate de supraveghere competenta nu respecta obligatiile privind asistenta reciproca in conformitate cu articolul 61 sau privind operatiunile comune in conformitate cu articolul 62.

(3) In cazurile mentionate la alineatele (1) si (2), comitetul emite un aviz cu privire la chestiunea care ii este prezentata, cu conditia sa nu fi emis deja un aviz cu privire la aceeasi chestiune. Avizul respectiv este adoptat in termen de opt saptamani cu majoritatea simpla a membrilor comitetului. Aceasta perioada poate fi prelungita cu sase saptamani, tinandu-se seama de complexitatea chestiunii. In ceea ce priveste proiectul de decizie mentionat la alineatul (1) transmis membrilor comitetului in conformitate cu alineatul (5), un membru care nu a emis obiectii intr-un termen rezonabil indicat de presedinte se considera a fi de acord cu proiectul de decizie.

(4) Autoritatile de supraveghere si Comisia comunica pe cale electronica comitetului, fara intarzieri nejustificate, printr-un formular standard, orice informatie relevanta, inclusiv, dupa caz, o sinteza a faptelor, proiectul de decizie, motivele care fac necesara adoptarea unei astfel de masuri, precum si opiniile altor autoritati de supraveghere vizate.

(5) Presedintele comitetului informeaza pe cale electronica, fara intarzieri nejustificate:

(a) membrii comitetului si Comisia cu privire la orice informatie relevanta care i-a fost comunicata, utilizand un formular standard. Secretariatul comitetului furnizeaza traduceri ale informatiilor relevante, acolo unde este necesar; si

(b) autoritatea de supraveghere mentionata, dupa caz, la alineatele (1) si (2), si Comisia cu privire la aviz si il publica.

(6) Autoritatea de supraveghere competenta nu isi adopta proiectul de decizie mentionat la alineatul (1) in termenul mentionat la alineatul (3).

(7) Autoritatea de supraveghere mentionata la alineatul (1) tine seama pe deplin de avizul comitetului si comunica pe cale electronica presedintelui comitetului, in termen de doua saptamani de la primirea avizului, daca isi va pastra sau isi va modifica proiectul de decizie si, daca este cazul, transmite proiectul de decizie modificat, utilizand un formular standard.

(8) In cazul in care autoritatea de supraveghere vizata informeaza presedintele comitetului, in termenul mentionat la alineatul (7) din prezentul articol, ca intentioneaza sa nu se conformeze avizului comitetului, integral sau partial, oferind motivele relevante, se aplica articolul 65 alineatul (1).

Articolul 65

Solutionarea litigiilor de catre comitet

(1) Pentru a asigura aplicarea corecta si coerenta a prezentului regulament in cazuri individuale, comitetul adopta o decizie obligatorie in urmatoarele cazuri:

(a) atunci cand, in unul dintre cazurile mentionate la articolul 60 alineatul (4), o autoritate de supraveghere vizata a formulat o obiectie relevanta si motivata la un proiect de decizie a autoritatii principale sau autoritatea principala a respins o astfel de obiectie ca nefiind relevanta sau motivata. Decizia obligatorie se refera la toate chestiunile vizate de obiectia relevanta si motivata, in special la chestiunea daca prezentul regulament a fost incalcat;

(b) in cazul in care exista opinii divergente cu privire la care dintre autoritatile de supraveghere vizate detine competenta pentru sediul principal;

(c) in cazul in care o autoritate de supraveghere competenta nu solicita avizul comitetului in cazurile mentionate la articolul 64 alineatul (1) sau nu tine seama de avizul comitetului emis in temeiul articolului 64. In acest caz, orice autoritate de supraveghere vizata sau Comisia poate comunica chestiunea comitetului.

(2) Decizia mentionata la alineatul (1) se adopta in termen de o luna de la prezentarea chestiunii, cu o majoritate de doua treimi a membrilor comitetului. Acest termen poate fi prelungit cu o luna, tinandu-se seama de complexitatea chestiunii. Decizia mentionata la alineatul (1) se motiveaza si se adreseaza autoritatii de supraveghere principale si tuturor autoritatilor de supraveghere vizate, fiind obligatorie pentru acestea.

(3) In cazul in care comitetul nu a fost in masura sa adopte o decizie in termenele mentionate la alineatul (2), acesta isi adopta decizia in termen de doua saptamani de la data expirarii celei de a doua luni mentionate la alineatul (2), cu o majoritate simpla a membrilor sai. In cazul in care membrii comitetului au opinii divergente in proportii egale, decizia se adopta prin votul presedintelui.

(4) Autoritatile de supraveghere vizate nu adopta o decizie asupra chestiunii prezentate comitetului in conformitate cu alineatul (1) in termenele mentionate la alineatele (2) si (3).

(5) Presedintele comitetului notifica, fara intarzieri nejustificate, decizia mentionata la alineatul (1) autoritatilor de supraveghere vizate. Comitetul informeaza Comisia cu privire la acest lucru. Decizia se publica pe site-ul comitetului, fara intarziere, dupa notificarea de catre autoritatea de supraveghere a deciziei finale mentionate la alineatul (6).

(6) Autoritatea de supraveghere principala sau, daca este cazul, autoritatea de supraveghere la care s-a depus plangerea isi adopta decizia finala pe baza deciziei mentionate la alineatul (1) din prezentul articol, fara intarziere nejustificata si in termen de cel mult o luna de la notificarea de catre comitet a deciziei sale. Autoritatea de supraveghere principala sau, daca este cazul, autoritatea de supraveghere la care s-a depus plangerea informeaza comitetul cu privire la data la care decizia sa finala este notificata operatorului sau persoanei imputernicite de operator si, respectiv, persoanei vizate. Decizia finala a autoritatilor de supraveghere vizate se adopta in conformitate cu conditiile prevazute la articolul 60 alineatele (7), (8) si (9). Decizia finala se refera la decizia mentionata la alineatul (1) din prezentul articol si precizeaza faptul ca decizia mentionata la respectivul alineat va fi publicata pe site-ul al comitetului, in conformitate cu alineatul (5). La decizia finala se anexeaza decizia mentionata la alineatul (1) din prezentul articol.

Articolul 66
Procedura de urgenta

(1) In circumstante exceptionale, atunci cand o autoritate de supraveghere vizata considera ca exista o necesitate urgenta de a actiona in scopul protejarii drepturilor si libertatilor persoanelor vizate, aceasta poate, prin derogare de la mecanismul pentru asigurarea coerentei mentionat la articolele 63, 64 si 65 sau de la procedura mentionata la articolul 60, sa adopte de indata masuri provizorii menite sa produca efecte juridice pe propriul sau teritoriu, cu o perioada de valabilitate determinata, care sa nu depaseasca trei luni. Autoritatea de supraveghere comunica fara intarziere aceste masuri si motivele adoptarii lor celorlalte autoritati de supraveghere vizate, comitetului si Comisiei.

(2) In cazul in care o autoritate de supraveghere a adoptat o masura in temeiul alineatului (1) si considera ca este necesara adoptarea de urgenta a unor masuri definitive, aceasta poate solicita un aviz de urgenta sau o decizie obligatorie urgenta din partea comitetului, indicand motivele pentru aceasta solicitare.

(3) Orice autoritate de supraveghere poate solicita un aviz de urgenta sau o decizie obligatorie urgenta, dupa caz, din partea comitetului in cazul in care o autoritate de supraveghere competenta nu a luat o masura adecvata intr-o situatie in care exista o necesitate urgenta de a actiona pentru a proteja drepturile si libertatile persoanelor vizate, indicand motivele pentru solicitarea unui astfel de aviz sau a unei astfel de decizii, inclusiv pentru necesitatea urgenta de a actiona.

(4) Prin derogare de la articolul 64 alineatul (3) si de la articolul 65 alineatul (2), un aviz de urgenta sau o decizie obligatorie urgenta mentionat(a) la alineatele (2) si (3) de la prezentul articol este adoptat(a) in termen de doua saptamani cu majoritate simpla a membrilor comitetului.

Articolul 67
Schimb de informatii

Comisia poate adopta acte de punere in aplicare cu un domeniu de aplicare general pentru a defini modalitatile de realizare a schimbului electronic de informatii intre autoritatile de supraveghere, precum si intre autoritatile de supraveghere si comitet, in special formularul standard mentionat la articolul 64.

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

Sectiunea 3
Comitetul european pentru protectia datelor

Articolul 68
Comitetul european pentru protectia datelor

(1) Comitetul european pentru protectia datelor ("comitetul") este instituit ca organ al Uniunii si are personalitate juridica.

(2) Comitetul este reprezentat de presedintele sau.

(3) Comitetul este alcatuit din seful unei autoritati de supraveghere din fiecare stat membru si din Autoritatea Europeana pentru Protectia Datelor sau reprezentantii respectivi ai acestora.

(4) In cazul in care intr-un stat membru mai multe autoritati de supraveghere sunt responsabile de monitorizarea aplicarii dispozitiilor adoptate in temeiul prezentului regulament, se numeste un reprezentant comun in conformitate cu dreptul intern al statului membru respectiv.

(5) Comisia are dreptul de a participa la activitatile si reuniunile comitetului fara a avea drept de vot. Comisia numeste un reprezentant. Presedintele comitetului comunica Comisiei activitatile comitetului.

(6) In cazurile mentionate la articolul 65, Autoritatea Europeana pentru Protectia Datelor detine drept de vot numai cu privire la deciziile care privesc principiile si normele aplicabile in ceea ce priveste institutiile, organismele, oficiile si agentiile Uniunii care corespund pe fond cu cele din prezentul regulament.

Articolul 69
Independenta

(1) Comitetul actioneaza independent in indeplinirea sarcinilor sale sau in exercitarea competentelor sale in conformitate cu articolele 70 si 71.

(2) Fara a aduce atingere solicitarilor din partea Comisiei mentionate la articolul 70 alineatul (1) litera (b) si la articolul 70 alineatul (2), comitetul, in indeplinirea sarcinilor sale sau in exercitarea competentelor sale, nu solicita si nu accepta instructiuni de la nicio parte externa.

Articolul 70

Sarcinile comitetului

(1) Comitetul asigura aplicarea coerenta a prezentului regulament. In acest scop, din proprie initiativa sau, dupa caz, la solicitarea Comisiei, comitetul are, in special, urmatoarele sarcini:

(a) sa monitorizeze si sa asigure aplicarea corecta a prezentului regulament, in cazurile prevazute la articolele 64 si 65, fara a aduce atingere sarcinilor autoritatilor nationale de supraveghere;

(b) sa ofere consiliere Comisiei cu privire la orice aspect legat de protectia datelor cu caracter personal in cadrul Uniunii, inclusiv cu privire la orice propunere de modificare a prezentului regulament;

(c) sa ofere consiliere Comisiei cu privire la formatul si procedurile pentru schimbul de informatii intre operatori, persoanele imputernicite de operatori si autoritatile de supraveghere pentru regulile corporatiste obligatorii;

(d) sa emita orientari, recomandari si bune practici privind procedurile de stergere a linkurilor catre datele cu caracter personal, a copiilor sau a reproducerilor acestora de care dispun serviciile de comunicatii accesibile publicului, astfel cum se mentioneaza la articolul 17 alineatul (2);

(e) sa examineze, din proprie initiativa, la cererea unuia dintre membrii sai sau la cererea Comisiei, orice chestiune referitoare la aplicarea prezentului regulament si sa emita orientari, recomandari si bune practici pentru a incuraja aplicarea coerenta a prezentului regulament;

(f) sa emita orientari, recomandari si bune practici in conformitate cu prezentul alineat litera (e) in vederea detalierii criteriilor si conditiilor pentru deciziile bazate pe crearea de profiluri mentionate la articolul 22 alineatul (2);

(g) sa emita orientari, recomandari si bune practici in conformitate cu litera (e) din prezentul alineat pentru stabilirea incalcarii securitatii datelor cu caracter personal si stabilirii intarzierilor nejustificate mentionate la articolul 33 alineatele (1) si (2), precum si pentru circumstantele speciale in care un operator sau o persoana imputernicita de catre operator are obligatia de a notifica incalcarea securitatii datelor cu caracter personal;

(h) sa emita orientari, recomandari si bune practici in conformitate cu litera (e) din prezentul alineat in ceea ce priveste circumstantele in care o incalcare a securitatii datelor cu caracter personal este susceptibila sa genereze un risc ridicat pentru drepturile si libertatile persoanelor fizice, mentionate la articolul 34 alineatul (1);

(i) sa emita orientari, recomandari si bune practici in conformitate cu litera (e) din prezentul alineat in scopul detalierii criteriilor si cerintelor aplicabile transferurilor de date cu caracter personal bazate pe regulile corporatiste obligatorii care trebuie respectate de operatori si cele care trebuie respectate de persoanele imputernicite de operatori, precum si cu privire la cerinte suplimentare necesare pentru a asigura protectia datelor cu caracter personal ale persoanelor vizate mentionate la articolul 47;

(j) sa emita orientari, recomandari si bune practici in conformitate cu litera (e) din prezentul alineat in vederea detalierii criteriilor si cerintelor pentru transferurile de date cu caracter personal mentionate la articolul 49 alineatul (1);

(k) sa elaboreze orientari destinate autoritatilor de supraveghere, referitoare la aplicarea masurilor mentionate la articolul 58 alineatele (1), (2) si (3) si sa stabileasca amenzile administrative in conformitate cu articolul 83;

(l) sa revizuiasca aplicarea practica a orientarilor, recomandarilor si bunelor practici mentionate la literele (e) si (f);

(m) sa emita orientari, recomandari si bune practici in conformitate cu litera (e) din prezentul alineat in vederea stabilirii procedurilor comune de raportare de catre persoanele fizice a incalcarilor prezentului regulament in conformitate cu articolul 54 alineatul (2);

(n) sa incurajeze elaborarea de coduri de conduita si stabilirea unor mecanisme de certificare, precum si a unor sigilii si marci in domeniul protectiei datelor, in conformitate cu articolele 40 si 42;

(o) sa efectueze acreditarea organismelor de certificare si revizuirea periodica a acreditarii in conformitate cu articolul 43 si sa tina un registru public al organismelor acreditate, in conformitate cu articolul 43 alineatul (6), si al operatorilor acreditati sau al persoanelor imputernicite de operator acreditate, stabiliti (stabilite) in tari terte, in conformitate cu articolul 42 alineatul (7);

(p) sa precizeze cerintele mentionate la articolul 43 alineatul (3), in vederea acreditarii organismelor de certificare prevazute la articolul 42;

(q) sa prezinte Comisiei un aviz privind cerintele de certificare mentionate la articolul 43 alineatul (8);

(r) sa prezinte Comisiei un aviz privind pictogramele mentionate la articolul 12 alineatul (7);

(s) sa prezinte Comisiei un aviz pentru evaluarea caracterului adecvat al nivelului de protectie intr-o tara terta sau o organizatie internationala, inclusiv pentru a determina daca o tara terta, un teritoriu, sau unul sau mai multe sectoare specificate din acea tara terta, sau o organizatie internationala nu mai asigura un nivel de protectie adecvat. In acest scop, Comisia pune la dispozitia comitetului toata documentatia necesara, inclusiv corespondenta purtata cu autoritatile publice ale tarii terte, in ceea ce priveste acea tara terta, acel teritoriu sau acel sector, sau cu organizatia internationala;

(t) sa emita avize privind proiectele de decizii ale autoritatilor de supraveghere in conformitate cu mecanismul pentru asigurarea coerentei mentionat la articolul 64 alineatul (1) privind chestiunile prezentate in conformitate cu articolul 64 alineatul (2) si sa emita decizii obligatorii in temeiul articolului 65, inclusiv in cazurile mentionate la articolul 66;

(u) sa promoveze cooperarea si schimbul eficient bilateral si multilateral de informatii si bune practici intre autoritatile de supraveghere;

(v) sa promoveze programe comune de formare si sa faciliteze schimburile de personal intre autoritatile de supraveghere, precum si, dupa caz, cu autoritatile de supraveghere ale tarilor terte sau organizatiilor internationale;

(w) sa promoveze schimbul de cunostinte si de documente privind legislatia si practicile in materie de protectie a datelor cu autoritatile de supraveghere a protectiei datelor la nivel mondial;

(x) sa emita avize privind codurile de conduita elaborate la nivelul Uniunii in temeiul articolului 40 alineatul (9); si

(y) sa tina un registru electronic accesibil publicului cu deciziile luate de autoritatile de supraveghere si de instante cu privire la chestiuni tratate in cadrul mecanismului pentru asigurarea coerentei.

(2) In cazul in care Comisia consulta comitetul, aceasta poate indica un termen limita, tinand seama de caracterul urgent al chestiunii.

(3) Comitetul isi transmite avizele, orientarile, recomandarile si bunele practici Comisiei si comitetului mentionat la articolul 93 si le face publice.

(4) Daca este cazul, comitetul consulta partile interesate si le ofera posibilitatea de a face observatii intr-un termen rezonabil. Fara a aduce atingere dispozitiilor articolului 76, comitetul publica rezultatele procedurii de consultare.

Articolul 71
Rapoarte

(1) Comitetul intocmeste un raport anual privind protectia persoanelor fizice cu privire la prelucrare in Uniune si, daca este relevant, in tari terte si organizatii internationale. Raportul este pus la dispozitia publicului si transmis Parlamentului European, Consiliului si Comisiei.

(2) Raportul anual include o revizuire a aplicarii practice a orientarilor, recomandarilor si bunelor practici mentionate la articolul 70 alineatul (1) litera (l), precum si a deciziilor obligatorii mentionate la articolul 65.

Articolul 72
Procedura

(1) Comitetul adopta decizii prin majoritate simpla a membrilor sai, cu exceptia cazului cand se prevede altfel in prezentul regulament.

(2) Comitetul isi adopta propriul regulament de procedura cu o majoritate de doua treimi a membrilor sai si isi organizeaza propriile mecanisme de functionare.

Articolul 73
Presedintele

(1) Comitetul alege un presedinte si doi vicepresedinti din randul membrilor sai, cu majoritate simpla.

(2) Mandatul presedintelui si al vicepresedintilor este de cinci ani si poate fi reinnoit o singura data.

Articolul 74
Sarcinile presedintelui

(1) Presedintele are urmatoarele sarcini:
(a) sa convoace reuniunile comitetului si sa stabileasca ordinea de zi;
(b) sa notifice deciziile adoptate de comitet, in conformitate cu articolul 65, autoritatii de supraveghere principale si autoritatilor de supraveghere vizate;
(c) sa asigure indeplinirea la timp a sarcinilor comitetului, in special in ceea ce priveste mecanismul pentru asigurarea coerentei mentionat la articolul 63.
(2) Comitetul stabileste in regulamentul sau de procedura repartizarea sarcinilor intre presedinte si vicepresedinti.

Articolul 75
Secretariatul

(1) Comitetul dispune de un secretariat, care este asigurat de Autoritatea Europeana pentru Protectia Datelor.
(2) Secretariatul isi indeplineste sarcinile exclusiv pe baza instructiunilor presedintelui comitetului.
(3) Personalul Autoritatii Europene pentru Protectia Datelor implicat in indeplinirea sarcinilor conferite comitetului in temeiul prezentului regulament face obiectul unor linii de raportare separate in raport cu personalul implicat in indeplinirea sarcinilor conferite Autoritatii Europene pentru Protectia Datelor.
(4) Daca este oportun, comitetul si Autoritatea Europeana pentru Protectia Datelor elaboreaza si publica un memorandum de intelegere pentru punerea in aplicare a prezentului articol, care sa stabileasca conditiile cooperarii si sa se aplice personalului Autoritatii Europene pentru Protectia Datelor implicat in indeplinirea sarcinilor conferite comitetului in temeiul prezentului regulament.
(5) Secretariatul ofera sprijin analitic, administrativ si logistic comitetului.
(6) Secretariatul este responsabil in special de urmatoarele:
(a) gestionarea curenta a activitatii comitetului;
(b) comunicarea dintre membrii comitetului, presedintele acestuia si Comisie;
(c) comunicarea cu alte institutii si cu publicul;
(d) utilizarea mijloacelor electronice pentru comunicarea interna si externa;
(e) traducerea informatiilor relevante;
(f) pregatirea si monitorizarea actiunilor ulterioare reuniunilor comitetului;
(g) pregatirea, redactarea si publicarea avizelor, deciziilor privind solutionarea litigiilor dintre autoritatile de supraveghere si a altor texte adoptate de comitet.

Articolul 76
Confidentialitate

(1) Discutiile din cadrul comitetului sunt confidentiale in cazul in care comitetul considera ca acest lucru este necesar in conformitate cu regulamentul sau de procedura.
(2) Accesul la documentele prezentate membrilor comitetului, expertilor si reprezentantilor partilor terte este reglementat prin Regulamentul (CE) nr. 1049/2001 al Parlamentului European si al Consiliului.

CAPITOLUL VIII
Cai de atac, raspundere si sanctiuni

Articolul 77
Dreptul de a depune o plangere la o autoritate de supraveghere

(1) Fara a aduce atingere oricaror alte cai de atac administrative sau judiciare, orice persoana vizata are dreptul de a depune o plangere la o autoritate de supraveghere, in special in statul membru in care isi are resedinta obisnuita, in care se afla locul sau de munca sau in care a avut loc presupusa incalcare, in cazul in care considera ca prelucrarea datelor cu caracter personal care o vizeaza incalca prezentul regulament.

(2) Autoritatea de supraveghere la care s-a depus plangerea informeaza reclamantul cu privire la evolutia si rezultatul plangerii, inclusiv posibilitatea de a exercita o cale de atac judiciara in temeiul articolului 78.

Articolul 78
Dreptul la o cale de atac judiciara eficienta impotriva unei autoritati de supraveghere

(1) Fara a aduce atingere oricaror alte cai de atac administrative sau nejudiciare, fiecare persoana fizica sau juridica are dreptul de a exercita o cale de atac judiciara eficienta impotriva unei decizii obligatorii din punct de vedere juridic a unei autoritati de supraveghere care o vizeaza.
(2) Fara a aduce atingere oricaror alte cai de atac administrative sau nejudiciare, fiecare persoana vizata are dreptul de a exercita o cale de atac judiciara eficienta in cazul in care autoritatea de supraveghere care este competenta in temeiul articolelor 55 si 56 nu trateaza o plangere sau nu informeaza persoana vizata in termen de trei luni cu privire la progresele sau la solutionarea plangerii depuse in temeiul articolului 77.
(3) Actiunile introduse impotriva unei autoritati de supraveghere sunt aduse in fata instantelor din statul membru in care este stabilita autoritatea de supraveghere.
(4) In cazul in care actiunile sunt introduse impotriva unei decizii a unei autoritati de supraveghere care a fost precedata de un aviz sau o decizie a comitetului in cadrul mecanismului pentru asigurarea coerentei, autoritatea de supraveghere transmite curtii avizul respectiv sau decizia respectiva.

Articolul 79
Dreptul la o cale de atac judiciara eficienta impotriva unui operator sau unei persoane imputernicite de operator

(1) Fara a aduce atingere vreunei cai de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plangere la o autoritate de supraveghere in temeiul articolului 77, fiecare persoana vizata are dreptul de a exercita o cale de atac judiciara eficienta in cazul in care considera ca drepturile de care beneficiaza in temeiul prezentului regulament au fost incalcate ca urmare a prelucrarii datelor sale cu caracter personal fara a se respecta prezentul regulament.
(2) Actiunile introduse impotriva unui operator sau unei persoane imputernicite de operator sunt prezentate in fata instantelor din statul membru unde operatorul sau persoana imputernicita de operator isi are un sediu. Alternativ, o astfel de actiune poate fi prezentata in fata instantelor din statul membru in care persoana vizata isi are resedinta obisnuita, cu exceptia cazului in care operatorul sau persoana imputernicita de operator este o autoritate publica a unui stat membru ce actioneaza in exercitarea competentelor sale publice.

Articolul 80
Reprezentarea persoanelor vizate

(1) Persoana vizata are dreptul de a mandata un organism, o organizatie sau o asociatie fara scop lucrativ, care au fost constituite in mod corespunzator in conformitate cu dreptul intern, ale caror obiective statutare sunt de interes public, care sunt active in domeniul protectiei drepturilor si libertatilor persoanelor vizate in ceea ce priveste protectia datelor lor cu caracter personal, sa depuna plangerea in numele sau, sa exercite in numele sau drepturile mentionate la articolele 77, 78 si 79, precum si sa exercite dreptul de a primi despagubiri mentionat la articolul 82 in numele persoanei vizate, daca acest lucru este prevazut in dreptul intern.
(2) Statele membre pot prevedea ca orice organism, organizatie sau asociatie mentionata la alineatul (1) din prezentul articol , independent de mandatul unei persoanei vizate, are dreptul de a depune in statul membru respectiv o plangere la autoritatea de supraveghere care este competenta in temeiul articolului 77 si de a exercita drepturile mentionate la articolele 78 si 79, in cazul in care considera ca drepturile unei persoane vizate in temeiul prezentului regulament au fost incalcate ca urmare a prelucrarii.

Articolul 81
Suspendarea procedurilor

(1) In cazul in care o instanta competenta a unui stat membru are informatii ca pe rolul unei instante dintr-un alt stat membru se afla o actiune avand acelasi obiect in ceea ce priveste activitatile de prelucrare ale aceluiasi

operator sau ale aceleasi persoane imputernicite de operator, instanta respectiva contacteaza instanta din celalalt stat membru pentru a confirma existenta unor astfel de actiuni.

(2) Atunci cand pe rolul unei instante dintr-un alt stat membru se afla o actiune avand acelasi obiect in ceea ce priveste activitatile de prelucrare ale aceluiasi operator sau ale aceleasi persoane imputernicite de operator, orice alta instanta competenta decat instanta sesizata initial poate suspenda actiunea aflata la ea pe rol.

(3) In cazul in care o astfel de actiune se judeca in prima instanta, orice instanta sesizata ulterior poate, de asemenea, la cererea uneia dintre parti, sa-si decline competenta, cu conditia ca respectiva actiune sa fie de competenta primei instante sesizate si ca dreptul aplicabil acesteia sa permita conexarea actiunilor.

Articolul 82

Dreptul la despagubiri si raspunderea

(1) Orice persoana care a suferit un prejudiciu materialesau moral ca urmare a unei incalcari a prezentului regulament are dreptul sa obtina despagubiri de la operator sau de la persoana imputernicita de operator pentru prejudiciul suferit.

(2) Orice operator implicat in operatiunile de prelucrare este raspunzator pentru prejudiciul cauzat de operatiunile sale de prelucrare care incalca prezentul regulament. Persoana imputernicita de operator este raspunzatoare pentru prejudiciul cauzat de prelucrare numai in cazul in care nu a respectat obligatiile din prezentul regulament care revin in mod specific persoanelor imputernicite de operator sau a actionat in afara sau in contradictie cu instructiunile legale ale operatorului.

(3) Operatorul sau persoana imputernicita de operator este exonerat(a) de raspundere in temeiul alineatului (2) daca dovedeste ca nu este raspunzator (raspunzatoare) in niciun fel pentru evenimentul care a cauzat prejudiciul.

(4) In cazul in care mai multi operatori sau mai multe persoane imputernicite de operator, sau un operator si o persoana imputernicita de operator sunt implicati (implicate) in aceeasi operatiune de prelucrare si raspund, in temeiul alineatelor (2) si (3), pentru orice prejudiciu cauzat de prelucrare, fiecare operator sau persoana imputernicita de operator este raspunzator (raspunzatoare) pentru intregul prejudiciu pentru a asigura despagubirea efectiva a persoanei vizate.

(5) In cazul in care un operator sau o persoana imputernicita de operator a platit, in conformitate cu alineatul (4), in totalitate despagubirile pentru prejudiciul ocazionat, respectivul operator sau respectiva persoana imputernicita de operator are dreptul sa solicite de la ceilalti operatori sau celelalte persoane imputernicite de operator implicate in aceeasi operatiune de prelucrare recuperarea acelei parti din despagubiri care corespunde partii lor de raspundere pentru prejudiciu, in conformitate cu conditiile stabilite la alineatul (2).

(6) Actiunile in exercitarea dreptului de recuperare a despagubirilor platite se introduc la instantele competente in temeiul dreptului statului membru mentionat la articolul 79 alineatul (2).

Articolul 83

Conditii generale pentru impunerea amenzilor administrative

(1) Fiecare autoritate de supraveghere asigura faptul ca impunerea unor amenzi administrative in conformitate cu prezentul articol pentru incalcarile prezentului regulament mentionate la alineatele (4), (5) si, (6) este, in fiecare caz, eficace, proportionala si disuasiva.

(2) In functie de circumstantele fiecarui caz in parte, amenzile administrative sunt impuse in completarea sau in locul masurilor mentionate la articolul 58 alineatul (2) literele (a) - (h) si (j). Atunci cand se ia decizia daca sa se impuna o amenda administrativa si decizia cu privire la valoarea amenzii administrative in fiecare caz in parte, se acorda atentia cuvenita urmatoarelor aspecte:

(a) natura, gravitatea si durata incalcarii, tinandu-se seama de natura, domeniul de aplicare sau scopul prelucrarii in cauza, precum si de numarul persoanelor vizate afectate si de nivelul prejudiciilor suferite de acestea;

(b) daca incalcarea a fost comisa intentionat sau din neglijenta;

(c) orice actiuni intreprinse de operator sau de persoana imputernicita de operator pentru a reduce prejudiciul suferit de persoana vizata;

(d) gradul de responsabilitate al operatorului sau al persoanei imputernicite de operator tinandu-se seama de masurile tehnice si organizatorice implementate de acestia in temeiul articolelor 25 si 32;

(e) eventualele incalcari anterioare relevante comise de operator sau de persoana imputernicita de operator;

(f) gradul de cooperare cu autoritatea de supraveghere pentru a remedia incalcarea si a atenua posibilele efecte negative ale incalcarii;

(g) categoriile de date cu caracter personal afectate de incalcare;

(h) modul in care incalcarea a fost adusa la cunostinta autoritatii de supraveghere, in special daca si in ce masura operatorul sau persoana imputernicita de operator a notificat incalcarea;

(i) in cazul in care masurile mentionate la articolul 58 alineatul (2) au fost dispuse anterior impotriva operatorului sau persoanei imputernicite de operator in cauza cu privire la acelasi obiect, respectarea respectivelor masuri;

(j) aderarea la coduri de conduita aprobate, in conformitate cu articolul 40, sau la mecanisme de certificare aprobate, in conformitate cu articolul 42; si

(k) orice alt factor agravant sau atenuant aplicabil circumstantelor cazului, cum ar fi beneficiile financiare dobandite sau pierderile evitate in mod direct sau indirect de pe urma incalcarii.

(3) In cazul in care un operator sau o persoana imputernicita de operator incalca in mod intentionat sau din neglijenta, pentru aceeasi operatiune de prelucrare sau pentru operatiuni de prelucrare conexe, mai multe dispozitii din prezentul regulament, cuantumul total al amenzii administrative nu poate depasi suma prevazuta pentru cea mai grava incalcare.

(4) Pentru incalcarile dispozitiilor urmatoare, in conformitate cu alineatul (2), se aplica amenzi administrative de pana la 10 000 000 EUR sau, in cazul unei intreprinderi, de pana la 2% din cifra de afaceri mondiala totala anuala corespunzatoare exercitiului financiar anterior, luandu-se in calcul cea mai mare valoare:

(a) obligatiile operatorului si ale persoanei imputernicite de operator in conformitate cu articolele 8, 11, 25-39, 42 si 43;

(b) obligatiile organismului de certificare in conformitate cu articolele 42 si 43;

(c) obligatiile organismului de monitorizare in conformitate cu articolul 41 alineatul (4).

(5) Pentru incalcarile dispozitiilor urmatoare, in conformitate cu alineatul (2), se aplica amenzi administrative de pana la 20 000 000 EUR sau, in cazul unei intreprinderi, de pana la 4% din cifra de afaceri mondiala totala anuala corespunzatoare exercitiului financiar anterior, luandu-se in calcul cea mai mare valoare:

(a) principiile de baza pentru prelucrare, inclusiv conditiile privind consimtamantul, in conformitate cu articolele 5, 6, 7 si 9;

(b) drepturile persoanelor vizate in conformitate cu articolele 12-22;

(c) transferurile de date cu caracter personal catre un destinatar dintr-o tara terta sau o organizatie internationala, in conformitate cu articolele 44-49;

(d) orice obligatii in temeiul legislatiei nationale adoptate in temeiul capitolului IX;

(e) nerespectarea unui ordin sau a unei limitari temporare sau definitive asupra prelucrarii, sau a suspendarii fluxurilor de date, emisa de catre autoritatea de supraveghere in temeiul articolului 58 alineatul (2), sau neacordarea accesului, incalcand articolul 58 alineatul (1).

(6) Pentru incalcarea unui ordin emis de autoritatea de supraveghere in conformitate cu articolul 58 alineatul (2) se aplica, in conformitate cu alineatul (2) din prezentul articol, amenzi administrative de pana la 20 000 000 EUR sau, in cazul unei intreprinderi, de pana la 4% din cifra de afaceri mondiala totala anuala corespunzatoare exercitiului financiar anterior, luandu-se in calcul cea mai mare valoare.

(7) Fara a aduce atingere competentelor corective ale autoritatilor de supraveghere mentionate la articolul 58 alineatul (2), fiecare stat membru poate prevedea norme prin care sa se stabileasca daca si in ce masura pot fi impuse amenzi administrative autoritatilor publice si organismelor publice stabilite in statul membru respectiv.

(8) Exercitarea de catre autoritatea de supraveghere a competentelor sale in temeiul prezentului articol are loc cu conditia existentei unor garantii procedurale adecvate in conformitate cu dreptul Uniunii si cu dreptul intern, inclusiv cai de atac judiciare eficiente si dreptul la un proces echitabil.

(9) In cazul in care sistemul juridic al statului membru nu prevede amenzi administrative, prezentul articol poate fi aplicat astfel incat amenda sa fie initiata de autoritatea de supraveghere competenta si impusa de instantele nationale competente, garantandu-se, in acelasi timp, faptul ca aceste cai de atac sunt eficiente si au un efect echivalent cu cel al amenzilor administrative impuse de autoritatile de supraveghere. In orice caz, amenzile impuse trebuie sa fie eficace, proportionale si disuasive. Respectivele state membre informeaza Comisia cu privire la dispozitiile de drept intern pe care le adopta in temeiul prezentului alineat pana la 25 mai 2018, precum si, fara intarziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioara a acestora.

Articolul 84
Sanctiuni

(1) Statele membre stabilesc normele privind alte sanctiunile aplicabile in caz de incalcare a prezentului regulament, in special pentru incalcari care nu fac obiectul unor amenzi administrative in temeiul articolului 83, si iau toate masurile necesare pentru a garanta faptul ca acestea sunt puse in aplicare. Sanctiunile respective sunt eficace, proportionale si disuasive.

(2) Fiecare stat membru informeaza Comisia cu privire la dispozitiile de drept intern pe care le adopta in temeiul alineatului (1) pana la 25 mai 2018, precum si, fara intarziere, cu privire la orice modificare ulterioara a acestora.

CAPITOLUL IX
Dispozitii referitoare la situatii specifice de prelucrare

Articolul 85
Prelucrarea si libertatea de exprimare si de informare

(1) Prin intermediul dreptului intern, statele membre asigura un echilibru intre dreptul la protectia datelor cu caracter personal in temeiul prezentului regulament si dreptul la libertatea de exprimare si de informare, inclusiv prelucrarea in scopuri jurnalistice sau in scopul exprimarii academice, artistice sau literare.

(2) Pentru prelucrarea efectuata in scopuri jurnalistice sau in scopul exprimarii academice, artistice sau literare, statele membre prevad exonerari sau derogari de la dispozitiile capitolului II (principii), ale capitolului III (drepturile persoanei vizate), ale capitolului IV (operatorul si persoana imputernicita de operator), ale capitolului V (transferul datelor cu caracter personal catre tari terte sau organizatii internationale), ale capitolului VI (autoritati de supraveghere independente), ale capitolului VII (cooperare si coerenta) si ale capitolului IX (situatii specifice de prelucrare a datelor) in cazul in care acestea sunt necesare pentru a asigura un echilibru intre dreptul la protectia datelor cu caracter personal si libertatea de exprimare si de informare.

(3) Fiecare stat membru informeaza Comisia cu privire la dispozitiile de drept intern pe care le-a adoptat in temeiul alineatului (2) precum si, fara intarziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioara a acestora.

Articolul 86
Prelucrarea si accesul public la documente oficiale

Datele cu caracter personal din documentele oficiale detinute de o autoritate publica sau de un organism public sau privat pentru indeplinirea unei sarcini care serveste interesului public pot fi divulgate de autoritatea sau organismul respectiv in conformitate cu dreptul Uniunii sau cu dreptul intern sub incidenta caruia intra autoritatea sau organismul, pentru a stabili un echilibru intre accesul public la documente oficiale si dreptul la protectia datelor cu caracter personal in temeiul prezentului regulament.

Articolul 87
Prelucrarea unui numar de identificare national

Statele membre pot detalia in continuare conditiile specifice de prelucrare a unui numar de identificare national sau a oricarui alt identificator cu aplicabilitate generala. In acest caz, numarul de identificare national sau orice alt identificator cu aplicabilitate generala este folosit numai in temeiul unor garantii corespunzatoare pentru drepturile si libertatile persoanei vizate in temeiul prezentului regulament.

Articolul 88
Prelucrarea in contextul ocuparii unui loc de munca

(1) Prin lege sau prin acorduri colective, statele membre pot prevedea norme mai detaliate pentru a asigura protectia drepturilor si a libertatilor cu privire la prelucrarea datelor cu caracter personal ale angajatilor in contextul ocuparii unui loc de munca, in special in scopul recrutarii, al indeplinirii clauzelor contractului de munca, inclusiv descarcarea de obligatiile stabilite prin lege sau prin acorduri colective, al gestionarii,

planificarii si organizarii muncii, al egalitatii si diversitatii la locul de munca, al asigurarii sanatatii si securitatii la locul de munca, al protejarii proprietatii angajatorului sau a clientului, precum si in scopul exercitarii si beneficierii, in mod individual sau colectiv, de drepturile si beneficiile legate de ocuparea unui loc de munca, precum si pentru incetarea raporturilor de munca.

(2) Aceste norme includ masuri corespunzatoare si specifice pentru garantarea demnitatii umane, a intereselor legitime si a drepturilor fundamentale ale persoanelor vizate, in special in ceea ce priveste transparenta prelucrarii, transferul de date cu caracter personal in cadrul unui grup de intreprinderi sau al unui grup de intreprinderi implicate intr-o activitate economica comuna si sistemele de monitorizare la locul de munca.

(3) Fiecare stat membru informeaza Comisia cu privire la dispozitiile de drept intern pe care le adopta in temeiul alineatului (1) pana la 25 mai 2018, precum si, fara intarziere, cu privire la orice modificare ulterioara a acestora.

Articolul 89

Garantii si derogari privind prelucrarea in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice

(1) Prelucrarea in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice are loc cu conditia existentei unor garantii corespunzatoare, in conformitate cu prezentul regulament, pentru drepturile si libertatile persoanelor vizate. Respectivele garantii asigura faptul ca au fost instituite masuri tehnice si organizatorice necesare pentru a se asigura, in special, respectarea principiului reducerii la minimum a datelor. Respectivele masuri pot include pseudonimizarea, cu conditia ca respectivele scopuri sa fie indeplinite in acest mod. Atunci cand respectivele scopuri pot fi indeplinite printr-o prelucrare ulterioara care nu permite sau nu mai permite identificarea persoanelor vizate, scopurile respective sunt indeplinite in acest mod.

(2) In cazul in care datele cu caracter personal sunt prelucrate in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice, dreptul Uniunii sau dreptul intern poate sa prevada derogari de la drepturile mentionate la articolele 15, 16, 18 si 21, sub rezerva conditiilor si a garantiilor prevazute la alineatul (1) din prezentul articol, in masura in care drepturile respective sunt de natura sa faca imposibila sau sa afecteze in mod grav realizarea scopurilor specifice, iar derogarile respective sunt necesare pentru indeplinirea acestor scopuri.

(3) In cazul in care datele cu caracter personal sunt prelucrate in scopuri de arhivare in interes public, dreptul Uniunii sau dreptul intern poate sa prevada derogari de la drepturile mentionate la articolele 15, 16, 18, 19, 20 si 21, sub rezerva conditiilor si a garantiilor prevazute la alineatul (1) din prezentul articol, in masura in care drepturile respective sunt de natura sa faca imposibila sau sa afecteze in mod grav realizarea scopurilor specifice, iar derogarile respective sunt necesare pentru indeplinirea acestor scopuri.

(4) In cazul in care prelucrarea mentionata la alineatele (2) si (3) serveste in acelasi timp si altui scop, derogarile se aplica numai prelucrarii in scopurile mentionate la alineatele respective.

Articolul 90

Obligatii privind pastrarea confidentialitatii

(1) Statele membre pot adopta norme specifice pentru a stabili competentele autoritatilor de supraveghere, prevazute la articolul 58 alineatul (1) literele (e) si (f), in legatura cu operatori sau cu persoane imputernicite de operatori care, in temeiul dreptului Uniunii sau al dreptului internsau in temeiul normelor stabilite de organismele nationale competente, au obligatia de a pastra secretul profesional sau alte obligatii echivalente de confidentialitate, in cazul in care acest lucru este necesar si proportional pentru a stabili un echilibru intre dreptul la protectia datelor cu caracter personal si obligatia pastrarii confidentialitatii. Respectivele norme se aplica doar in ceea ce priveste datele cu caracter personal pe care operatorul sau persoana imputernicita de operator le-a primit in urma sau in contextul unei activitati care intra sub incidenta acestei obligatii de pastrare a confidentialitatii.

(2) Fiecare stat membru notifica Comisiei normele adoptate in temeiul alineatului (1) pana la 25 mai 2018, precum si, fara intarziere, orice modificare ulterioara a acestora.

Articolul 91

Normele existente in domeniul protectiei datelor pentru

biserici si asociatii religioase

(1) In cazul in care, intr-un stat membru, bisericile si asociatiile sau comunitatile religioase aplica, la data intrarii in vigoare a prezentului regulament, un set cuprinzator de norme de protectie a persoanelor fizice cu privire la prelucrare, aceste norme pot continua sa se aplice, cu conditia sa fie aliniate la prezentul regulament.

(2) Bisericile si asociatiile religioase care aplica un set cuprinzator de norme in conformitate cu alineatul (1) din prezentul articol sunt supuse supravegherii unei autoritati de supraveghere independente care poate fi specifica, cu conditia sa indeplineasca conditiile stabilite in capitolul VI din prezentul regulament.

CAPITOLUL X
Acte delegate si acte de punere in aplicare

Articolul 92
Exercitarea delegarii

(1) Competenta de a adopta acte delegate este conferita Comisiei in conditiile prevazute de prezentul articol.

(2) Delegarea de competente prevazuta la articolul 12 alineatul (8) si la articolul 43 alineatul (8) se confera Comisiei pe o perioada nedeterminata de la 24 mai 2016.

(3) Delegarea de competente mentionata la articolul 12 alineatul (8) si la articolul 43 alineatul (8) poate fi revocata in orice moment de Parlamentul European sau de Consiliu. O decizie de revocare pune capat delegarii de competente specificata in decizia respectiva. Decizia produce efecte din ziua urmatoare datei publicarii acesteia in Jurnalul Oficial al Uniunii Europene sau de la o data ulterioara mentionata in decizie. Decizia nu aduce atingere validitatii actelor delegate care sunt deja in vigoare.

(4) De indata ce adopta un act delegat, Comisia il notifica simultan Parlamentului European si Consiliului.

(5) Un act delegat adoptat in conformitate cu articolul 12 alineatul (8) si cu articolul 43 alineatul (8) intra in vigoare numai in cazul in care nici Parlamentul European si nici Consiliul nu au formulat obiectiuni in termen de trei luni de la notificarea acestuia Parlamentului European si Consiliului, sau in cazul in care, inainte de expirarea termenului respectiv, Parlamentul European si Consiliul au informat Comisia ca nu vor formula obiectiuni. Respectivul termen se prelungeste cu trei luni la initiativa Parlamentului European sau a Consiliului.

Articolul 93
Procedura comitetului

(1) Comisia este asistata de un comitet. Comitetul respectiv este un comitet in intelesul Regulamentului (UE) nr. 182/2011.

(2) In cazul in care se face trimitere la prezentul alineat, se aplica articolul 5 din Regulamentul (UE) nr. 182/2011.

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

CAPITOLUL XI
Dispozitii finale

Articolul 94
Abrogarea Directivei 95/46/CE

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

(2) Trimiterile la directiva abrogata se interpreteaza ca trimiteri la prezentul regulament. Trimiterile la Grupul de lucru pentru protectia persoanelor in ceea ce priveste prelucrarea datelor cu caracter personal instituit prin articolul 29 din Directiva 95/46/CE se interpreteaza ca trimiteri la Comitetul european pentru protectia datelor instituit prin prezentul regulament.

Articolul 95
Relatia cu Directiva 2002/58/CE

Prezentul regulament nu impune obligatii suplimentare pentru persoanele fizice sau juridice in ceea ce priveste prelucrarea in legatura cu furnizarea de servicii de comunicatii electronice destinate publicului in retelele de comunicatii publice din Uniune, cu privire la aspectele pentru care acestora le revin obligatii specifice cu acelasi obiectiv prevazut in Directiva 2002/58/CE.

Articolul 96
Relatia cu acordurile incheiate anterior

Acordurile internationale care implica transferul de date cu caracter personal catre tari terte sau organizatii internationale, care au fost incheiate de statele membre inainte de 24 mai 2016 si care sunt in conformitate cu dreptul Uniunii aplicabil inainte de data respectiva, raman in vigoare pana cand vor fi modificate, inlocuite sau revocate.

Articolul 97
Rapoartele Comisiei

(1) Pana la 25 mai 2020 si, ulterior, la fiecare patru ani, Comisia transmite Parlamentului European si Consiliului un raport privind evaluarea si revizuirea prezentului regulament. Rapoartele sunt facute publice.
(2) In contextul evaluarilor si revizuirilor mentionate la alineatul (1), Comisia examineaza in special aplicarea si functionarea:
(a) capitolului V privind transferul datelor cu caracter personal catre tari terte sau organizatii internationale, avand in vedere in special deciziile adoptate in temeiul articolului 45 alineatul (3) din prezentul regulament si deciziile adoptate in temeiul articolului 25 alineatul (6) din Directiva 95/46/CE;
(b) capitolul VII privind cooperarea si coerenta.
(3) In scopul alineatului (1), Comisia poate solicita informatii de la statele membre si de la autoritatile de supraveghere.
(4) La efectuarea evaluarilor si a revizuirilor mentionate la alineatele (1) si (2), Comisia ia in considerare pozitiile si constatarile Parlamentului European, ale Consiliului, precum si ale altor organisme sau surse relevante.
(5) Comisia transmite, daca este necesar, propuneri corespunzatoare de modificare a prezentului regulament, in special tinand seama de evolutiile din domeniul tehnologiei informatiei si avand in vedere progresele societatii informationale.

Articolul 98
Revizuirea altor acte juridice ale Uniunii in materie
de protectie a datelor

Daca este cazul, Comisia prezinta propuneri legislative in vederea modificarii altor acte juridice ale Uniunii privind protectia datelor cu caracter personal, in vederea asigurarii unei protectii uniforme si consecvente a persoanelor fizice in ceea ce priveste prelucrarea. Acest lucru priveste in special normele referitoare la protectia persoanelor fizice in ceea ce priveste prelucrarea de catre institutiile, organismele, oficiile si agentiile Uniunii, precum si normele referitoare la libera circulatie a acestor date.

Articolul 99
Intrare in vigoare si aplicare

(1) Prezentul regulament intra in vigoare in a douazecea zi de la data publicarii in Jurnalul Oficial al Uniunii Europene.
(2) Prezentul regulament se aplica de la 25 mai 2018.

Prezentul regulament este obligatoriu in toate elementele sale si se aplica direct in toate statele membre.

Adoptat la Bruxelles, 27 aprilie 2016.

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