

**REGULAMENT (UE) nr. 679 din 27 aprilie 2016** privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE)

EMITENT

• ACT INTERNAȚIONAL

Publicat în JURNAL OFICIAL L nr. 119 din 4 mai 2016

Modificat prin Rectificare, JO L 127, 23.5.2018, p. 2

(2016/679)PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII

EUROPENE,având în vedere [Tratatul privind funcționarea Uniunii Europene](#), în special [articolul 16](#),având în vedere propunerea Comisiei Europene,după transmiterea proiectului de act legislativ către parlamentele naționale,având în vedere avizul Comitetului Economic și Social European \*1),având în vedere avizul Comitetului Regiunilor \*2),hotărând în conformitate cu procedura legislativă ordinară \*3),întrucât:(1) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. [Articolul 8 alineatul \(1\) din Carta drepturilor fundamentale](#) a Uniunii Europene ("carta") și [articolul 16 alineatul \(1\) din Tratatul privind funcționarea Uniunii Europene \(TFUE\)](#) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc.(2) Principiile și normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal ar trebui, indiferent de cetățenia sau de locul de reședință al persoanelor fizice, să respecte drepturile și libertățile fundamentale ale acestora, în special dreptul la protecția datelor cu caracter personal. Prezentul regulament urmărește să contribuie la realizarea unui spațiu de libertate, securitate și justiție și a unei uniuni economice, la progresul economic și social, la consolidarea și convergența economiilor în cadrul pieței interne și la bunăstarea persoanelor fizice.(3) [Directiva 95/46/CE](#) a Parlamentului European și a Consiliului \*4) vizează armonizarea nivelului de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește activitățile de prelucrare și asigurarea liberei circulații a datelor cu caracter personal între statele membre.(4) Prelucrarea datelor cu caracter personal ar trebui să fie în serviciul cetățenilor. Dreptul la protecția datelor cu caracter personal nu este un drept absolut; acesta trebuie luat în considerare în raport cu funcția pe care o îndeplinește în societate și echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității. Prezentul regulament respectă toate drepturile fundamentale și libertățile și principiile recunoscute în cartă astfel cum sunt consacrate în tratate, în special respectarea vieții private și de familie, a reședinței și a comunicațiilor, a protecției datelor cu caracter personal, a libertății de gândire, de conștiință și de religie, a libertății de exprimare și de informare, a libertății de a desfășura o activitate comercială, dreptul la o cale

de atac eficientă și la un proces echitabil, precum și diversitatea culturală, religioasă și lingvistică.(5) Integrarea economică și socială care rezultă din funcționarea pieței interne a condus la o creștere substanțială a fluxurilor transfrontaliere de date cu caracter personal. Schimbul de date cu caracter personal între actori publici și privați, inclusiv persoane fizice, asociații și întreprinderi, s-a intensificat în întreaga Uniune. Conform dreptului Uniunii, autoritățile naționale din statele membre sunt chemate să coopereze și să facă schimb de date cu caracter personal pentru a putea să își îndeplinească atribuțiile sau să execute sarcini în numele unei autorități dintr-un alt stat membru.(6) Evoluțiile tehnologice rapide și globalizarea au generat noi provocări pentru protecția datelor cu caracter personal. Amploarea colectării și a schimbului de date cu caracter personal a crescut în mod semnificativ. Tehnologia permite atât societăților private, cât și autorităților publice să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităților lor. Din ce în ce mai mult, persoanele fizice fac publice la nivel mondial informații cu caracter personal. Tehnologia a transformat deopotrivă economia și viața socială și ar trebui să faciliteze în continuare libera circulație a datelor cu caracter personal în cadrul Uniunii și transferul către țări terțe și organizații internaționale, asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal.(7) Aceste evoluții impun un cadru solid și mai coerent în materie de protecție a datelor în Uniune, însoțit de o aplicare riguroasă a normelor, luând în considerare importanța creării unui climat de încredere care va permite economiei digitale să se dezvolte pe piața internă. Persoanele fizice ar trebui să aibă control asupra propriilor date cu caracter personal, iar securitatea juridică și practică pentru persoane fizice, operatori economici și autorități publice ar trebui să fie consolidată.(8) În cazul în care prezentul regulament prevede specificări sau restricționări ale normelor sale de către dreptul intern, statele membre pot, în măsura în care acest lucru este necesar pentru coerență și pentru a asigura înțelegerea dispozițiilor naționale de către persoanele cărora li se aplică acestea, să încorporeze elemente din prezentul regulament în dreptul lor intern.(9) Obiectivele și principiile [Directivei 95/46/CE](#) rămân solide, dar aceasta nu a prevenit fragmentarea modului în care protecția datelor este pusă în aplicare în Uniune, insecuritatea juridică sau percepția publică larg răspândită conform căreia există riscuri semnificative pentru protecția persoanelor fizice, în special în legătură cu activitatea online. Diferențele dintre nivelurile de protecție a drepturilor și libertăților persoanelor fizice, în special a dreptului la protecția datelor cu caracter personal, în ceea ce privește prelucrarea datelor cu caracter personal din statele membre pot împiedica libera circulație a datelor cu caracter personal în întreaga Uniune. Aceste diferențe pot constitui, prin urmare, un obstacol în desfășurarea de activități economice la nivelul Uniunii, pot denatura concurența și pot împiedica autoritățile să îndeplinească responsabilitățile care le revin în

temeiul dreptului Uniunii. Această diferență între nivelurile de protecție este cauzată de existența unor deosebiri în ceea ce privește transpunerea și aplicarea [Directivei 95/46/CE](#).<sup>(10)</sup> Pentru a se asigura un nivel consecvent și ridicat de protecție a persoanelor fizice și pentru a se îndepărta obstacolele din calea circulației datelor cu caracter personal în cadrul Uniunii, nivelul protecției drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea unor astfel de date ar trebui să fie echivalent în toate statele membre. Aplicarea consecventă și omogenă a normelor în materie de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ar trebui să fie asigurată în întreaga Uniune. În ceea ce privește prelucrarea datelor cu caracter personal în vederea respectării unei obligații legale, a îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul, statelor membre ar trebui să li se permită să mențină sau să introducă dispoziții de drept intern care să clarifice într-o mai mare măsură aplicarea normelor prezentului regulament. În coroborare cu legislația generală și orizontală privind protecția datelor, prin care este pusă în aplicare [Directiva 95/46/CE](#), statele membre au mai multe legi sectoriale specifice în domenii care necesită dispoziții mai precise. Prezentul regulament oferă, de asemenea, statelor membre o marjă de manevră în specificarea normelor sale, inclusiv în ceea ce privește prelucrarea categoriilor speciale de date cu caracter personal ("date sensibile"). În acest sens, prezentul regulament nu exclude dreptul statelor membre care stabilește circumstanțele aferente unor situații de prelucrare specifice, inclusiv stabilirea cu o mai mare precizie a condițiilor în care prelucrarea datelor cu caracter personal este legală.<sup>(11)</sup> Protecția efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea și stabilirea în detaliu a drepturilor persoanelor vizate și a obligațiilor celor care prelucrează și decid prelucrarea datelor cu caracter personal, ci și competențe echivalente pentru monitorizarea și asigurarea conformității cu normele de protecție a datelor cu caracter personal și sancțiuni echivalente pentru infracțiuni în statele membre.<sup>(12)</sup> [Articolul 16 alineatul \(2\) din TFUE](#) mandatează Parlamentul European și Consiliul să stabilească normele privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal, precum și normele privind libera circulație a acestor date.<sup>(13)</sup> În vederea asigurării unui nivel uniform de protecție pentru persoanele fizice în întreaga Uniune și a preîntâmpinării discrepanțelor care împiedică libera circulație a datelor în cadrul pieței interne, este necesar un regulament în scopul de a furniza securitate juridică și transparență pentru operatorii economici, inclusiv microîntreprinderi și întreprinderi mici și mijlocii, precum și de a oferi persoanelor fizice în toate statele membre același nivel de drepturi, obligații și responsabilități opozabile din punct de vedere juridic pentru operatori și persoanele împuternicite de

aceștia, pentru a se asigura o monitorizare coerentă a prelucrării datelor cu caracter personal, sancțiuni echivalente în toate statele membre, precum și cooperarea eficace a autorităților de supraveghere ale diferitelor state membre. Pentru buna funcționare a pieței interne este necesar ca libera circulație a datelor cu caracter personal în cadrul Uniunii să nu fie restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal. Pentru a se lua în considerare situația specifică a microîntreprinderilor și a întreprinderilor mici și mijlocii, prezentul regulament include o derogare pentru organizațiile cu mai puțin de 250 de angajați în ceea ce privește păstrarea evidențelor. În plus, instituțiile și organele Uniunii și statele membre și autoritățile lor de supraveghere sunt încurajate să ia în considerare necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii în aplicarea prezentului regulament. Noțiunea de microîntreprinderi și de întreprinderi mici și mijlocii ar trebui să se bazeze pe articolul 2 din anexa la [Recomandarea 2003/361/CE](#) a Comisiei \*5).

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

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

(16) Prezentul regulament nu se aplică chestiunilor de protecție a drepturilor și libertăților fundamentale sau la libera circulație a datelor cu caracter personal referitoare la activități care nu intră în domeniul de aplicare al dreptului Uniunii, de exemplu activitățile privind securitatea națională. Prezentul regulament nu se aplică prelucrării datelor cu caracter personal de către statele membre atunci când acestea desfășoară activități legate de politica externă și de securitatea comună a Uniunii.

(17) [Regulamentul \(CE\) nr. 45/2001](#) al Parlamentului European și al Consiliului \*6) se aplică prelucrării de date cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii. [Regulamentul \(CE\) nr. 45/2001](#) și alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal ar trebui adaptate la principiile și normele stabilite în prezentul regulament și aplicate

în conformitate cu prezentul regulament. În vederea asigurării unui cadru solid și coerent în materie de protecție a datelor în Uniune, ar trebui ca după adoptarea prezentului regulament să se aducă [Regulamentului \(CE\) nr. 45/2001](#) adaptările necesare, astfel încât acestea să poată fi aplicate odată cu prezentul regulament.(18) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice și care, prin urmare, nu are legătură cu o activitate profesională sau comercială. Activitățile personale sau domestice ar putea include corespondența și repertoriul de adrese sau activitățile din cadrul rețelelor sociale și activitățile online desfășurate în contextul respectivelor activități. Cu toate acestea, prezentul regulament se aplică operatorilor sau persoanelor împuternicite de operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activități personale sau domestice.(19) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, precum și libera circulație a acestor date, face obiectul unui act juridic specific al Uniunii. Prin urmare, prezentul regulament nu ar trebui să se aplice activităților de prelucrare în aceste scopuri. Cu toate acestea, datele cu caracter personal prelucrate de către autoritățile publice în temeiul prezentului regulament, atunci când sunt utilizate în aceste scopuri, ar trebui să fie reglementate printr-un act juridic mai specific al Uniunii, și anume [Directiva \(UE\) 2016/680](#) a Parlamentului European și a Consiliului \*7). Statele membre pot încredința autorităților competente în sensul [Directivei \(UE\) 2016/680](#) sarcini care nu sunt neapărat îndeplinite în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, astfel încât prelucrarea datelor cu caracter personal pentru alte scopuri, în măsura în care se încadrează în domeniul de aplicare al dreptului Uniunii, să intre în domeniul de aplicare al prezentului regulament.În ceea ce privește prelucrarea datelor cu caracter personal de către aceste autorități competente în scopuri care intră în domeniul de aplicare al prezentului regulament, statele membre ar trebui să poată menține sau introduce dispoziții mai detaliate pentru a adapta aplicarea normelor din prezentul regulament. Aceste dispoziții pot stabili mai precis cerințe specifice pentru prelucrarea datelor cu caracter personal de către respectivele autorități competente în aceste alte scopuri, ținând seama de structura constituțională, organizatorică și administrativă a statului membru în cauză. Atunci când prelucrarea de date cu caracter personal de către organisme private face obiectul prezentului regulament, prezentul regulament ar trebui să prevadă posibilitatea ca statele membre, în anumite condiții, să

impună prin lege restricții asupra anumitor obligații și drepturi, în cazul în care asemenea restricții constituie o măsură necesară și proporțională într-o societate democratică în scopul garantării unor interese specifice importante, printre care se numără siguranța publică și prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor sau executarea pedepselor, inclusiv protejarea împotriva amenințărilor la adresa siguranței publice și prevenirea acestora. Acest lucru este relevant, de exemplu, în cadrul combaterii spălării de bani sau al activităților laboratoarelor criminalistice.(20) Deși prezentul regulament se aplică, inter alia, activităților instanțelor și ale altor autorități judiciare, dreptul Uniunii sau al statelor membre ar putea să precizeze operațiunile și procedurile de prelucrare în ceea ce privește prelucrarea datelor cu caracter personal de către instanțe și alte autorități judiciare. Prelucrarea datelor cu caracter personal nu ar trebui să fie de competența autorităților de supraveghere în cazul în care instanțele își exercită atribuțiile judiciare, în scopul garantării independenței sistemului judiciar în îndeplinirea sarcinilor sale judiciare, inclusiv în luarea deciziilor. Supravegherea unor astfel de operațiuni de prelucrare a datelor ar trebui să poată fi încredințată unor organisme specifice din cadrul sistemului judiciar al statului membru, care ar trebui să asigure în special respectarea normelor prevăzute de prezentul regulament, să sensibilizeze membrii sistemului judiciar cu privire la obligațiile care le revin în temeiul prezentului regulament și să trateze plângerile în legătură cu astfel de operațiuni de prelucrare a datelor.(21) Prezentul regulament nu aduce atingere aplicării [Directivei 2000/31/CE](#) a Parlamentului European și a Consiliului \*8), în special normelor privind răspunderea furnizorilor intermediari de servicii prevăzute la articolele 12-15 din directiva menționată. Respectiva directivă își propune să contribuie la buna funcționare a pieței interne, prin asigurarea liberei circulații a serviciilor societății informaționale între statele membre.(22) Orice prelucrare a datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune ar trebui efectuată în conformitate cu prezentul regulament, indiferent dacă procesul de prelucrare în sine are loc sau nu în cadrul Uniunii. Sediul implică exercitarea efectivă și reală a unei activități în cadrul unor înțelegeri stabile. Forma juridică a unor astfel de înțelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință.(23) Pentru a se asigura că persoanele fizice nu sunt lipsite de protecția la care au dreptul în temeiul prezentului regulament, prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Uniunii de către un operator sau o persoană împuternicită de acesta care nu își are sediul în Uniune ar trebui să facă obiectul prezentului regulament în cazul în care activitățile de prelucrare au legătură cu oferirea de bunuri sau servicii unor astfel de persoane vizate, indiferent dacă acestea sunt sau nu legate de o plată. Pentru a determina dacă un astfel de operator sau o astfel

de persoană împuternicită de operator oferă bunuri sau servicii unor persoane vizate care se află pe teritoriul Uniunii, ar trebui să se stabilească dacă reiese că operatorul sau persoana împuternicită de operator intenționează să furnizeze servicii persoanelor vizate din unul sau mai multe state membre din Uniune. Întrucât simplul fapt că există acces la un site al operatorului, al persoanei împuternicite de operator sau al unui intermediar în Uniune, că este disponibilă o adresă de e-mail și alte date de contact sau că este utilizată o limbă folosită în general în țara terță în care operatorul își are sediul este insuficient pentru a confirma o astfel de intenție, factori precum utilizarea unei limbi sau a unei monede utilizate în general în unul sau mai multe state membre cu posibilitatea de a comanda bunuri și servicii în respectiva limbă sau menționarea unor clienți sau utilizatori care se află pe teritoriul Uniunii pot conduce la concluzia că operatorul intenționează să ofere bunuri sau servicii unor persoane vizate în Uniune.(24) Prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Uniunii de către un operator sau o persoană împuternicită de acesta care nu își are sediul în Uniune ar trebui, de asemenea, să facă obiectul prezentului regulament în cazul în care este legată de monitorizarea comportamentului unor astfel de persoane vizate, în măsura în care acest comportament se manifestă pe teritoriul Uniunii. Pentru a se determina dacă o activitate de prelucrare poate fi considerată ca "monitorizare a comportamentului" persoanelor vizate, ar trebui să se stabilească dacă persoanele fizice sunt urmărite pe internet, inclusiv posibila utilizare ulterioară a unor tehnici de prelucrare a datelor cu caracter personal care constau în crearea unui profil al unei persoane fizice, în special în scopul de a lua decizii cu privire la aceasta sau de a analiza sau de a face previziuni referitoare la preferințele personale, comportamentele și atitudinile acesteia.(25) În cazul în care dreptul unui stat membru se aplică în temeiul dreptului internațional public, prezentul regulament ar trebui să se aplice, de asemenea, unui operator care nu este stabilit în Uniune, ci, de exemplu, într-o misiune diplomatică sau într-un oficiu consular al unui stat membru.(26) Principiile protecției datelor ar trebui să se aplice oricărei informații referitoare la o persoană fizică identificată sau identificabilă. Datele cu caracter personal care au fost supuse pseudonimizării, care ar putea fi atribuite unei persoane fizice prin utilizarea de informații suplimentare, ar trebui considerate informații referitoare la o persoană fizică identificabilă. Pentru a se determina dacă o persoană fizică este identificabilă, ar trebui să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană, în scopul identificării, în mod direct sau indirect, a persoanei fizice respective. Pentru a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace pentru identificarea persoanei fizice, ar trebui luați în considerare toți factorii obiectivi, precum costurile și intervalul de timp necesare pentru identificare, ținându-se seama atât de tehnologia disponibilă la momentul

prelucrării, cât și de dezvoltarea tehnologică. Principiile protecției datelor ar trebui, prin urmare, să nu se aplice informațiilor anonime, adică informațiilor care nu sunt legate de o persoană fizică identificată sau identificabilă sau datelor cu caracter personal care sunt anonimizate astfel încât persoana vizată nu este sau nu mai este identificabilă. Prin urmare, prezentul regulament nu se aplică prelucrării unor astfel de informații anonime, inclusiv în cazul în care acestea sunt utilizate în scopuri statistice sau de cercetare.(27) Prezentul regulament nu se aplică datelor cu caracter personal referitoare la persoane decedate. Statele membre pot să prevadă norme privind prelucrarea datelor cu caracter personal referitoare la persoane decedate.(28) Aplicarea pseudonimizării datelor cu caracter personal poate reduce riscurile pentru persoanele vizate și poate ajuta operatorii și persoanele împuternicite de aceștia să își îndeplinească obligațiile de protecție a datelor. Introducerea explicită a conceptului de "pseudonimizare" în prezentul regulament nu este destinată să împiedice alte eventuale măsuri de protecție a datelor.(29) Pentru a crea stimulente pentru aplicarea pseudonimizării atunci când sunt prelucrate date cu caracter personal, ar trebui să fie posibile măsuri de pseudonimizare, permițând în același timp analiza generală, în cadrul aceluiași operator atunci când operatorul a luat măsurile tehnice și organizatorice necesare pentru a se asigura că prezentul regulament este pus în aplicare în ceea ce privește respectiva prelucrare a datelor și că informațiile suplimentare pentru atribuirea datelor cu caracter personal unei anumite persoane vizate sunt păstrate separat. Operatorul care prelucrează datele cu caracter personal ar trebui să indice persoanele autorizate din cadrul aceluiași operator.(30) Persoanele fizice pot fi asociate cu identificatorii online furnizați de dispozitivele, aplicațiile, instrumentele și protocoalele lor, cum ar fi adresele IP, identificatorii cookie sau alți identificatori precum etichetele de identificare prin frecvențe radio. Aceștia pot lăsa urme care, în special atunci când sunt combinate cu identificatori unici și alte informații primite de servere, pot fi utilizate pentru crearea de profiluri ale persoanelor fizice și pentru identificarea lor.(31) Autoritățile publice cărora le sunt divulgate date cu caracter personal în conformitate cu o obligație legală în vederea exercitării funcției lor oficiale, cum ar fi autoritățile fiscale și vamale, unitățile de investigare financiară, autoritățile administrative independente sau autoritățile piețelor financiare responsabile de reglementarea și supravegherea piețelor titlurilor de valoare, nu ar trebui să fie considerate destinatari în cazul în care primesc date cu caracter personal care sunt necesare pentru efectuarea unei anumite anchete de interes general, în conformitate cu dreptul Uniunii sau cel al statelor membre. Cererile de divulgare trimise de autoritățile publice ar trebui să fie întotdeauna prezentate în scris, motivate și ocazionale și nu ar trebui să se refere la un sistem de evidență în totalitate sau să conducă la interconectarea sistemelor de evidență. Prelucrarea datelor cu caracter personal de către

autoritățile publice respective ar trebui să respecte normele aplicabile în materie de protecție a datelor în conformitate cu scopurile prelucrării.(32) Consimțământul ar trebui acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declarație făcută în scris, inclusiv în format electronic, sau verbal. Acesta ar putea include bifarea unei căsuțe atunci când persoana vizitează un site, alegerea parametrilor tehnici pentru serviciile societății informaționale sau orice altă declarație sau acțiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu ar trebui să constituie un consimțământ. Consimțământul ar trebui să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul ar trebui dat pentru toate scopurile prelucrării. În cazul în care consimțământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară și concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimțământul.(33) Adesea nu este posibil, în momentul colectării datelor cu caracter personal, să se identifice pe deplin scopul prelucrării datelor în scopuri de cercetare științifică. Din acest motiv, persoanelor vizate ar trebui să li se permită să își exprime consimțământul pentru anumite domenii ale cercetării științifice atunci când sunt respectate standardele etice recunoscute pentru cercetarea științifică. Persoanele vizate ar trebui să aibă posibilitatea de a-și exprima consimțământul doar pentru anumite domenii de cercetare sau părți ale proiectelor de cercetare în măsura permisă de scopul preconizat.(34) Datele genetice ar trebui definite drept date cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care rezultă în urma unei analize a unei mostre de material biologic al persoanei fizice în cauză, în special a unei analize cromozomiale, a unei analize a acidului dezoxiribonucleic (ADN) sau a acidului ribonucleic (ARN) sau a unei analize a oricărui alt element ce permite obținerea unor informații echivalente.(35) Datele cu caracter personal privind sănătatea ar trebui să includă toate datele având legătură cu starea de sănătate a persoanei vizate care dezvăluie informații despre starea de sănătate fizică sau mentală trecută, prezentă sau viitoare a persoanei vizate. Acestea includ informații despre persoana fizică colectate în cadrul înscrierii acesteia la serviciile de asistență medicală sau în cadrul acordării serviciilor respective persoanei fizice în cauză, astfel cum sunt menționate în [Directiva 2011/24/UE](#) a Parlamentului European și a Consiliului \*9); un număr, un simbol sau un semn distinctiv atribuit unei persoane fizice pentru identificarea singulară a acesteia în scopuri medicale; informații rezultate din testarea sau

examinarea unei părți a corpului sau a unei substanțe corporale, inclusiv din date genetice și eșantioane de material biologic; precum și orice informații privind, de exemplu, o boală, un handicap, un risc de îmbolnăvire, istoricul medical, tratamentul clinic sau starea fiziologică sau biomedicală a persoanei vizate, indiferent de sursa acestora, ca de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro.(36) Sediul principal al unui operator în Uniune ar trebui să fie locul în care se află administrația centrală a acestuia în Uniune, cu excepția cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului în Uniune. În acest caz, acesta din urmă ar trebui considerat drept sediul principal. Sediul principal al unui operator în Uniune ar trebui să fie determinat conform unor criterii obiective și ar trebui să implice exercitarea efectivă și reală a unor activități de gestionare care să determine principalele decizii cu privire la scopurile și mijloacele de prelucrare în cadrul unor înțelegeri stabile. Acest criteriu nu ar trebui să depindă de realizarea prelucrării datelor cu caracter personal în locul respectiv. Prezența și utilizarea mijloacelor tehnice și a tehnologiilor de prelucrare a datelor cu caracter personal sau activitățile de prelucrare nu constituie un sediu principal și, prin urmare, nu sunt criteriul determinant în acest sens. Sediul principal al persoanei împuternicite de operator ar trebui să fie locul în care se află administrația centrală a acestuia în Uniune sau, în cazul în care nu are o administrație centrală în Uniune, locul în care se desfășoară principalele activități de prelucrare în Uniune. În cazurile care implică atât operatorul, cât și persoana împuternicită de operator, autoritatea de supraveghere principală competentă ar trebui să rămână autoritatea de supraveghere a statului membru în care operatorul își are sediul principal, dar autoritatea de supraveghere a persoanei împuternicite de operator ar trebui considerată ca fiind o autoritate de supraveghere vizată și acea autoritate de supraveghere ar trebui să participe la procedura de cooperare prevăzută de prezentul regulament. În orice caz, autoritățile de supraveghere ale statului membru sau ale statelor membre în care persoana împuternicită de operator are unul sau mai multe sedii nu ar trebui considerate ca fiind autorități de supraveghere vizate în cazul în care proiectul de decizie nu se referă decât la operator. În cazul în care prelucrarea este efectuată de un grup de întreprinderi, sediul principal al întreprinderii care exercită controlul ar trebui considerat drept sediul principal al grupului de întreprinderi, cu excepția cazului în care scopurile și mijloacele aferente prelucrării sunt stabilite de o altă întreprindere.(37) Un grup de întreprinderi ar trebui să cuprindă o întreprindere care exercită controlul și întreprinderile controlate de aceasta, în cadrul căruia întreprinderea care exercită controlul ar trebui să fie întreprinderea care poate exercita o influență dominantă asupra celorlalte întreprinderi, de exemplu în temeiul proprietății, al participării financiare sau al regulilor care o reglementează sau

al competenței de a pune în aplicare norme în materie de protecție a datelor cu caracter personal. O întreprindere care controlează prelucrarea datelor cu caracter personal în întreprinderile sale afiliate ar trebui considerată, împreună cu acestea din urmă, drept "grup de întreprinderi".(38) Copiii au nevoie de o protecție specifică a datelor lor cu caracter personal, întrucât pot fi mai puțin conștienți de riscurile, consecințele, garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal. Această protecție specifică ar trebui să se aplice în special utilizării datelor cu caracter personal ale copiilor în scopuri de marketing sau pentru crearea de profiluri de personalitate sau de utilizator și la colectarea datelor cu caracter personal privind copiii în momentul utilizării serviciilor oferite direct copiilor. Consimțământul titularului răspunderii părintești nu ar trebui să fie necesar în contextul serviciilor de prevenire sau consiliere oferite direct copiilor.(39) Orice prelucrare de date cu caracter personal ar trebui să fie legală și echitabilă. Ar trebui să fie transparent pentru persoanele fizice că sunt colectate, utilizate, consultate sau prelucrate în alt mod datele cu caracter personal care le privesc și în ce măsură datele cu caracter personal sunt sau vor fi prelucrate. Principiul transparenței prevede că orice informații și comunicări referitoare la prelucrarea respectivelor date cu caracter personal sunt ușor accesibile și ușor de înțeles și că se utilizează un limbaj simplu și clar. Acest principiu se referă în special la informarea persoanelor vizate privind identitatea operatorului și scopurile prelucrării, precum și la oferirea de informații suplimentare, pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoanele fizice vizate și dreptul acestora de a li se confirma și comunica datele cu caracter personal care le privesc care sunt prelucrate. Persoanele fizice ar trebui informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal și cu privire la modul în care să își exercite drepturile în legătură cu prelucrarea. În special, scopurile specifice în care datele cu caracter personal sunt prelucrate ar trebui să fie explicite și legitime și să fie determinate la momentul colectării datelor respective. Datele cu caracter personal ar trebui să fie adecvate, relevante și limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Aceasta necesită, în special, asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum. Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace. În vederea asigurării faptului că datele cu caracter personal nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ștergere sau revizuirea periodică. Ar trebui să fie luate toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau șterse. Datele cu caracter personal ar trebui prelucrate într-un mod care să asigure în mod adecvat securitatea și confidențialitatea acestora, inclusiv în scopul

prevenirii accesului neautorizat la acestea sau utilizarea neautorizată a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare.(40) Pentru ca prelucrarea datelor cu caracter personal să fie legală, aceasta ar trebui efectuată pe baza consimțământului persoanei vizate sau în temeiul unui alt motiv legitim, prevăzut de lege, fie în prezentul regulament, fie în alt act din dreptul Uniunii sau din dreptul intern, după cum se prevede în prezentul regulament, inclusiv necesitatea respectării obligațiilor legale la care este supus operatorul sau necesitatea de a executa un contract la care persoana vizată este parte sau pentru a parcurge etapele premergătoare încheierii unui contract, la solicitarea persoanei vizate.(41) Ori de câte ori prezentul regulament face trimitere la un temei juridic sau la o măsură legislativă, aceasta nu necesită neapărat un act legislativ adoptat de către un parlament, fără a aduce atingere cerințelor care decurg din ordinea constituțională a statului membru în cauză. Cu toate acestea, un astfel de temei juridic sau o astfel de măsură legislativă ar trebui să fie clară și precisă, iar aplicarea acesteia ar trebui să fie previzibilă pentru persoanele vizate de aceasta, în conformitate cu jurisprudența Curții de Justiție a Uniunii Europene ("Curtea de Justiție") și a Curții Europene a Drepturilor Omului.(42) În cazul în care prelucrarea se bazează pe consimțământul persoanei vizate, operatorul ar trebui să fie în măsură să demonstreze faptul că persoana vizată și-a dat consimțământul pentru operațiunea de prelucrare. În special, în contextul unei declarații scrise cu privire la un alt aspect, garanțiile ar trebui să asigure că persoana vizată este conștientă de faptul că și-a dat consimțământul și în ce măsură a făcut acest lucru. În conformitate cu [Directiva 93/13/CEE](#) a Consiliului \*10), ar trebui furnizată o declarație de consimțământ formulată în prealabil de către operator, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, iar această declarație nu ar trebui să conțină clauze abuzive. Pentru ca acordarea consimțământului să fie în cunoștință de cauză, persoana vizată ar trebui să fie la curent cel puțin cu identitatea operatorului și cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal. Consimțământul nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată.(43) Pentru a garanta faptul că a fost acordat în mod liber, consimțământul nu ar trebui să constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal în cazul particular în care există un dezechilibru evident între persoana vizată și operator, în special în cazul în care operatorul este o autoritate publică, iar acest lucru face improbabilă acordarea consimțământului în mod liber în toate circumstanțele aferente respectivei situații particulare. Consimțământul este considerat a nu fi acordat în mod liber în cazul în care aceasta nu permite să se acorde consimțământul separat pentru diferitele operațiuni de prelucrare a datelor cu caracter personal, deși

acest lucru este adecvat în cazul particular, sau dacă executarea unui contract, inclusiv furnizarea unui serviciu, este condiționată de consimțământ, în ciuda faptului că consimțământul în cauză nu este necesar pentru executarea contractului.(44) Prelucrarea ar trebui să fie considerată legală în cazul în care este necesară în cadrul unui contract sau în vederea încheierii unui contract.(45) În cazul în care prelucrarea este efectuată în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice, prelucrarea ar trebui să aibă un temei în dreptul Uniunii sau în dreptul intern. Prezentul regulament nu impune existența unei legi specifice pentru fiecare prelucrare în parte. Poate fi suficientă o singură lege drept temei pentru mai multe operațiuni de prelucrare efectuate în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice. De asemenea, ar trebui ca scopul prelucrării să fie stabilit în dreptul Uniunii sau în dreptul intern. Mai mult decât atât, dreptul respectiv ar putea să specifice condițiile generale ale prezentului regulament care reglementează legalitatea prelucrării datelor cu caracter personal, să determine specificațiile pentru stabilirea operatorului, a tipului de date cu caracter personal care fac obiectul prelucrării, a persoanelor vizate, a entităților cărora le pot fi divulgate datele cu caracter personal, a limitărilor în funcție de scop, a perioadei de stocare și a altor măsuri pentru a garanta o prelucrare legală și echitabilă. De asemenea, ar trebui să se stabilească în dreptul Uniunii sau în dreptul intern dacă operatorul care îndeplinește o sarcină care servește unui interes public sau care face parte din exercitarea autorității publice ar trebui să fie o autoritate publică sau o altă persoană fizică sau juridică guvernată de dreptul public sau, atunci când motive de interes public justifică acest lucru, inclusiv în scopuri medicale, precum sănătatea publică și protecția socială, precum și gestionarea serviciilor de asistență medicală, de dreptul privat, cum ar fi o asociație profesională.(46) Prelucrarea datelor cu caracter personal ar trebui, de asemenea, să fie considerată legală în cazul în care este necesară în scopul asigurării protecției unui interes care este esențial pentru viața persoanei vizate sau pentru viața unei alte persoane fizice. Prelucrarea datelor cu caracter personal care are drept temei interesele vitale ale unei alte persoane fizice ar trebui efectuată numai în cazul în care prelucrarea nu se poate baza în mod evident pe un alt temei juridic. Unele tipuri de prelucrare pot servi atât unor motive importante de interes public, cât și intereselor vitale ale persoanei vizate, de exemplu în cazul în care prelucrarea este necesară în scopuri umanitare, inclusiv în vederea monitorizării unei epidemii și a răspândirii acesteia sau în situații de urgențe umanitare, în special în situații de dezastre naturale sau provocate de om.(47) Interesele legitime ale unui operator, inclusiv cele ale unui operator

căruia îi pot fi divulgate datele cu caracter personal sau ale unei terțe părți, pot constitui un temei juridic pentru prelucrare, cu condiția să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate, luând în considerare așteptările rezonabile ale persoanelor vizate bazate pe relația acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relație relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia. În orice caz, existența unui interes legitim ar necesita o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată poate preconiza în mod rezonabil, în momentul și în contextul colectării datelor cu caracter personal, posibilitatea prelucrării în acest scop. Interesele și drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date atunci când datele cu caracter personal sunt prelucrate în circumstanțe în care persoanele vizate nu preconizează în mod rezonabil o prelucrare ulterioară. Întrucât legiuitorul trebuie să furnizeze temeiul juridic pentru prelucrarea datelor cu caracter personal de către autoritățile publice, temeiul juridic respectiv nu ar trebui să se aplice prelucrării de către autoritățile publice în îndeplinirea sarcinilor care le revin. Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor constituie, de asemenea, un interes legitim al operatorului de date în cauză. Prelucrarea de date cu caracter personal care are drept scop marketingul direct poate fi considerată ca fiind desfășurată pentru un interes legitim.<sup>(48)</sup> Operatorii care fac parte dintr-un grup de întreprinderi sau instituții afiliate unui organism central pot avea un interes legitim de a transmite date cu caracter personal în cadrul grupului de întreprinderi în scopuri administrative interne, inclusiv în scopul prelucrării datelor cu caracter personal ale clienților sau angajaților. Principiile generale ale transferului de date cu caracter personal, în cadrul unui grup de întreprinderi, către o întreprindere situată într-o țară terță rămân neschimbate.<sup>(49)</sup> Prelucrarea datelor cu caracter personal în măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor, și anume capacitatea unei rețele sau a unui sistem de informații de a face față, la un anumit nivel de încredere, evenimentelor accidentale sau acțiunilor ilegale sau rău intenționate care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor cu caracter personal stocate sau transmise, precum și securitatea serviciilor conexe oferite de aceste rețele și sisteme, sau accesibile prin intermediul acestora, de către autoritățile publice, echipele de intervenție în caz de urgență informatică, echipele de intervenție în cazul producerii unor incidente care afectează securitatea informatică, furnizorii de rețele și servicii de comunicații electronice, precum și de către furnizorii de servicii și tehnologii de securitate, constituie un interes legitim al operatorului de date în cauză. Acesta ar putea include, de exemplu, prevenirea accesului neautorizat la rețelele de

comunicații electronice și a difuzării de coduri dăunătoare și oprirea atacurilor de "blocare a serviciului", precum și prevenirea daunelor aduse calculatoarelor și sistemelor de comunicații electronice.(50) Prelucrarea datelor cu caracter personal în alte scopuri decât scopurile pentru care datele cu caracter personal au fost inițial colectate ar trebui să fie permisă doar atunci când prelucrarea este compatibilă cu scopurile respective pentru care datele cu caracter personal au fost inițial colectate. În acest caz nu este necesar un temei juridic separat de cel pe baza căruia a fost permisă colectarea datelor cu caracter personal. În cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul, dreptul Uniunii sau dreptul intern poate stabili și specifica sarcinile și scopurile pentru care prelucrarea ulterioară ar trebui considerată a fi compatibilă și legală. Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ar trebui considerată ca reprezentând operațiuni de prelucrare legale compatibile. Temeiul juridic prevăzut în dreptul Uniunii sau în dreptul intern pentru prelucrarea datelor cu caracter personal poate constitui, de asemenea, un temei juridic pentru prelucrarea ulterioară. Pentru a stabili dacă scopul prelucrării ulterioare este compatibil cu scopul pentru care au fost colectate inițial datele cu caracter personal, operatorul, după ce a îndeplinit toate cerințele privind legalitatea prelucrării inițiale, ar trebui să țină seama, printre altele, de orice legătură între respectivele scopuri și scopurile prelucrării ulterioare preconizate, de contextul în care au fost colectate datele cu caracter personal, în special de așteptările rezonabile ale persoanelor vizate, bazate pe relația lor cu operatorul, în ceea ce privește utilizarea ulterioară a datelor, de natura datelor cu caracter personal, de consecințele prelucrării ulterioare preconizate asupra persoanelor vizate, precum și de existența garanțiilor corespunzătoare atât în cadrul operațiunilor de prelucrare inițiale, cât și în cadrul operațiunilor de prelucrare ulterioare preconizate. În cazul în care persoana vizată și-a dat consimțământul sau prelucrarea se bazează pe dreptul Uniunii sau pe dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja, în special, obiective importante de interes public general, operatorul ar trebui să aibă posibilitatea de a prelucra în continuare datele cu caracter personal, indiferent de compatibilitatea scopurilor. În orice caz, aplicarea principiilor stabilite de prezentul regulament și, în special, informarea persoanei vizate cu privire la aceste alte scopuri și la drepturile sale, inclusiv dreptul la opoziție, ar trebui să fie garantate. Indicarea unor posibile infracțiuni sau amenințări la adresa siguranței publice de către operator și transmiterea către o autoritate competentă a datelor cu caracter personal relevante în cazuri individuale sau în mai multe cazuri legate de aceeași infracțiune sau de aceleași amenințări la adresa siguranței publice ar trebui considerată ca fiind

în interesul legitim urmărit de operator. Cu toate acestea, o astfel de transmitere în interesul legitim al operatorului sau prelucrarea ulterioară a datelor cu caracter personal ar trebui interzisă în cazul în care prelucrarea nu este compatibilă cu o obligație legală, profesională sau cu o altă obligație de păstrare a confidențialității.(51) Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale necesită o protecție specifică, deoarece contextul prelucrării acestora ar putea genera riscuri considerabile la adresa drepturilor și libertăților fundamentale. Aceste date cu caracter personal ar trebui să includă datele cu caracter personal care dezvăluie originea rasială sau etnică, utilizarea termenului "origine rasială" în prezentul regulament neimplicând o acceptare de către Uniune a teoriilor care urmăresc să stabilească existența unor rase umane separate. Prelucrarea fotografiilor nu ar trebui să fie considerată în mod sistematic ca fiind o prelucrare de categorii speciale de date cu caracter personal, întrucât fotografiile intră sub incidența definiției datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice. Asemenea date cu caracter personal nu ar trebui prelucrate, cu excepția cazului în care prelucrarea este permisă în cazuri specifice prevăzute de prezentul regulament, ținând seama de faptul că dreptul statelor membre poate prevedea dispoziții specifice cu privire la protecția datelor în scopul adaptării aplicării normelor din prezentul regulament în vederea respectării unei obligații legale sau a îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul. Pe lângă cerințele specifice pentru o astfel de prelucrare, ar trebui să se aplice principiile generale și alte norme prevăzute de prezentul regulament, în special în ceea ce privește condițiile pentru prelucrarea legală. Ar trebui prevăzute în mod explicit derogări de la interdicția generală de prelucrare a acestor categorii speciale de date cu caracter personal, printre altele atunci când persoana vizată își dă consimțământul explicit sau în ceea ce privește nevoile specifice în special atunci când prelucrarea este efectuată în cadrul unor activități legitime de către anumite asociații sau fundații al căror scop este de a permite exercitarea libertăților fundamentale.(52) Derogarea de la interdicția privind prelucrarea categoriilor speciale de date cu caracter personal ar trebui să fie permisă, de asemenea, în cazul în care dreptul Uniunii sau dreptul intern prevede acest lucru și ar trebui să facă obiectul unor garanții adecvate, astfel încât să fie protejate datele cu caracter personal și alte drepturi fundamentale, atunci când acest lucru se justifică din motive de interes public, în special în cazul prelucrării datelor cu caracter personal în domeniul legislației privind ocuparea forței de muncă, protecția socială, inclusiv pensiile, precum și în scopuri de securitate, supraveghere și alertă în materie de sănătate, pentru prevenirea sau controlul bolilor transmisibile și a altor

amenințări grave la adresa sănătății. Această derogare poate fi acordată în scopuri medicale, inclusiv sănătatea publică și gestionarea serviciilor de asistență medicală, în special în vederea asigurării calității și eficienței din punctul de vedere al costurilor ale procedurilor utilizate pentru soluționarea cererilor de prestații și servicii în cadrul sistemului de asigurări de sănătate, sau în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. De asemenea, prelucrarea unor asemenea date cu caracter personal ar trebui permisă, printr-o derogare, atunci când este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiție, indiferent dacă are loc în cadrul unei proceduri în fața unei instanțe sau în cadrul unei proceduri administrative sau a unei proceduri extrajudiciare.(53) Categoriile speciale de date cu caracter personal care necesită un nivel mai ridicat de protecție ar trebui prelucrate doar în scopuri legate de sănătate atunci când este necesar pentru realizarea acestor scopuri în beneficiul persoanelor fizice și al societății în general, în special în contextul gestionării serviciilor și sistemelor de sănătate sau de asistență socială, inclusiv prelucrarea acestor date de către autoritățile de management și de către autoritățile centrale naționale din domeniul sănătății în scopul controlului calității, furnizării de informații de gestiune și al supravegherii generale a sistemului de sănătate sau de asistență socială la nivel național și local, precum și în contextul asigurării continuității asistenței medicale sau sociale și a asistenței medicale transfrontaliere ori în scopuri de securitate, supraveghere și alertă în materie de sănătate ori în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice în temeiul dreptului Uniunii sau al dreptului intern, care trebuie să urmărească un obiectiv de interes public, precum și în cazul studiilor realizate în interes public în domeniul sănătății publice. Prin urmare, prezentul regulament ar trebui să prevadă condiții armonizate pentru prelucrarea categoriilor speciale de date cu caracter personal privind sănătatea, în ceea ce privește nevoile specifice, în special atunci când prelucrarea acestor date este efectuată în anumite scopuri legate de sănătate de către persoane care fac obiectul unei obligații legale de a păstra secretul profesional. Dreptul Uniunii sau dreptul intern ar trebui să prevadă măsuri specifice și adecvate pentru a proteja drepturile fundamentale și datele cu caracter personal ale persoanelor fizice. Statele membre ar trebui să aibă posibilitatea de a menține sau de a introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea. Totuși, acest lucru nu ar trebui să împiedice libera circulație a datelor cu caracter personal în cadrul Uniunii atunci când aceste condiții se aplică prelucrării transfrontaliere a unor astfel de date.(54) Prelucrarea categoriilor speciale de date cu caracter personal poate fi necesară din motive de interes public în domeniile sănătății publice, fără consimțământul persoanei vizate. O astfel de prelucrare ar trebui condiționată

de măsuri adecvate și specifice destinate să protejeze drepturile și libertățile persoanelor fizice. În acest context, conceptul de "sănătate publică" ar trebui interpretat astfel cum este definit în [Regulamentul \(CE\) nr. 1338/2008](#) al Parlamentului European și al Consiliului \*11), și anume toate elementele referitoare la sănătate și anume starea de sănătate, inclusiv morbiditatea sau handicapul, factorii determinanți care au efect asupra stării de sănătate, necesitățile în domeniul asistenței medicale, resursele alocate asistenței medicale, furnizarea asistenței medicale și asigurarea accesului universal la aceasta, precum și cheltuielile și sursele de finanțare în domeniul sănătății și cauzele mortalității. Această prelucrare a datelor privind sănătatea din motive de interes public nu ar trebui să ducă la prelucrarea acestor date în alte scopuri de către părți terțe, cum ar fi angajatorii sau societățile de asigurări și băncile.(55) În plus, prelucrarea datelor cu caracter personal de către autoritățile publice în vederea realizării obiectivelor prevăzute de dreptul constituțional sau de dreptul internațional public, ale asociațiilor religioase recunoscute oficial se efectuează din motive de interes public.(56) În cazul în care, în cadrul activităților electorale, funcționarea sistemului democratic necesită, într-un stat membru, ca partidele politice să colecteze date cu caracter personal privind opiniile politice ale persoanelor, prelucrarea unor astfel de date poate fi permisă din motive de interes public, cu condiția să se prevadă garanțiile corespunzătoare.(57) Dacă datele cu caracter personal prelucrate de un operator nu îi permit acestuia să identifice o persoană fizică, operatorul de date nu ar trebui să aibă obligația de a obține informații suplimentare în vederea identificării persoanei vizate, cu unicul scop de a respecta oricare dintre dispozițiile prezentului regulament. Cu toate acestea, operatorul nu ar trebui să refuze să preia informațiile suplimentare furnizate de persoana vizată cu scopul de a sprijini exercitarea drepturilor acesteia. Identificarea ar trebui să includă identificarea digitală a unei persoane vizate, de exemplu prin mecanisme de autentificare precum aceleași acreditări utilizate de către persoana vizată pentru a accesa serviciile online oferite de operatorul de date.(58) Principiul transparenței prevede că orice informații care se adresează publicului sau persoanei vizate să fie concise, ușor accesibile și ușor de înțeles și să se utilizeze un limbaj simplu și clar, precum și vizualizare acolo unde este cazul. Aceste informații ar putea fi furnizate în format electronic, de exemplu atunci când sunt adresate publicului, prin intermediul unui site. Acest lucru este important în special în situații în care datorită multitudinii actorilor și a complexității, din punct de vedere tehnologic, a practicii, este dificil ca persoana vizată să știe și să înțeleagă dacă datele cu caracter personal care o privesc sunt colectate, de către cine și în ce scop, cum este cazul publicității online. Întrucât copiii necesită o protecție specifică, orice informații și orice comunicare, în cazul în care prelucrarea vizează un copil, ar trebui să fie exprimate într-un limbaj simplu și clar, astfel încât copilul să îl poată înțelege cu ușurință.(59) Ar trebui să fie

prevăzute modalități de facilitare a exercitării de către persoana vizată a drepturilor care îi sunt conferite prin prezentul regulament, inclusiv mecanismele prin care aceasta poate solicita și, dacă este cazul, obține, în mod gratuit, în special, acces la datele cu caracter personal, precum și rectificarea sau ștergerea acestora, și exercitarea dreptului la opoziție. Operatorul ar trebui să ofere, de asemenea, modalități de introducere a cererilor pe cale electronică, mai ales în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice. Operatorul ar trebui să aibă obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate și cel târziu în termen de o lună și, în cazul în care nu intenționează să se conformeze respectivele cereri, să motiveze acest refuz.(60) Conform principiilor prelucrării echitabile și transparente, persoana vizată este informată cu privire la existența unei operațiuni de prelucrare și la scopurile acesteia. Operatorul ar trebui să furnizeze persoanei vizate orice informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă, ținând seama de circumstanțele specifice și de contextul în care sunt prelucrate datele cu caracter personal. În plus, persoana vizată ar trebui informată cu privire la crearea de profiluri, precum și la consecințele acesteia. Atunci când datele cu caracter personal sunt colectate de la persoana vizată, aceasta ar trebui informată, de asemenea, dacă are obligația de a furniza datele cu caracter personal și care sunt consecințele în cazul unui refuz. Aceste informații pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea ar trebui să poată fi citite automat.(61) Informațiile în legătură cu prelucrarea datelor cu caracter personal referitoare la persoana vizată ar trebui furnizate acesteia la momentul colectării de la persoana vizată sau, în cazul în care datele cu caracter personal sunt obținute din altă sursă, într-o perioadă rezonabilă, în funcție de circumstanțele cazului. În cazul în care datele cu caracter personal pot fi divulgate în mod legitim unui alt destinatar, persoana vizată ar trebui informată atunci când datele cu caracter personal sunt divulgate pentru prima dată destinatarului. În cazul în care operatorul intenționează să prelucreze datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul ar trebui să furnizeze persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și alte informații necesare. În cazul în care originea datelor cu caracter personal nu a putut fi comunicată persoanei vizate din cauză că au fost utilizate surse diverse, informațiile generale ar trebui furnizate.(62) Cu toate acestea, nu este necesară impunerea obligației de a furniza informații în cazul în care persoana vizată deține deja informațiile, în cazul în care înregistrarea sau divulgarea datelor cu caracter personal este prevăzută în mod expres de lege sau în cazul în care informarea persoanei vizate se dovedește imposibilă sau

ar implica eforturi disproporționate. Acesta din urmă ar putea fi cazul în special atunci când prelucrarea se efectuează în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. În această privință, ar trebui luate în considerare numărul persoanelor vizate, vechimea datelor și orice garanții adecvate adoptate.(63) O persoană vizată ar trebui să aibă drept de acces la datele cu caracter personal colectate care o privesc și ar trebui să își exercite acest drept cu ușurință și la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia. Acest lucru include dreptul persoanelor vizate de a avea acces la datele lor privind sănătatea, de exemplu datele din registrele lor medicale conținând informații precum diagnostice, rezultate ale examinărilor, evaluări ale medicilor curanți și orice tratament sau intervenție efectuată. Orice persoană vizată ar trebui, prin urmare, să aibă dreptul de a cunoaște și de a i se comunica în special scopurile în care sunt prelucrate datele, dacă este posibil perioada pentru care se prelucrează datele cu caracter personal, destinatarii datelor cu caracter personal, logica de prelucrare automată a datelor cu caracter personal și, cel puțin în cazul în care se bazează pe crearea de profiluri, consecințele unei astfel de prelucrări. Dacă acest lucru este posibil, operatorul de date ar trebui să poată furniza acces de la distanță la un sistem sigur, care să ofere persoanei vizate acces direct la datele sale cu caracter personal. Acest drept nu ar trebui să aducă atingere drepturilor sau libertăților altora, inclusiv secretului comercial sau proprietății intelectuale și, în special, drepturilor de autor care asigură protecția programelor software. Cu toate acestea, considerațiile de mai sus nu ar trebui să aibă drept rezultat refuzul de a furniza toate informațiile persoanei vizate. Atunci când operatorul prelucrează un volum mare de informații privind persoana vizată, operatorul ar trebui să poată solicita ca, înainte de a îi fi furnizate informațiile, persoana vizată să precizeze informațiile sau activitățile de prelucrare la care se referă cererea sa.(64) Operatorul ar trebui să ia toate măsurile rezonabile pentru a verifica identitatea unei persoane vizate care solicită acces la date, în special în contextul serviciilor online și al identificărilor online. Un operator nu ar trebui să rețină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacționeze la cereri potențiale.(65) O persoană vizată ar trebui să aibă dreptul la rectificarea datelor cu caracter personal care o privesc și "dreptul de a fi uitată", în cazul în care păstrarea acestor date încalcă prezentul regulament sau dreptul Uniunii sau dreptul intern sub incidența căruia intră operatorul. În special, persoanele vizate ar trebui să aibă dreptul ca datele lor cu caracter personal să fie șterse și să nu mai fie prelucrate, în cazul în care datele cu caracter personal nu mai sunt necesare pentru scopurile în care sunt colectate sau sunt prelucrate, în cazul în care persoanele vizate și-au retras consimțământul pentru prelucrare sau în cazul în care acestea se opun prelucrării datelor cu caracter personal care le privesc

sau în cazul în care prelucrarea datelor cu caracter personal ale acestora nu este conformă cu prezentul regulament. Acest drept este relevant în special în cazul în care persoana vizată și-a dat consimțământul când era copil și nu cunoștea pe deplin riscurile pe care le implică prelucrarea, iar ulterior dorește să elimine astfel de date cu caracter personal, în special de pe internet. Persoana vizată ar trebui să aibă posibilitatea de a-și exercita acest drept în pofida faptului că nu mai este copil. Cu toate acestea, păstrarea în continuare a datelor cu caracter personal ar trebui să fie legală în cazul în care este necesară pentru exercitarea dreptului la libertatea de exprimare și de informare, pentru respectarea unei obligații legale, pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul, din motive de interes public în domeniul sănătății publice, în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice sau pentru constatarea, exercitarea sau apărarea unui drept în instanță.(66) Pentru a se consolida "dreptul de a fi uitat" în mediul online, dreptul de ștergere ar trebui să fie extins astfel încât un operator care a făcut publice date cu caracter personal ar trebui să aibă obligația de a informa operatorii care prelucrează respectivele date cu caracter personal să șteargă orice linkuri către datele respective sau copii sau reproduceri ale acestora. În acest scop, operatorul în cauză ar trebui să ia măsuri rezonabile, ținând seama de tehnologia disponibilă și de mijloacele aflate la dispoziția lui, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal în ceea ce privește cererea persoanei vizate.(67) Metodele de restricționare a prelucrării de date cu caracter personal ar putea include, printre altele, mutarea temporară a datelor cu caracter personal selectate într-un alt sistem de prelucrare, sau anularea accesului utilizatorilor la datele selectate sau înlăturarea temporară a datelor publicate de pe un site. În ceea ce privește sistemele automatizate de evidență a datelor, restricționarea prelucrării ar trebui, în principiu, asigurată prin mijloace tehnice în așa fel încât datele cu caracter personal să nu facă obiectul unor operațiuni de prelucrare ulterioară și să nu mai poată fi schimbate. Faptul că prelucrarea datelor cu caracter personal este restricționată ar trebui indicat în mod clar în sistem.(68) Pentru a spori suplimentar controlul asupra propriilor date, persoana vizată ar trebui, în cazul în care datele cu caracter personal sunt prelucrate prin mijloace automate, să poată primi datele cu caracter personal care o privesc și pe care le-a furnizat unui operator, într-un format structurat, utilizat în mod curent, prelucrabil automat și interoperabil și să le poată transmite unui alt operator. Operatorii de date ar trebui să fie încurajați să dezvolte formate interoperabile care să permită portabilitatea datelor. Acest drept ar trebui să se aplice în cazul în care persoana vizată a furnizat datele cu caracter personal pe baza propriului consimțământ sau în cazul în care prelucrarea datelor este necesară pentru executarea unui contract. Acest drept nu ar

trebui să se aplice în cazul în care prelucrarea se bazează pe un alt temei juridic decât consimțământul sau contractul. Prin însăși natura sa, acest drept nu ar trebui exercitat împotriva operatorilor care prelucrează date cu caracter personal în cadrul exercitării funcțiilor lor publice. Acesta nu ar trebui să se aplice în special în cazul în care prelucrarea de date cu caracter personal este necesară în vederea respectării unei obligații legale căreia îi este supus operatorul sau în cazul îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea unei autorități 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 să creeze pentru operatori obligația de a adopta sau de a menține sisteme de prelucrare care să fie compatibile din punct de vedere tehnic. În cazul în care, într-un anumit set de date cu caracter personal, sunt implicate mai multe persoane vizate, dreptul de a primi datele cu caracter personal nu ar trebui să aducă atingere drepturilor și libertăților altor persoane vizate, în conformitate cu prezentul regulament. De asemenea, acest drept nu ar trebui să aducă atingere dreptului persoanei vizate de a obține ștergerea datelor cu caracter personal și limitărilor dreptului respectiv, astfel cum sunt prevăzute în prezentul regulament, și nu ar trebui, în special, să implice ștergerea acelor date cu caracter personal referitoare la persoana vizată care au fost furnizate de către aceasta în vederea executării unui contract, în măsura în care și atât timp cât datele respective sunt necesare pentru executarea contractului. Persoana vizată ar trebui să aibă dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul, dacă acest lucru este fezabil din punct de vedere tehnic.(69) În cazurile în care datele cu caracter personal ar putea fi prelucrate în mod legal deoarece prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul sau pe baza intereselor legitime ale unui operator sau ale unei părți terțe, o persoană vizată ar trebui să aibă totuși dreptul de a se opune prelucrării oricăror date cu caracter personal care se referă la situația sa particulară. Ar trebui să revină operatorului sarcina de a demonstra că interesele sale legitime și imperioase prevalează asupra intereselor sau a drepturilor și libertăților fundamentale ale persoanei vizate.(70) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de marketing direct, persoana vizată ar trebui să aibă dreptul de a se opune unei astfel de prelucrări, inclusiv creării de profiluri în măsura în care aceasta are legătură cu marketingul direct, indiferent dacă prelucrarea în cauză este cea inițială sau una ulterioară, în orice moment și în mod gratuit. Acest drept ar trebui adus în mod explicit în atenția persoanei vizate și prezentat în mod clar și separat de orice alte informații.(71) Persoana vizată ar trebui să aibă dreptul de a nu face obiectul unei decizii, care poate include o măsură, care evaluează aspecte personale referitoare la persoana vizată, care se bazează exclusiv pe prelucrarea

automată și care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă, cum ar fi refuzul automat al unei cereri de credit online sau practicile de recrutare pe cale electronică, fără intervenție umană. O astfel de prelucrare include "crearea de profiluri", care constă în orice formă de prelucrare automată a datelor cu caracter personal prin evaluarea aspectelor personale referitoare la o persoană fizică, în special în vederea analizării sau preconizării anumitor aspecte privind randamentul la locul de muncă al persoanei vizate, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările, atunci când aceasta produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă. Cu toate acestea, luarea de decizii pe baza unei astfel de prelucrări, inclusiv crearea de profiluri, ar trebui permisă în cazul în care este autorizată în mod expres în dreptul Uniunii sau în dreptul intern care se aplică operatorului, inclusiv în scopul monitorizării și prevenirii fraudei și a evaziunii fiscale, desfășurate în conformitate cu reglementările, standardele și recomandările instituțiilor Uniunii sau ale organismelor naționale de supraveghere, și în scopul asigurării securității și fiabilității unui serviciu oferit de operator sau în cazul în care este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator sau în cazul în care persoana vizată și-a dat în mod explicit consimțământul. În orice caz, o astfel de prelucrare ar trebui să facă obiectul unor garanții corespunzătoare, care ar trebui să includă o informare specifică a persoanei vizate și dreptul acesteia de a obține intervenție umană, de a-și exprima punctul de vedere, de a primi o explicație privind decizia luată în urma unei astfel de evaluări, precum și dreptul de a contesta decizia. O astfel de măsură nu ar trebui să se refere la un copil. Pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată, având în vedere circumstanțele specifice și contextul în care sunt prelucrate datele cu caracter personal, operatorul ar trebui să utilizeze proceduri matematice sau statistice adecvate pentru crearea de profiluri, să implementeze măsuri tehnice și organizatorice adecvate pentru a asigura în special faptul că factorii care duc la inexactități ale datelor cu caracter personal sunt corecți și că riscul de erori este redus la minimum, precum și să securizeze datele cu caracter personal într-un mod care să țină seama de pericolele potențiale la adresa intereselor și drepturilor persoanei vizate și care să prevină, printre altele, efectele discriminatorii împotriva persoanelor pe motiv de rasă sau origine etnică, opinii politice, religie sau convingeri, apartenență sindicală, caracteristici genetice, stare de sănătate sau orientare sexuală sau care să ducă la măsuri care să aibă astfel de efecte. Procesul decizional automatizat și crearea de profiluri pe baza unor categorii speciale de date cu caracter personal ar trebui permise numai în condiții specifice.(72) Crearea de profiluri este supusă normelor prezentului regulament care reglementează prelucrarea

datelor cu caracter personal, precum temeiurile juridice ale prelucrării sau principiile de protecție a datelor. Comitetul european pentru protecția datelor instituit prin prezentul regulament ("comitetul") ar trebui să poată emite orientări în acest context.(73) Dreptul Uniunii sau dreptul intern poate impune restricții în privința unor principii specifice, în privința dreptului de informare, a dreptului de acces la datele cu caracter personal și de rectificare sau ștergere a acestora, în privința dreptului la portabilitatea datelor, a dreptului la opoziție, a deciziilor bazate pe crearea de profiluri, precum și în privința comunicării unei încălcări a securității datelor cu caracter personal persoanei vizate și a anumitor obligații conexe ale operatorilor, în măsura în care acest lucru este necesar și proporțional într-o societate democratică pentru a se garanta siguranța publică, inclusiv protecția vieții oamenilor, în special ca răspuns la dezastre naturale sau provocate de om, prevenirea, investigarea și urmărirea penală a infracțiunilor sau executarea pedepselor, inclusiv protejarea împotriva amenințărilor la adresa siguranței publice sau împotriva încălcării eticii în cazul profesiilor reglementate și prevenirea acestora, alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, menținerea de registre publice din motive de interes public general, prelucrarea ulterioară a datelor cu caracter personal arhivate pentru a transmite informații specifice legate de comportamentul politic în perioada regimurilor fostelor state totalitare, protecția persoanei vizate sau a drepturilor și libertăților unor terți, inclusiv protecția socială, sănătatea publică și scopurile umanitare. Aceste restricții ar trebui să fie conforme cu cerințele prevăzute de cartă și de Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale.(74) Ar trebui să se stabilească responsabilitatea și răspunderea operatorului pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său. În special, operatorul ar trebui să fie obligat să implementeze măsuri adecvate și eficace și să fie în măsură să demonstreze conformitatea activităților de prelucrare cu prezentul regulament, inclusiv eficacitatea măsurilor. Aceste măsuri ar trebui să țină seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul pentru drepturile și libertățile persoanelor fizice.(75) Riscul pentru drepturile și libertățile persoanelor fizice, prezentând grade diferite de probabilitate de materializare și de gravitate, poate fi rezultatul unei prelucrări a datelor cu caracter personal care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care: prelucrarea poate conduce la discriminare, furt sau fraudă a identității, pierdere financiară, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional, inversarea neautorizată a pseudonimizării sau la orice alt dezavantaj semnificativ de natură economică sau socială; persoanele vizate ar putea fi private de drepturile și libertățile lor sau împiedicate să-și

exercite controlul asupra datelor lor cu caracter personal; datele cu caracter personal prelucrate sunt date care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența sindicală; sunt prelucrate date genetice, date privind sănătatea sau date privind viața sexuală sau privind condamnările penale și infracțiunile sau măsurile de securitate conexe; sunt evaluate aspecte de natură personală, în special analizarea sau previzionarea unor aspecte privind randamentul la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările, în scopul de a se crea sau de a se utiliza profiluri personale; sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale unor copii; sau prelucrarea implică un volum mare de date cu caracter personal și afectează un număr larg de persoane vizate.(76) Probabilitatea de a se materializa și gravitatea riscului pentru drepturile și libertățile persoanei vizate ar trebui să fie determinate în funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor cu caracter personal. Riscul ar trebui apreciat pe baza unei evaluări obiective prin care se stabilește dacă operațiunile de prelucrare a datelor prezintă un risc sau un risc ridicat.(77) Orientări pentru implementarea unor măsuri adecvate și pentru demonstrarea conformității de către operator sau persoana împuternicită de operator, mai ales în ceea ce privește identificarea riscului legat de prelucrare, evaluarea acestuia din punctul de vedere al originii, naturii, probabilității de a se materializa și al gravității, precum și identificarea bunelor practici pentru atenuarea riscului ar putea fi oferite în special prin coduri de conduită aprobate, certificări aprobate, orientări ale comitetului sau prin indicații furnizate de un responsabil cu protecția datelor. Comitetul poate, de asemenea, să emită orientări cu privire la operațiunile de prelucrare care sunt considerate puțin susceptibile de a genera un risc ridicat pentru drepturile și libertățile persoanelor fizice și să indice măsurile care se pot dovedi suficiente în asemenea cazuri pentru a aborda un astfel de risc.(78) Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare pentru a se asigura îndeplinirea cerințelor din prezentul regulament. Pentru a fi în măsură să demonstreze conformitatea cu prezentul regulament, operatorul ar trebui să adopte politici interne și să pună în aplicare măsuri care să respecte în special principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor. Astfel de măsuri ar putea consta, printre altele, în reducerea la minimum a prelucrării datelor cu caracter personal, pseudonimizarea acestor date cât mai curând posibil, transparența în ceea ce privește funcțiile și prelucrarea datelor cu caracter personal, abilitarea persoanei vizate să monitorizeze prelucrarea datelor, abilitarea operatorului să creeze elemente de siguranță și să le îmbunătățească. Atunci când elaborează, proiectează, selectează și utilizează

aplicații, servicii și produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează date cu caracter personal pentru a-și îndeplini rolul, producătorii acestor produse și furnizorii acestor servicii și aplicații ar trebui să fie încurajați să aibă în vedere dreptul la protecția datelor la momentul elaborării și proiectării unor astfel de produse, servicii și aplicații și, ținând cont de stadiul actual al dezvoltării, să se asigure că operatorii și persoanele împuternicite de operatori sunt în măsură să își îndeplinească obligațiile referitoare la protecția datelor. Principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor ar trebui să fie luate în considerare și în contextul licitațiilor publice. (79) Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și a persoanelor împuternicite de operator, inclusiv în ceea ce privește monitorizarea de către autoritățile de supraveghere și măsurile adoptate de acestea, necesită o atribuire clară a responsabilităților în temeiul prezentului regulament, inclusiv în cazul în care un operator stabilește scopurile și mijloacele prelucrării împreună cu alți operatori sau în cazul în care o operațiune de prelucrare este efectuată în numele unui operator. (80) Atunci când un operator sau o persoană împuternicită de operator care nu este stabilită în Uniune prelucrează date cu caracter personal ale unor persoane vizate care se află pe teritoriul Uniunii, iar activitățile sale de prelucrare au legătură cu oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată, sau cu monitorizarea comportamentului unor persoane vizate dacă acesta se manifestă în cadrul Uniunii, operatorul sau persoana împuternicită de operator ar trebui să desemneze un reprezentant, cu excepția cazului în care prelucrarea are caracter ocazional, nu include prelucrarea pe scară largă a unor categorii speciale de date cu caracter personal și nici prelucrarea de date referitoare la condamnări penale și la infracțiuni, și este puțin susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice, având în vedere natura, contextul, domeniul de aplicare și scopurile prelucrării, precum și a cazului în care operatorul este o autoritate publică sau un organism public. Reprezentantul ar trebui să acționeze în numele operatorului sau al persoanei împuternicite de operator, putând fi contactat de orice autoritate de supraveghere. Reprezentantul ar trebui desemnat în mod explicit, printr-un mandat scris al operatorului sau al persoanei împuternicite de operator, să acționeze în numele acestuia (acesteia) în ceea ce privește obligațiile lor în temeiul prezentului regulament. Desemnarea unui astfel de reprezentant nu aduce atingere responsabilității sau răspunderii operatorului sau a persoanei împuternicite de operator în temeiul prezentului regulament. Un astfel de reprezentant ar trebui să își îndeplinească sarcinile în conformitate cu mandatul primit de la operator sau de la persoana împuternicită de operator, inclusiv să coopereze cu autoritățile de supraveghere competente în ceea ce

privește orice acțiune întreprinsă pentru a asigura respectarea prezentului regulament. Reprezentantul desemnat ar trebui să fie supus unor proceduri de asigurare a respectării legii în cazul nerespectării prezentului regulament de către operator sau de către persoana împuternicită de operator.(81) Pentru a asigura respectarea cerințelor impuse de prezentul regulament în ceea ce privește prelucrarea care trebuie efectuată în numele operatorului de către persoana împuternicită de operator, atunci când atribuie activități de prelucrare unei persoane împuternicite de operator, acesta din urmă ar trebui să utilizeze numai persoane împuternicite care oferă garanții suficiente, în special în ceea ce privește cunoștințele de specialitate, fiabilitatea și resursele, pentru a implementa măsuri tehnice și organizatorice care îndeplinesc cerințele impuse de prezentul regulament, inclusiv pentru securitatea prelucrării. Aderarea de către persoana împuternicită de operator la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate fi utilizată drept element care să demonstreze respectarea obligațiilor de către operator. Efectuarea prelucrării de către o persoană împuternicită de un operator ar trebui să fie reglementată printr-un contract sau un alt tip de act juridic, în temeiul dreptului Uniunii sau al dreptului intern, care creează obligații pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopurile prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate, și ar trebui să țină seama de sarcinile și responsabilitățile specifice ale persoanei împuternicite de operator în contextul prelucrării care trebuie efectuată, precum și de riscul pentru drepturile și libertățile persoanei vizate. Operatorul și persoana împuternicită de operator pot alege să utilizeze un contract individual sau clauze contractuale standard care sunt adoptate fie direct de Comisie, fie de o autoritate de supraveghere în conformitate cu mecanismul de asigurare a coerenței și apoi adoptate de Comisie. După finalizarea prelucrării în numele operatorului, persoana împuternicită de operator ar trebui să returneze sau să șteargă, în funcție de opțiunea operatorului, datele cu caracter personal, cu excepția cazului în care există o cerință de stocare a datelor cu caracter personal în temeiul dreptului Uniunii sau al dreptului intern care instituie obligații pentru persoana împuternicită de operator.(82) În vederea demonstrării conformității cu prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să păstreze evidențe ale activităților de prelucrare aflate în responsabilitatea sa. Fiecare operator și fiecare persoană împuternicită de operator ar trebui să aibă obligația de a coopera cu autoritatea de supraveghere și de a pune la dispoziția acesteia, la cerere, aceste evidențe, pentru a putea fi utilizate în scopul monitorizării operațiunilor de prelucrare respective.(83) În vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să evalueze riscurile inerente prelucrării și să implementeze măsuri pentru

atenuarea acestor riscuri, cum ar fi criptarea. Măsurile respective ar trebui să asigure un nivel corespunzător de securitate, inclusiv confidențialitatea, luând în considerare stadiul actual al dezvoltării și costurile implementării în raport cu riscurile și cu natura datelor cu caracter personal a căror protecție trebuie asigurată. La evaluarea riscului pentru securitatea datelor cu caracter personal, ar trebui să se acorde atenție riscurilor pe care le prezintă prelucrarea datelor, cum ar fi distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, în mod accidental sau ilegal, care pot duce în special la prejudicii fizice, materiale sau morale.(84) Pentru a favoriza respectarea dispozițiilor prezentului regulament în cazurile în care operațiunile de prelucrare sunt susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul ar trebui să fie responsabil de efectuarea unei evaluări a impactului asupra protecției datelor, care să estimeze, în special, originea, natura, specificitatea și gravitatea acestui risc. Rezultatul evaluării ar trebui luat în considerare la stabilirea măsurilor adecvate care trebuie luate pentru a demonstra că prelucrarea datelor cu caracter personal respectă prezentul regulament. În cazul în care o evaluare a impactului asupra protecției datelor arată că operațiunile de prelucrare implică un risc ridicat, pe care operatorul nu îl poate atenua prin măsuri adecvate sub aspectul tehnologiei disponibile și al costurilor implementării, ar trebui să aibă loc o consultare a autorității de supraveghere înainte de prelucrare.(85) Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză. Prin urmare, de îndată ce a luat cunoștință de producerea unei încălcări a securității datelor cu caracter personal, operatorul ar trebui să notifice această încălcare autorității de supraveghere, fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore după ce a luat la cunoștință de existența acesteia, cu excepția cazului în care operatorul este în măsură să demonstreze, în conformitate cu principiul responsabilității, că încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. Atunci când notificarea nu se poate realiza în termen de 72 de ore, aceasta ar trebui să cuprindă motivele întârzierii, iar informațiile pot fi furnizate treptat, fără altă întârziere.(86) Operatorul ar trebui să comunice persoanei vizate o încălcare a securității datelor cu caracter personal, fără întârzieri nejustificate, atunci când încălcarea este

susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanei fizice, pentru a-i permite să ia măsurile de precauție necesare. Comunicarea ar trebui să descrie natura încălcării securității datelor cu caracter personal și să cuprindă recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative. Comunicările către persoanele vizate ar trebui efectuate în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu autoritatea de supraveghere, respectându-se orientările furnizate de aceasta sau de alte autorități competente, cum ar fi autoritățile de aplicare a legii. De exemplu, necesitatea de a atenua un risc imediat de producere a unui prejudiciu ar presupune comunicarea cu promptitudine către persoanele vizate, în timp ce necesitatea de a implementa măsuri corespunzătoare împotriva încălcării în continuare a securității datelor cu caracter personal sau împotriva unor încălcări similare ale securității datelor cu caracter personal ar putea justifica un termen mai îndelungat pentru comunicare.(87) Ar trebui să se stabilească dacă au fost implementate toate măsurile tehnologice de protecție și organizatorice corespunzătoare în scopul de a se stabili imediat dacă s-a produs o încălcare a securității datelor cu caracter personal și de a se informa cu promptitudine autoritatea de supraveghere și persoana vizată. Faptul că notificarea a fost efectuată fără întârziere nejustificată ar trebui stabilit luându-se în considerare, în special, natura și gravitatea încălcării securității datelor cu caracter personal, precum și consecințele și efectele negative ale acesteia asupra persoanei vizate. Această notificare poate conduce la o intervenție a autorității de supraveghere, în conformitate cu sarcinile și competențele specificate în prezentul regulament.(88) La stabilirea de norme detaliate privind formatul și procedurile aplicabile notificării referitoare la încălcările securității datelor cu caracter personal, ar trebui să se acorde atenția cuvenită circumstanțelor în care a avut loc încălcarea, stabilindu-se inclusiv dacă protecția datelor cu caracter personal a fost sau nu a fost asigurată prin măsuri tehnice de protecție corespunzătoare, care să limiteze efectiv probabilitatea fraudării identității sau a altor forme de utilizare abuzivă. În plus, astfel de norme și proceduri ar trebui să țină cont de interesele legitime ale autorităților de aplicare a legii în cazurile în care divulgarea timpurie ar putea îngreuna în mod inutil investigarea circumstanțelor în care a avut loc o încălcare a datelor cu caracter personal.(89) [Directiva 95/46/CE](#) a prevăzut o obligație generală de a notifica prelucrarea datelor cu caracter personal autorităților de supraveghere. Cu toate că obligația respectivă generează sarcini administrative și financiare, aceasta nu a contribuit întotdeauna la îmbunătățirea protecției datelor cu caracter personal. Prin urmare, astfel de obligații de notificare generală nediferențiată ar trebui să fie abrogate și înlocuite cu proceduri și mecanisme eficace care să pună accentul, în schimb, pe acele tipuri de operațiuni de prelucrare susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice prin însăși natura lor,

prin domeniul lor de aplicare, prin contextul și prin scopurile lor. Astfel de tipuri de operațiuni de prelucrare pot fi cele care presupun, în special, utilizarea unor noi tehnologii sau care reprezintă un nou tip de operațiuni, pentru care nicio evaluare a impactului asupra protecției datelor nu a fost efectuată anterior de către operator ori care devin necesare dată fiind perioada de timp care s-a scurs de la prelucrarea inițială.(90) În astfel de cazuri, operatorul ar trebui să efectueze, înainte de prelucrare, o evaluare a impactului asupra protecției datelor, în scopul evaluării gradului specific de probabilitate a materializării riscului ridicat și gravitatea acestuia, având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și sursele riscului. Respectiva evaluare a impactului ar trebui să includă, în special, măsurile, garanțiile și mecanismele avute în vedere pentru atenuarea riscului respectiv, pentru asigurarea protecției datelor cu caracter personal și pentru demonstrarea conformității cu prezentul regulament.(91) Aceasta ar trebui să se aplice, în special, operațiunilor de prelucrare la scară largă, care au drept obiectiv prelucrarea unui volum considerabil de date cu caracter personal la nivel regional, național sau supranațional, care ar putea afecta un număr mare de persoane vizate și care sunt susceptibile de a genera un risc ridicat, de exemplu, din cauza sensibilității lor, în cazul în care, în conformitate cu nivelul atins al cunoștințelor tehnologice, se folosește la scară largă o tehnologie nouă, precum și altor operațiuni de prelucrare care generează un risc ridicat pentru drepturile și libertățile persoanelor vizate, în special în cazul în care operațiunile respective limitează capacitatea persoanelor vizate de a-și exercita drepturile. Ar trebui efectuată o evaluare a impactului asupra protecției datelor și în situațiile în care datele cu caracter personal sunt prelucrate în scopul luării de decizii care vizează anumite persoane fizice în urma unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, pe baza creării de profiluri pentru datele respective, sau în urma prelucrării unor categorii speciale de date cu caracter personal, a unor date biometrice sau a unor date privind condamnările penale și infracțiunile sau măsurile de securitate conexe. Este la fel de necesară o evaluare a impactului asupra protecției datelor pentru monitorizarea la scară largă a zonelor accesibile publicului, mai ales în cazul utilizării dispozitivelor optoelectronice sau pentru orice alte operațiuni în cazul în care autoritatea de supraveghere competentă consideră că prelucrarea este susceptibilă de a genera un risc ridicat pentru drepturile și libertățile persoanelor vizate, în special deoarece acestea împiedică persoanele vizate să exercite un drept sau să utilizeze un serviciu ori un contract, sau deoarece acestea sunt efectuate în mod sistematic la scară largă. Prelucrarea datelor cu caracter personal nu ar trebui considerată a fi la scară largă în cazul în care prelucrarea se referă la date cu caracter personal de la pacienți sau clienți de către un anumit medic, un alt profesionist în domeniul sănătății sau un avocat. În aceste

cazuri, o evaluare a impactului asupra protecției datelor nu ar trebui să fie obligatorie.(92) În unele circumstanțe ar putea fi rezonabil și util din punct de vedere economic ca o evaluare a impactului asupra protecției datelor să aibă o perspectivă mai extinsă decât cea a unui singur proiect, de exemplu în cazul în care autorități sau organisme publice intenționează să instituie o aplicație sau o platformă de prelucrare comună sau în cazul în care mai mulți operatori preconizează să introducă o aplicație comună sau un mediu de prelucrare comun în cadrul unui sector sau segment industrial sau pentru o activitate orizontală utilizată la scară largă.(93) În contextul adoptării legislației naționale pe care se bazează îndeplinirea sarcinilor autorității publice sau ale organismului public și care reglementează operațiunea sau seria de operațiuni de prelucrare în cauză, statele membre pot considera că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.(94) În cazul în care o evaluare a impactului asupra protecției datelor arată că prelucrarea ar genera, în absența garanțiilor, măsurilor de securitate și mecanismelor de atenuare a riscului, un risc ridicat pentru drepturile și libertățile persoanelor fizice, iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile și al costurilor implementării, autoritatea de supraveghere ar trebui să fie consultată înainte de începerea activităților de prelucrare. Un astfel de risc ridicat este susceptibil să fie generat de anumite tipuri de prelucrare, precum și de amploarea și frecvența prelucrării, care pot duce și la producerea unor prejudicii sau pot atinge drepturile și libertățile persoanelor fizice. Autoritatea de supraveghere ar trebui să răspundă cererii de consultare într-un anumit termen. Cu toate acestea, lipsa unei reacții din partea autorității de supraveghere în termenul respectiv ar trebui să nu aducă atingere niciunei intervenții a autorității de supraveghere în conformitate cu sarcinile și competențele sale prevăzute în prezentul regulament, inclusiv competența de a interzice operațiuni de prelucrare. Ca parte a acestui proces de consultare, rezultatul unei evaluări a impactului asupra protecției datelor efectuate cu privire la prelucrarea în cauză poate fi transmis autorității de supraveghere, în special măsurile avute în vedere pentru a atenua riscul pentru drepturile și libertățile persoanelor fizice.(95) Persoana împuternicită de operator ar trebui să acorde asistență operatorului, dacă este necesar și la cerere, la asigurarea respectării obligațiilor care decurg din realizarea de evaluări ale impactului asupra protecției datelor și din consultarea prealabilă a autorității de supraveghere.(96) În timpul elaborării unei măsuri legislative sau de reglementare care prevede prelucrarea unor date cu caracter personal ar trebui, de asemenea, să aibă loc o consultare a autorității de supraveghere, pentru a garanta conformitatea prelucrării avute în vedere cu prezentul regulament și, în special, pentru a atenua riscul la care este expusă persoana vizată.(97) În cazul în care prelucrarea este efectuată de o autoritate publică, cu excepția instanțelor sau a autorităților judiciare

independente atunci când acționează în calitatea lor judiciară, în cazul în care, în sectorul privat, prelucrarea este efectuată de un operator a cărui activitate principală constă în operațiuni de prelucrare care necesită o monitorizare regulată și sistematică a persoanelor vizate pe scară largă, sau în cazul în care activitatea principală a operatorului sau a persoanei împuternicite de operator constă în prelucrarea pe scară largă de categorii speciale de date cu caracter personal și de date privind condamnările penale și infracțiunile, o persoană care deține cunoștințe de specialitate în materie de legislație și practici privind protecția datelor ar trebui să acorde asistență operatorului sau persoanei împuternicite de operator pentru monitorizarea conformității, la nivel intern, cu prezentul regulament. În sectorul privat, activitățile principale ale unui operator se referă la activitățile sale de bază, și nu la prelucrarea datelor cu caracter personal drept activități auxiliare. Nivelul necesar al cunoștințelor de specialitate ar trebui să fie stabilit în special în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate de operator sau de persoana împuternicită de operator. Acești responsabili cu protecția datelor, indiferent dacă sunt sau nu angajați ai operatorului, ar trebui să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent.(98) Asociațiile sau alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori ar trebui încurajate să elaboreze coduri de conduită, în limitele prezentului regulament, astfel încât să se faciliteze aplicarea efectivă a prezentului regulament, luându-se în considerare caracteristicile specifice ale prelucrării efectuate în anumite sectoare și necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii. În special, astfel de coduri de conduită ar putea să ajusteze obligațiile operatorilor și ale persoanelor împuternicite de operatori, ținând seama de riscul aferent prelucrării care este susceptibil de a fi generat pentru drepturile și libertățile persoanelor fizice.(99) Atunci când elaborează un cod de conduită sau când modifică sau extind un astfel de cod, asociațiile și alte organisme care reprezintă categorii de operatori sau persoane împuternicite de operatori ar trebui să consulte părțile implicate relevante, inclusiv persoanele vizate, dacă este fezabil, și să ia în considerare contribuțiile transmise și opiniile exprimate în cadrul unor astfel de consultări.(100) Pentru a se îmbunătăți transparența și conformitatea cu prezentul regulament, ar trebui să se încurajeze instituirea de mecanisme de certificare, precum și de sigilii și mărci în materie de protecție a datelor, care să permită persoanelor vizate să evalueze rapid nivelul de protecție a datelor aferent produselor și serviciilor relevante.(101) Fluxurile de date cu caracter personal către și dinspre țări situate în afara Uniunii și organizații internaționale sunt necesare pentru dezvoltarea comerțului internațional și a cooperării internaționale. Creșterea acestor fluxuri a generat noi provocări și preocupări cu privire la protecția datelor cu caracter personal. Cu toate

acestea, în cazul în care se transferă date cu caracter personal din Uniune către operatori, persoane împuternicite de operatori sau alți destinatari din țări terțe sau organizații internaționale, nivelul de protecție a persoanelor fizice asigurat în Uniune prin prezentul regulament nu ar trebui să fie diminuat, inclusiv în cazurile de transferuri ulterioare de date cu caracter personal dinspre țara terță sau organizația internațională către operatori, persoane împuternicite de operatori din aceeași sau dintr-o altă țară terță sau organizație internațională. În orice caz, transferurile către țări terțe și organizații internaționale pot fi desfășurate numai în conformitate deplină cu prezentul regulament. Un transfer ar putea avea loc numai dacă, sub rezerva respectării celorlalte dispoziții ale prezentului regulament, operatorul sau persoana împuternicită de operator îndeplinește condițiile prevăzute de dispozițiile prezentului regulament privind transferul de date cu caracter personal către țări terțe sau organizații internaționale.(102) Prezentul regulament nu aduce atingere acordurilor internaționale încheiate între Uniune și țări terțe în vederea reglementării transferului de date cu caracter personal, inclusiv garanții adecvate pentru persoanele vizate. Statele membre pot încheia acorduri internaționale care implică transferul de date cu caracter personal către țări terțe sau organizații internaționale, în măsura în care astfel de acorduri nu afectează prezentul regulament și nici alte dispoziții din dreptul Uniunii și includ un nivel corespunzător de protecție a drepturilor fundamentale ale persoanelor vizate.(103) Comisia poate decide, cu efect în întreaga Uniune, că o țară terță, un teritoriu sau un anumit sector dintr-o țară terță sau o organizație internațională oferă un nivel adecvat de protecție a datelor, asigurând astfel securitate juridică și uniformitate în Uniune în ceea ce privește țara terță sau organizația internațională care este considerată a furniza un astfel de nivel de protecție. În aceste cazuri, transferurile de date cu caracter personal către țara terță sau organizația internațională respectivă pot avea loc fără a fi necesar să se obțină autorizări suplimentare. De asemenea, Comisia poate să decidă, după trimiterea unei notificări și a unei justificări complete țării terțe sau organizației internaționale, să anuleze o astfel de decizie.(104) În conformitate cu valorile fundamentale pe care se întemeiază Uniunea, în special protecția drepturilor omului, Comisia ar trebui, în evaluarea sa referitoare la țara terță sau la un teritoriu sau la un sector specificat dintr-o țară terță, să ia în considerare modul în care aceasta respectă statul de drept, accesul la justiție, precum și normele și standardele internaționale în materie de drepturi ale omului și legislația sa generală și sectorială, inclusiv legislația privind securitatea publică, apărarea și securitatea națională, precum și ordinea publică și dreptul penal. Adoptarea unei decizii privind caracterul adecvat al nivelului de protecție pentru un teritoriu sau un sector specificat dintr-o țară terță ar trebui să țină seama de criterii clare și obiective, cum ar fi activitățile specifice de prelucrare și domeniul de aplicare al standardelor legale aplicabile și legislația în vigoare în

țara terță respectivă. Țara terță ar trebui să ofere garanții care să asigure un nivel adecvat de protecție, echivalent în esență cu cel asigurat în cadrul Uniunii, în special atunci când datele cu caracter personal sunt prelucrate în unul sau mai multe sectoare specifice. În special, țara terță ar trebui să asigure o supraveghere efectivă independentă în materie de protecție a datelor și să prevadă mecanisme de cooperare cu autoritățile statelor membre de protecție a datelor, iar persoanele vizate ar trebui să beneficieze de drepturi efective și opozabile și de reparații efective pe cale administrativă și judiciară.(105) Pe lângă angajamentele internaționale asumate de țara terță sau de organizația internațională, Comisia ar trebui să țină seama de obligațiile care decurg din participarea țării terțe sau a organizației internaționale la sistemele multilaterale sau regionale, în special în ceea ce privește protecția datelor cu caracter personal, precum și de punerea în aplicare a unor astfel de obligații. În special, ar trebui să fie luată în considerare aderarea țării terțe la Convenția Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal și protocolul adițional la aceasta. Comisia ar trebui să consulte comitetul atunci când evaluează nivelul de protecție din țările terțe sau din organizațiile internaționale.(106) Comisia ar trebui să monitorizeze funcționarea deciziilor privind nivelul de protecție dintr-o țară terță sau un teritoriu sau un anumit sector dintr-o țară terță sau dintr-o organizație internațională și să monitorizeze funcționarea deciziilor adoptate în temeiul articolului 25 alineatul (6) sau al articolului 26 alineatul (4) din [Directiva 95/46/CE](#). În deciziile sale privind caracterul adecvat al nivelului de protecție, Comisia ar trebui să prevadă un mecanism de revizuire periodică a modului lor de funcționare. Această revizuire periodică ar trebui să fie efectuată în consultare cu țara terță sau organizația internațională în cauză și ar trebui să ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională. În scopul monitorizării și al efectuării revizuirilor periodice, Comisia ar trebui să ia în considerare opiniile și constatările Parlamentului European și ale Consiliului, precum și ale altor organisme și surse relevante. Comisia ar trebui să evalueze, într-un termen rezonabil, funcționarea deciziilor din urmă și să raporteze toate constatările relevante comitetului, în sensul [Regulamentului \(UE\) nr. 182/2011](#) al Parlamentului European și al Consiliului \*12), după cum s-a stabilit în temeiul prezentului regulament, Parlamentului European și Consiliului.(107) Comisia poate să recunoască faptul că o țară terță, un teritoriu sau un sector specificat dintr-o țară terță sau o organizație internațională nu mai asigură un nivel adecvat de protecție a datelor. În consecință, transferul de date cu caracter personal către țara terță sau organizația internațională respectivă ar trebui să fie interzis, cu excepția cazului în care sunt îndeplinite cerințele prevăzute în prezentul regulament privind transferurile în baza unor garanții adecvate, inclusiv regulile corporatiste obligatorii și derogările de la situațiile specifice.

În acest caz, ar trebui să se prevadă dispoziții pentru consultări între Comisie și astfel de țări terțe sau organizații internaționale. Comisia ar trebui ca, în timp util, să informeze țara terță sau organizația internațională cu privire la aceste motive și să inițieze consultări cu aceasta pentru remedierea situației.(108) În absența unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator ar trebui să adopte măsuri pentru a compensa lipsa protecției datelor într-o țară terță prin intermediul unor garanții adecvate pentru persoana vizată. Astfel de garanții adecvate pot consta în utilizarea regulilor corporatiste obligatorii, a clauzelor standard de protecție a datelor adoptate de Comisie, a clauzelor standard de protecție a datelor adoptate de o autoritate de supraveghere sau a clauzelor contractuale autorizate de o autoritate de supraveghere. Respectivile garanții ar trebui să asigure respectarea cerințelor în materie de protecție a datelor și drepturi ale persoanelor vizate corespunzătoare prelucrării în interiorul Uniunii, inclusiv disponibilitatea unor drepturi opozabile ale persoanelor vizate și a unor căi de atac eficiente, printre care dreptul de acces la reparații efective pe cale administrativă sau judiciară și dreptul de a solicita despăgubiri, în Uniune sau într-o țară terță. Acestea ar trebui să se refere în special la respectarea principiilor generale privind prelucrarea datelor cu caracter personal: principiul protecției datelor începând cu momentul conceperii și principiul protecției implicite a datelor. Transferurile pot fi efectuate și de către autoritățile sau organismele publice cu autorități sau organisme publice în țări terțe sau cu organizații internaționale cu atribuții și funcții corespunzătoare, inclusiv pe baza dispozițiilor care prevăd drepturi opozabile și efective pentru persoanele vizate, care trebuie introduse în acordurile administrative, cum ar fi un memorandum de înțelegere. Autorizația din partea autorității de supraveghere competente ar trebui obținută atunci când garanțiile sunt oferite în cadrul unor acorduri administrative fără caracter juridic obligatoriu.(109) Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecție a datelor, adoptate de Comisie sau de o autoritate de supraveghere, nu ar trebui să împiedice operatorii sau persoanele împuternicite de aceștia să includă clauzele standard în materie de protecție a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator și o altă persoană împuternicită de operator, și nici să adauge alte clauze sau garanții suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de o autoritate de supraveghere sau nu prejudiciază drepturile sau libertățile fundamentale ale persoanelor vizate. Operatorii și persoanele împuternicite de operatori ar trebui să fie încurajați să ofere garanții suplimentare prin intermediul unor angajamente contractuale care să completeze clauzele standard în materie de protecție.(110) Un grup de întreprinderi sau un grup de întreprinderi implicat într-o activitate economică

comună ar trebui să poată utiliza regulile corporatiste obligatorii aprobate pentru transferurile sale internaționale dinspre Uniune către organizații din cadrul aceluiași grup de întreprinderi sau grup de întreprinderi implicate într-o activitate economică comună, cu condiția ca astfel de reguli corporatiste să includă toate principiile esențiale și drepturile opozabile în scopul asigurării unor garanții adecvate pentru transferurile sau categoriile de transferuri de date cu caracter personal.(111) Ar trebui să se prevadă posibilitatea de a se efectua transferuri în anumite circumstanțe în care persoana vizată și-a dat consimțământul explicit, în care transferul este ocazional și necesar în legătură cu un contract sau cu o acțiune în justiție, indiferent dacă este în contextul unei proceduri judiciare sau în contextul unei proceduri administrative sau extrajudiciare, inclusiv în cadrul procedurilor înaintate organismelor de reglementare. De asemenea, ar trebui să se prevadă posibilitatea de a se efectua transferuri în cazul în care motive importante de interes public stabilite de dreptul Uniunii sau de dreptul intern impun acest lucru sau în cazul în care transferul se efectuează dintr-un registru instituit prin lege și destinat să fie consultat de către public sau de către persoane care au un interes legitim. În acest ultim caz, un astfel de transfer nu ar trebui să implice totalitatea datelor cu caracter personal sau ansamblul categoriilor de date conținute în registru, iar atunci când registrul este destinat să fie consultat de persoane care au un interes legitim, transferul ar trebui să fie efectuat doar la cererea persoanelor respective sau dacă acestea sunt destinatarii, luând pe deplin în considerare interesele și drepturile fundamentale ale persoanei vizate.(112) Aceste derogări ar trebui să se aplice, în special, transferurilor de date solicitate și necesare din considerente importante de interes public, de exemplu în cazul schimbului internațional de date între autoritățile din domeniul concurenței, administrațiile fiscale sau vamale, între autoritățile de supraveghere financiară, între serviciile competente în materie de securitate socială sau de sănătate publică, de exemplu în cazul depistării punctelor de contact pentru bolile contagioase sau pentru reducerea și/sau eliminarea dopajului în sport. Un transfer de date cu caracter personal ar trebui, de asemenea, să fie considerat legal în cazul în care este necesar în scopul protejării unui interes care este esențial în interesele vitale ale persoanei vizate sau ale unei alte persoane, inclusiv pentru integritatea fizică sau pentru viața acesteia, în cazul în care persoana vizată nu are capacitatea să își dea consimțământul. În absența unei decizii privind caracterul adecvat al nivelului de protecție, dreptul Uniunii sau dreptul intern poate, din considerente importante de interes public, stabili în mod expres limite asupra transferului unor categorii specifice de date către o țară terță sau o organizație internațională. Statele membre ar trebui să notifice Comisiei aceste dispoziții. Orice transfer către o organizație umanitară internațională al datelor cu caracter personal ale unei persoane vizate care se află în incapacitate fizică sau juridică de a își da consimțământul, în vederea

îndeplinirii unei sarcini care decurge din Convențiile de la Geneva sau în vederea conformării cu dreptul internațional umanitar aplicabil în conflictele armate, ar putea fi considerat necesar pentru un motiv important de interes public sau pentru că este în interesul vital al persoanei vizate.(113) Transferurile care pot fi considerate ca nefiind repetitive și care se referă doar la un număr limitat de persoane vizate, ar putea, de asemenea, să fie efectuate în scopul realizării intereselor legitime urmărite de operator, atunci când asupra respectivelor interese nu prevalează interesele sau drepturile și libertățile persoanei vizate și atunci când operatorul a evaluat toate circumstanțele aferente transferului de date. Operatorul ar trebui să acorde o atenție deosebită naturii datelor cu caracter personal, scopului și duratei operațiunii sau operațiunilor propuse de prelucrare, precum și situației din țara de origine, din țara terță și din țara de destinație finală și ar trebui să ofere garanții adecvate pentru protecția drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Astfel de transferuri ar trebui să fie posibile numai în cazurile reziduale în care nu se poate aplica niciunul dintre celelalte motive de transfer. În ceea ce privește scopurile de cercetare științifică sau istorică sau scopurile statistice, ar trebui să se ia în considerare așteptările legitime ale societății cu privire la creșterea nivelului de cunoștințe. Operatorul ar trebui să informeze autoritatea de supraveghere și persoana vizată cu privire la transfer.(114) În orice caz, atunci când Comisia nu a luat o decizie cu privire la nivelul adecvat de protecție a datelor dintr-o țară terță, operatorul sau persoana împuternicită de operator ar trebui să utilizeze soluții care să ofere persoanelor vizate drepturi opozabile și efective în ceea ce privește prelucrarea datelor lor în Uniune odată ce aceste date au fost transferate, astfel încât persoanele vizate să beneficieze în continuare de drepturi fundamentale și garanții.(115) Unele țări terțe au adoptat legi, reglementări și alte acte juridice care au drept obiectiv să reglementeze în mod direct activitățile de prelucrare a datelor ale persoanelor fizice și juridice aflate sub jurisdicția statelor membre. Aceasta poate include hotărâri ale instanțelor judecătorești sau decizii ale autorităților administrative din țări terțe care solicită unui operator sau unei persoane împuternicite de operator să transfere sau să divulge date cu caracter personal și care nu se bazează pe un acord internațional, cum ar fi un tratat de asistență juridică reciprocă, în vigoare între țara terță solicitantă și Uniune sau un stat membru. Aplicarea extraterritorială a acestor legi, reglementări și alte acte juridice poate încălca dreptul internațional și poate împiedica asigurarea protecției persoanelor fizice asigurată în Uniune prin prezentul regulament. Transferurile ar trebui să fie permise numai în cazul îndeplinirii condițiilor prevăzute de prezentul regulament pentru un transfer către țări terțe. Acesta ar putea fi cazul, inter alia, atunci când divulgarea este necesară dintr-un motiv important de interes public recunoscut în dreptul Uniunii sau în dreptul intern care se aplică

operatorului.(116) Fluxul transfrontalier de date cu caracter personal în afara Uniunii poate expune unui risc sporit capacitatea persoanelor fizice de a-și exercita drepturile în materie de protecție a datelor, în special pentru a-și asigura protecția împotriva utilizării sau a divulgării ilegale a acestor informații. În același timp, autoritățile de supraveghere pot constata că se află în imposibilitatea de a trata plângeri sau de a efectua investigații referitoare la activitățile desfășurate în afara frontierelor lor. Eforturile acestora de a conlucra în context transfrontalier pot fi, de asemenea, îngreunate de insuficiența competențelor de prevenire sau remediere, de caracterul eterogen al regimurilor juridice și de existența unor obstacole de ordin practic, cum ar fi constrângerile în materie de resurse. Prin urmare, este necesar să se promoveze o cooperare mai strânsă între autoritățile de supraveghere a protecției datelor pentru a putea face schimb de informații și a desfășura investigații împreună cu omologii lor internaționali. În scopul elaborării de mecanisme de cooperare internațională pentru a facilita și a oferi asistență internațională reciprocă în asigurarea aplicării legislației din domeniul protecției datelor cu caracter personal, Comisia și autoritățile de supraveghere ar trebui să facă schimb de informații și să coopereze în cadrul activităților legate de exercitarea competențelor lor cu autoritățile competente din țări terțe, pe bază de reciprocitate și în conformitate cu prezentul regulament.(117) Instituirea în statele membre a unor autorități de supraveghere, împuternicite să își îndeplinească sarcinile și să își exercite competențele în deplină independență, este un element esențial al protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Statele membre ar trebui să poată institui mai multe autorități de supraveghere, pentru a reflecta structura lor constituțională, organizatorică și administrativă.(118) Independența autorităților de supraveghere nu ar trebui să însemne că autoritățile de supraveghere nu pot face obiectul unor mecanisme de control sau de monitorizare în ceea ce privește cheltuielile acestora sau unui control jurisdicțional.(119) În cazul în care un stat membru instituie mai multe autorități de supraveghere, acesta ar trebui să stabilească prin lege mecanisme care să asigure participarea efectivă a autorităților de supraveghere respective la mecanismul pentru asigurarea coerenței. Statul membru respectiv ar trebui, în special, să desemneze autoritatea de supraveghere care îndeplinește funcția de punct unic de contact pentru participarea efectivă a acestor autorități la mecanism, în scopul asigurării unei cooperări rapide și armonioase cu alte autorități de supraveghere, cu comitetul și cu Comisia.(120) Fiecare autoritate de supraveghere ar trebui să beneficieze de resurse financiare și umane, de spațiile și de infrastructura necesare pentru îndeplinirea cu eficacitate a sarcinilor lor, inclusiv a celor legate de asistență reciprocă și cooperarea cu alte autorități de supraveghere în întreaga Uniune. Fiecare autoritate de supraveghere ar trebui să aibă un buget public anual separat, care poate face parte din bugetul general de stat

sau național.(121) Condițiile generale pentru membrul sau membrii autorității de supraveghere ar trebui stabilite de lege în fiecare stat membru și ar trebui, în special, să prevadă că respectivii membri sunt numiți printr-o procedură transparentă fie de parlamentul, de guvernul ori șeful de stat al statului membru pe baza unei propuneri din partea guvernului, a unui membru al guvernului, a parlamentului sau a unei camere a parlamentului, fie de către un organism independent împuternicit prin dreptul intern. În vederea asigurării independenței autorității de supraveghere, membrul sau membrii acesteia ar trebui să acționeze cu integritate, să nu întreprindă acțiuni incompatibile cu îndatoririle lor, iar, pe durata mandatului, ar trebui să nu desfășoare activități incompatibile, remunerate sau nu. Autoritatea de supraveghere ar trebui să aibă personal propriu, ales de autoritatea de supraveghere sau de un organism independent înființat în temeiul dreptului intern, care ar trebui să fie subordonat exclusiv membrului sau membrilor autorității de supraveghere.(122) Fiecare autoritate de supraveghere ar trebui să aibă, pe teritoriul statului membru de care aparține, atribuția de a exercita competențele și de a îndeplini sarcinile cu care este învestită în conformitate cu prezentul regulament. Aceasta ar trebui să includă în special prelucrarea în contextul activităților unui sediu al operatorului sau al persoanei împuternicite de operator pe teritoriul propriului stat membru, prelucrarea datelor cu caracter personal efectuată de autoritățile publice sau de organisme private care acționează în interes public, prelucrarea care afectează persoanele vizate de pe teritoriul său sau prelucrarea efectuată de către un operator sau o persoană împuternicită de operator care nu își are sediul în Uniune în cazul în care aceasta privește persoane vizate care își au reședința pe teritoriul său. Aceasta ar trebui să includă tratarea plângerilor depuse de o persoană vizată, efectuarea de investigații privind aplicarea prezentului regulament și promovarea informării publicului cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal.(123) Autoritățile de supraveghere ar trebui să monitorizeze aplicarea dispozițiilor prevăzute de prezentul regulament și să contribuie la aplicarea coerentă a acestuia în întreaga Uniune, în scopul asigurării protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal și al facilitării liberei circulații a datelor cu caracter personal în interiorul pieței interne. În acest sens, autoritățile de supraveghere ar trebui să coopereze reciproc, precum și cu Comisia, fără să fie necesar niciun acord între statele membre cu privire la acordarea de asistență reciprocă sau cu privire la respectiva cooperare.(124) În cazul în care prelucrarea datelor cu caracter personal se desfășoară în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune, iar operatorul sau persoana împuternicită de operator are sedii în mai multe state membre, sau în cazul în care prelucrarea care se desfășoară în contextul activităților unui singur sediu al unui operator sau al

unei persoane împuternicite de operator din Uniune afectează sau este susceptibilă să afecteze semnificativ persoane vizate din mai multe state membre, autoritatea de supraveghere a sediului principal al operatorului sau al persoanei împuternicite de operator ori a sediului unic al operatorului sau al persoanei împuternicite de operator ar trebui să acționeze în calitate de autoritate principală. Aceasta ar trebui să coopereze cu celelalte autorități vizate, pentru că operatorul sau persoana împuternicită de operator are un sediu pe teritoriul statului lor membru, pentru că persoanele vizate care își au reședința pe teritoriul lor sunt afectate în mod semnificativ sau pentru că le-a fost înaintată o plângere. De asemenea, în cazul în care o persoană vizată care nu își are reședința în statul membru respectiv a depus o plângere, autoritatea de supraveghere la care a fost depusă plângerea ar trebui, de asemenea, să fie o autoritate de supraveghere vizată. În cadrul sarcinilor sale de a emite orientări cu privire la orice chestiune referitoare la punerea în aplicare a prezentului regulament, comitetul ar trebui să poată emite orientări privind, în special, criteriile care trebuie luate în considerare pentru a se stabili dacă prelucrarea în cauză afectează în mod semnificativ persoane vizate din mai multe state membre și privind conținutul unei obiecții relevante și motivate.(125) Autoritatea principală ar trebui să aibă competența de a adopta decizii obligatorii privind măsurile de aplicare a competențelor care îi sunt conferite în conformitate cu prezentul regulament. În calitatea sa de autoritate principală, autoritatea de supraveghere ar trebui să implice îndeaproape și să coordoneze activitățile autorităților de supraveghere vizate în procesul decizional. În cazurile în care decizia este de respingere parțială sau totală a plângerii din partea persoanei vizate, o asemenea decizie ar trebui adoptată de către autoritatea de supraveghere la care s-a depus plângerea.(126) Decizia ar trebui convenită în comun de autoritatea de supraveghere principală și de autoritățile de supraveghere vizate și ar trebui să vizeze sediul principal sau sediul unic al operatorului sau al persoanei împuternicite de operator și să fie obligatorie pentru operator și pentru persoana împuternicită de operator. Operatorul sau persoana împuternicită de operator ar trebui să ia măsurile necesare pentru a asigura conformitatea cu prezentul regulament și punerea în aplicare a deciziei notificate de autoritatea de supraveghere principală sediului principal al operatorului sau al persoanei împuternicite de operator în ceea ce privește activitățile de prelucrare în Uniune.(127) Fiecare autoritate de supraveghere care nu acționează ca autoritate de supraveghere principală ar trebui să aibă competența de a trata cazuri locale, în care operatorul sau persoana împuternicită de operator are sedii în mai multe state membre, dar obiectul respectivei prelucrări privește doar prelucrarea efectuată într-un singur stat membru și implicând doar persoane vizate din acel unic stat membru, de exemplu în cazul în care obiectul îl constituie prelucrarea datelor cu caracter personal ale angajaților în contextul specific legat de forța de muncă dintr-un

stat membru. În astfel de cazuri, autoritatea de supraveghere ar trebui să informeze fără întârziere autoritatea de supraveghere principală cu privire la această chestiune. După ce a fost informată, autoritatea de supraveghere principală ar trebui să decidă dacă va trata ea însăși cazul în temeiul dispoziției privind cooperarea între autoritatea de supraveghere principală și alte autorități de supraveghere vizate ("mecanismul ghișeului unic"), sau dacă autoritatea de supraveghere care a informat-o ar trebui să se ocupe de caz la nivel local. Atunci când decide dacă va trata cazul, autoritatea de supraveghere principală ar trebui să ia în considerare dacă există un sediu al operatorului sau al persoanei împuternicite de operator în statul membru al autorității de supraveghere care a informat-o, în vederea garantării respectării efective a unei decizii în ceea ce privește operatorul sau persoana împuternicită de operator. În cazul în care autoritatea de supraveghere principală decide să trateze cazul, autoritatea de supraveghere care a informat-o ar trebui să beneficieze de posibilitatea de a prezenta un proiect de decizie, de care autoritatea de supraveghere principală ar trebui să țină seama în cea mai mare măsură atunci când pregătește proiectul său de decizie în cadrul respectivului mecanism al ghișeului unic.(128) Normele privind autoritatea de supraveghere principală și mecanismul ghișeului unic nu ar trebui să se aplice în cazul în care prelucrarea este efectuată de autorități publice sau organisme private în interes public. În asemenea cazuri, singura autoritate de supraveghere competentă să își exercite competențele care i-au fost atribuite în conformitate cu prezentul regulament ar trebui să fie autoritatea de supraveghere a statului membru în care autoritatea publică sau organismul privat își are sediul.(129) Pentru a se asigura consecvența monitorizării și a aplicării prezentului regulament în întreaga Uniune, autoritățile de supraveghere ar trebui să aibă în fiecare stat membru aceleași sarcini și competențe efective, inclusiv competențe de investigare, competențe corective și sancțiuni, precum și competențe de autorizare și de consiliere, în special în cazul plângerilor depuse de persoane fizice, precum și, fără a aduce atingere competențelor autorităților de urmărire penală în temeiul dreptului intern, de a aduce în atenția autorităților judiciare cazurile de încălcare a prezentului regulament și de a se implica în proceduri judiciare. Aceste competențe ar trebui să includă și competența de a impune o limitare temporară sau definitivă, inclusiv o interdicție, asupra prelucrării. Statele membre pot stabili alte sarcini legate de protecția datelor cu caracter personal în temeiul prezentului regulament. Competențele autorităților de supraveghere ar trebui exercitate în conformitate cu garanții procedurale adecvate prevăzute în dreptul Uniunii și în dreptul intern, în mod imparțial, echitabil și într-un termen rezonabil. În special, fiecare măsură ar trebui să fie adecvată, necesară și proporțională în scopul de a asigura conformitatea cu dispozițiile prezentului regulament, luând în considerare circumstanțele fiecărui caz în parte, să respecte dreptul oricărei persoane de a fi ascultată

Înainte de luarea oricărei măsuri individuale care ar putea să îi aducă atingere și să evite costurile inutile și inconvenientele excesive pentru persoanele în cauză. Competențele de investigare în ceea ce privește accesul în incinte ar trebui exercitate în conformitate cu cerințele specifice din dreptul procedural național, cum ar fi obligația de a obține în prealabil o autorizare judiciară. Fiecare măsură obligatorie din punct de vedere juridic luată de autoritatea de supraveghere ar trebui să fie prezentată în scris, să fie clară și lipsită de ambiguitate, să indice autoritatea de supraveghere care a emis măsura, data emiterii măsurii, să poarte semnătura șefului sau a unui membru al autorității de supraveghere autorizat de acesta, să furnizeze motivele pentru care s-a luat măsura și să facă trimitere la dreptul la o cale de atac eficientă. Acest lucru nu ar trebui să excludă cerințe suplimentare în conformitate cu dreptul procedural național. Adoptarea unor astfel de decizii obligatorii din punct de vedere juridic implică faptul că se poate da naștere unui control jurisdicțional în statul membru al autorității de supraveghere care a adoptat decizia.(130) În cazul în care autoritatea de supraveghere la care s-a depus plângerea nu este autoritatea de supraveghere principală, autoritatea de supraveghere principală ar trebui să coopereze îndeaproape cu autoritatea de supraveghere la care s-a depus plângerea, în conformitate cu dispozițiile privind cooperarea și consecvența prevăzute în prezentul regulament. În astfel de cazuri, autoritatea de supraveghere principală ar trebui, atunci când ia măsuri destinate să producă efecte juridice, inclusiv impunerea de amenzi administrative, să țină seama cât mai mult posibil de opinia autorității de supraveghere la care a fost depusă plângerea și care ar trebui să își mențină competența de a desfășura orice investigație pe teritoriul propriului stat membru, în colaborare cu autoritatea de supraveghere principală.(131) În cazurile în care o altă autoritate de supraveghere ar trebui să acționeze în calitate de autoritate de supraveghere principală pentru activitățile de prelucrare ale operatorului sau ale persoanei împuternicite de operator, dar obiectul concret al unei plângeri sau posibila încălcare vizează numai activitățile de prelucrare ale operatorului sau ale persoanei împuternicite de operator în statul membru în care a fost depusă plângerea sau a fost depistată posibila încălcare, iar chestiunea nu afectează în mod substanțial sau nu este susceptibilă să afecteze în mod substanțial persoane vizate din alte state membre, autoritatea de supraveghere care a primit o plângere sau a depistat ori a fost informată în alt mod asupra unor situații de posibile încălcări ale prezentului regulament ar trebui să încerce o soluționare pe cale amiabilă cu operatorul și, în cazul în care aceasta eșuează, să își exercite plenitudinea competențelor. Aceasta ar trebui să includă activități specifice de prelucrare efectuate pe teritoriul statului membru al autorității de supraveghere ori cu privire la persoane vizate de pe teritoriul aceluia stat membru, activități de prelucrare care au loc în contextul unei oferte de bunuri sau servicii destinate în mod special persoanelor vizate pe teritoriul statului

membru al autorității de supraveghere sau activități de prelucrare care trebuie evaluate ținând seama de obligațiile juridice relevante în temeiul dreptului intern.(132) Activitățile de creștere a gradului de conștientizare organizate pentru public de autoritățile de supraveghere ar trebui să includă măsuri specifice care să vizeze operatorii și persoanele împuternicite de operatori, inclusiv microîntreprinderile și întreprinderile mici și mijlocii, precum și persoanele fizice, în special în context educațional.(133) Autoritățile de supraveghere ar trebui să își acorde reciproc asistență în îndeplinirea sarcinilor care le revin, pentru a se asigura coerența aplicării prezentului regulament pe piața internă. O autoritate de supraveghere care solicită asistență reciprocă poate adopta o măsură provizorie în cazul în care nu primește un răspuns la o solicitare de asistență reciprocă în termen de o lună de la primirea solicitării de către cealaltă autoritate de supraveghere.(134) Fiecare autoritate de supraveghere ar trebui să participe, după caz, la operațiuni comune între autoritățile de supraveghere. Autoritatea de supraveghere căreia i s-a adresat solicitarea ar trebui să aibă obligația de a răspunde cererii într-un anumit termen.(135) Pentru a se asigura aplicarea coerentă a prezentului regulament în întreaga Uniune, ar trebui să se instituie un mecanism pentru asigurarea coerenței în cadrul căruia autoritățile de supraveghere să coopereze. Acest mecanism ar trebui să se aplice, în special, în cazul în care o autoritate de supraveghere intenționează să adopte o măsură prevăzută a produce efecte juridice în ceea ce privește operațiunile de prelucrare care afectează în mod substanțial un număr semnificativ de persoane vizate din mai multe state membre. Mecanismul ar trebui să se aplice, de asemenea, în cazul în care o autoritate de supraveghere vizată sau Comisia solicită ca aspectul respectiv să fie tratat în cadrul mecanismului pentru asigurarea coerenței. Acest mecanism nu ar trebui să aducă atingere măsurilor pe care Comisia le poate adopta în exercitarea competențelor care îi revin în temeiul tratatelor.(136) În aplicarea mecanismului pentru asigurarea coerenței, comitetul ar trebui, într-un anumit termen, să emită un aviz în cazul în care o majoritate a membrilor săi decide astfel sau în cazul în care orice autoritate de supraveghere vizată sau Comisia solicită acest lucru. Comitetul ar trebui, de asemenea, să fie împuternicit să adopte decizii obligatorii din punct de vedere juridic în cazul unor litigii între autoritățile de supraveghere. În acest scop, acesta ar trebui să emită, în principiu cu o majoritate de două treimi din membrii săi, decizii obligatorii din punct de vedere juridic, în cazuri bine definite, în cazul în care există opinii divergente între autoritățile de supraveghere, în special în cadrul mecanismului de cooperare între autoritatea de supraveghere principală și autoritățile de supraveghere vizate privind fondul cauzei, în special existența sau nu a unei încălcări a prezentului regulament.(137) Este posibil să existe o necesitate urgentă de a se acționa pentru asigurarea protecției drepturilor și libertăților persoanelor vizate, în

special în cazul în care există pericolul ca exercitarea unui drept al unei persoane vizate să fie împiedicată în mod considerabil. Prin urmare, o autoritate de supraveghere ar trebui să poată adopta măsuri provizorii pe teritoriul său, justificate în mod corespunzător, având o perioadă de valabilitate determinată care nu ar trebui să depășească trei luni.(138) Aplicarea unui astfel de mecanism ar trebui să constituie o condiție pentru legalitatea unei măsuri destinate să producă efecte juridice, luate de o autoritate de supraveghere, în cazurile în care aplicarea acesteia este obligatorie. În alte cazuri cu relevanță transfrontalieră, ar trebui pus în aplicare mecanismul de cooperare între autoritatea de supraveghere principală și autoritățile de supraveghere vizate, iar între autoritățile de supraveghere vizate s-ar putea acorda asistență reciprocă și s-ar putea desfășura operațiuni comune pe bază bilaterală sau multilaterală, fără declanșarea mecanismului pentru asigurarea coerenței.(139) Cu scopul de a promova aplicarea coerentă a prezentului regulament, comitetul ar trebui instituit ca organ independent al Uniunii. Pentru a-și îndeplini obiectivele, comitetul ar trebui să aibă personalitate juridică. Comitetul ar trebui să fie reprezentat de președintele său. Acesta ar trebui să înlocuiască Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, instituit prin [Directiva 95/46/CE](#). Acesta ar trebui să fie alcătuit din șefii autorităților de supraveghere din fiecare stat membru și din Autoritatea Europeană pentru Protecția Datelor sau reprezentanții acestora. Comisia ar trebui să participe la activitățile comitetului fără a avea drept de vot, iar Autoritatea Europeană pentru Protecția Datelor ar trebui să aibă drepturi de vot speciale. Comitetul ar trebui să contribuie la aplicarea coerentă a prezentului regulament în întreaga Uniune, inclusiv prin oferirea de consiliere Comisiei, în special cu privire la nivelul de protecție în țările terțe și în cadrul organizațiilor internaționale, și prin promovarea cooperării autorităților de supraveghere în întreaga Uniune. Comitetul ar trebui să acționeze în mod independent în îndeplinirea sarcinilor sale.(140) Comitetul ar trebui să fie asistat de un secretariat asigurat de Autoritatea Europeană pentru Protecția Datelor. Personalul Autorității Europene pentru Protecția Datelor implicat în îndeplinirea sarcinilor conferite comitetului în temeiul prezentului regulament ar trebui să își îndeplinească sarcinile exclusiv conform instrucțiunilor președintelui comitetului și să raporteze acestuia.(141) Orice persoană vizată ar trebui să aibă dreptul de a depune o plângere la o singură autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, precum și dreptul la o cale de atac eficientă în conformitate cu articolul 47 din cartă, în cazul în care persoana vizată consideră că drepturile sale în temeiul prezentului regulament sunt încălcate sau în cazul în care autoritatea de supraveghere nu reacționează la o plângere, respinge sau refuză parțial sau total o plângere sau nu acționează atunci când o astfel de acțiune este necesară pentru asigurarea protecției

drepturilor persoanei vizate. Investigația în urma unei plângeri ar trebui să fie efectuată, sub control judiciar, în măsura în care este necesar, în funcție de caz. Autoritatea de supraveghere ar trebui să informeze persoana vizată cu privire la evoluția și soluționarea plângerii într-un termen rezonabil. În eventualitatea în care cazul necesită o investigare suplimentară sau coordonarea cu o altă autoritate de supraveghere, ar trebui să se furnizeze informații intermediare persoanei vizate. În vederea facilitării depunerii plângerilor, fiecare autoritate de supraveghere ar trebui să ia măsuri precum punerea la dispoziție a unui formular de depunere a plângerii, care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.(142) În cazul în care persoana vizată consideră că drepturile sale în temeiul prezentului regulament sunt încălcate, aceasta ar trebui să aibă dreptul de a mandata un organism, o organizație sau o asociație fără scop lucrativ care este înființat(ă) în conformitate cu dreptul intern, ale cărui (cărei) obiective statutare sunt în interesul public și care își desfășoară activitatea în domeniul asigurării protecției datelor cu caracter personal, să depună o plângere în numele său la o autoritate de supraveghere, să exercite dreptul la o cale de atac în numele persoanelor vizate sau, în cazul în care se prevede în dreptul intern, să exercite dreptul de a primi despăgubiri în numele persoanelor vizate. Un stat membru poate prevedea ca un astfel de organism, organizație sau asociație să aibă dreptul de a depune o plângere în statul membru respectiv, independent de mandatul acordat de o persoană vizată, și să aibă dreptul la o cale de atac eficientă în cazul în care are motive să considere că drepturile unei persoane vizate au fost încălcate ca rezultat al unei prelucrări a datelor cu caracter personal care încalcă prezentul regulament. Organismul, organizația sau asociația în cauza nu poate pretinde despăgubiri în numele unei persoane vizate, independent de mandatul acordat de persoana vizată.(143) Orice persoană fizică sau juridică are dreptul de a introduce o acțiune în anulare împotriva deciziilor comitetului în fața Curții de Justiție, în conformitate cu condițiile prevăzute la [articolul 263 din TFUE](#). În calitate de destinatar ale acestor decizii, autoritățile de supraveghere vizate care doresc să le conteste trebuie să introducă o acțiune împotriva deciziilor respective în termen de două luni de la data la care le-au fost notificate, în conformitate cu [articolul 263 din TFUE](#). În cazul în care deciziile comitetului vizează în mod direct și individual un operator, o persoană împuternicită de operator sau reclamantul, aceștia din urmă pot introduce o acțiune în anularea respectivelor decizii în termen de două luni de la publicarea acestora pe site-ul comitetului, în conformitate cu [articolul 263 din TFUE](#). Fără a aduce atingere acestui drept în temeiul [articolului 263 din TFUE](#), orice persoană fizică sau juridică ar trebui să aibă dreptul la o cale de atac judiciară eficientă în fața instanței naționale competente împotriva unei decizii a unei autorități de supraveghere care produce efecte juridice privind respectiva persoană. O astfel de decizie se referă în special la exercitarea

competențelor de investigare, corective și de autorizare de către autoritatea de supraveghere sau la refuzul sau respingerea plângerilor. Cu toate acestea, dreptul la o cale de atac judiciară eficientă nu include măsuri ale autorităților de supraveghere care nu sunt obligatorii din punct de vedere juridic, cum ar fi avizele emise de autoritatea de supraveghere sau consiliere furnizată de aceasta. Acțiunile împotriva unei autorități de supraveghere ar trebui să fie aduse în fața instanțelor statului membru în care este stabilită autoritatea de supraveghere și ar trebui să se desfășoare în conformitate cu dreptul procesual al statului membru respectiv. Respectivul instanțe ar trebui să își exercite competența judiciară deplină, care ar trebui să includă competența de a examina toate aspectele de fapt sau de drept care au relevanță pentru litigiul cu care acestea sunt sesizate. În cazul în care o plângere a fost respinsă sau refuzată de o autoritate de supraveghere, reclamantul poate introduce o acțiune la instanțele din același stat membru. În contextul căilor de atac judiciare privind aplicarea prezentului regulament, instanțele naționale care consideră necesară o decizie privind chestiunea respectivă pentru a le permite să ia o hotărâre pot sau, în cazul prevăzut la [articolul 267 din TFUE](#), trebuie să solicite Curții de Justiție să pronunțe o decizie preliminară privind interpretarea dreptului Uniunii, inclusiv a prezentului regulament. În plus, în cazul în care o decizie a unei autorități de supraveghere care pune în aplicare o decizie a comitetului este contestată în fața unei instanțe naționale și este în discuție validitatea deciziei comitetului, respectiva instanță națională nu are competența de a declara nulă decizia comitetului, ci trebuie să aducă chestiunea validității în fața Curții de Justiție, în conformitate cu [articolul 267 din TFUE](#), astfel cum a fost interpretat de Curtea de Justiție, ori de câte ori instanța națională consideră decizia nulă. Cu toate acestea, o instanță națională nu poate să transmită o chestiune cu privire la validitatea deciziei comitetului la cererea unei persoane fizice sau juridice care a avut posibilitatea de a introduce o acțiune în anulare împotriva respectivei decizii, în special dacă aceasta era vizată în mod direct și individual de decizia în cauză, dar nu a făcut acest lucru în termenul prevăzut la [articolul 263 din TFUE](#).<sup>(144)</sup> Atunci când o instanță sesizată cu o procedură împotriva unei decizii a unei autorități de supraveghere are motive să creadă că în fața unei instanțe competente dintr-un alt stat membru au fost introduse proceduri cu privire la aceeași prelucrare, cum ar fi același obiect al prelucrării, de către același operator sau aceleași persoană împuternicită de operator, sau aceeași cauză, instanța respectivă ar trebui să contacteze cea de a doua instanță pentru a confirma existența unor astfel de proceduri conexe. În cazul în care aceste proceduri conexe se află pe rolul unei instanțe dintr-un alt stat membru, orice instanță, cu excepția celei sesizate inițial, poate să își suspende procedurile sau, la cererea uneia dintre părți, își poate declina competența în favoarea instanței sesizate inițial, cu condiția ca aceasta din urmă să aibă competența de a soluționa procedurile în cauză și ca

dreptul care i se aplică să îi permită consolidarea acestor proceduri conexe. Procedurile sunt considerate conexe atunci când sunt atât de strâns legate între ele încât este oportună instrumentarea și judecarea lor în același timp pentru a se evita riscul pronunțării unor hotărâri ireconciliabile în cazul judecării lor în mod separat.(145) În ceea ce privește acțiunile inițiate împotriva unui operator sau unei persoane împuternicite de operator, reclamantul ar trebui să aibă posibilitatea de a introduce acțiunea în fața instanțelor din statele membre în care operatorul sau persoana împuternicită de operator are un sediu sau în care persoana vizată își are reședința, cu excepția cazului în care operatorul este o autoritate publică dintr-un stat membru ce acționează în exercitarea competențelor sale publice.(146) Operatorul sau persoana împuternicită de operator ar trebui să plătească despăgubiri pentru orice prejudiciu pe care o persoană îl poate suferi ca urmare a unei prelucrări care încalcă prezentul regulament. Operatorul sau persoana împuternicită de operator ar trebui să fie exonerati de răspundere dacă dovedesc că nu sunt în niciun fel răspunzători pentru prejudiciu. Conceptul de prejudiciu ar trebui interpretat în sens larg, din perspectiva jurisprudenței Curții de Justiție, într-un mod care să reflecte pe deplin obiectivele prezentului regulament. Această dispoziție nu aduce atingere niciunei cereri de despăgubire care rezultă din încălcarea altor norme din dreptul Uniunii sau din dreptul intern. O prelucrare care încalcă prezentul regulament include și prelucrarea care încalcă actele delegate și de punere în aplicare adoptate în conformitate cu prezentul regulament și cu dreptul intern care specifică norme din prezentul regulament. Persoanele vizate ar trebui să primească despăgubiri integrale și eficace pentru prejudiciul pe care le-au suferit. În cazul în care operatorii sau persoanele împuternicite de operatori sunt implicate în aceeași prelucrare, fiecare operator sau fiecare persoană împuternicită de operator ar trebui să fie considerată răspunzătoare pentru întregul prejudiciu. Cu toate acestea, atunci când procedurile juridice care le vizează sunt conexe, în conformitate cu dreptul intern, despăgubirile pot fi împărțite în funcție de răspunderea fiecărui operator sau a fiecărei persoane împuternicite de operator, cu condiția să se asigure despăgubirea integrală și efectivă a persoanei vizate care a suferit prejudiciul. Orice operator sau persoană împuternicită de operator care a plătit despăgubiri integrale poate formula ulterior o acțiune în regres împotriva altor operatori sau persoane împuternicite de operatori implicate în aceeași prelucrare.(147) În cazul în care prezentul regulament cuprinde norme specifice privind competența judiciară, în special în ceea ce privește căile de atac judiciare, inclusiv acțiunile în despăgubiri, împotriva unui operator sau a unei persoane împuternicite de operator, normele generale privind competența judiciară precum cele din [Regulamentul \(UE\) nr. 1215/2012](#) al Parlamentului European și al Consiliului \*13) nu ar trebui să aducă atingere aplicării unor astfel de norme specifice.(148) Pentru a consolida respectarea aplicării normelor

prevăzute în prezentul regulament, ar trebui impuse sancțiuni, inclusiv amenzi administrative, pentru orice încălcare a prezentului regulament, pe lângă sau în locul măsurilor adecvate impuse de autoritatea de supraveghere în temeiul prezentului regulament. În cazul unei încălcări minore sau în cazul în care amenda susceptibilă de a fi impusă ar constitui o sarcină disproporționată pentru o persoană fizică, poate fi emis un avertisment în locul unei amenzi. Cu toate acestea, ar trebui să se ia în considerare în mod corespunzător natura, gravitatea și durata încălcării, caracterul deliberat al încălcării, acțiunile întreprinse pentru a reduce prejudiciul cauzat, gradul de răspundere sau orice încălcări anterioare relevante, modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, conformitatea cu măsurile adoptate împotriva operatorului sau a persoanei împuternicite de operator, aderarea la un cod de conduită și orice alt factor agravant sau atenuant. Impunerea de sancțiuni, inclusiv de amenzi administrative, ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu [carta](#), inclusiv o protecție judiciară eficientă și un proces echitabil.(149) Statele membre ar trebui să poată stabili normele privind sancțiunile penale pentru încălcările prezentului regulament, inclusiv pentru încălcarea normelor de drept intern adoptate în temeiul și în limitele prezentului regulament. Respectivele sancțiuni penale pot, de asemenea, permite privarea de profiturile obținute prin încălcarea prezentului regulament. Cu toate acestea, impunerea de sancțiuni penale pentru încălcări ale unor asemenea norme de drept intern și de sancțiuni administrative nu ar trebui să ducă la încălcarea principiului ne bis in idem, astfel cum a fost interpretat de Curtea de Justiție.(150) Pentru consolidarea și armonizarea sancțiunilor administrative în cazul încălcării prezentului regulament, fiecare autoritate de supraveghere ar trebui să aibă competența de a impune amenzi administrative. Prezentul regulament ar trebui să indice încălcările, și limita maximă și criteriile pentru stabilirea amenzilor administrative aferente, care ar trebui să fie stabilite de autoritatea de supraveghere competentă în fiecare caz în parte, ținând seama de toate circumstanțele relevante ale situației specifice, luându-se în considerare în mod corespunzător, în special, natura, gravitatea și durata încălcării, precum și consecințele acesteia și măsurile luate pentru a se asigura respectarea obligațiilor în temeiul prezentului regulament și pentru a se preveni sau atenua consecințele încălcării. În cazul în care amenzile administrative sunt impuse unei întreprinderi, o întreprindere ar trebui înțeleasă ca fiind o întreprindere în conformitate cu [articolele 101 și 102 din TFUE](#) în aceste scopuri. În cazul în care se impun amenzi administrative unor persoane care nu sunt întreprinderi, autoritatea de supraveghere ar trebui să țină seama de nivelul general al veniturilor din statul membru respectiv, precum și de situația economică a persoanei atunci când estimează cuantumul adecvat al amenzii. Mecanismul pentru asigurarea coerenței poate fi, de asemenea,

utilizat pentru a promova aplicarea consecventă a amenzilor administrative. Competența de a stabili dacă și în ce măsură autoritățile publice ar trebui să facă obiectul unor amenzi administrative ar trebui să revină statelor membre. Impunerea unei amenzi administrative sau transmiterea unei avertizări nu afectează aplicarea altor competențe ale autorităților de supraveghere sau a altor sancțiuni în temeiul prezentului regulament.(151) Sistemele juridice ale Danemarcei și Estoniei nu permit amenzi administrative astfel cum sunt prevăzute în prezentul regulament. Normele privind amenzile administrative pot fi aplicate astfel încât, în Danemarca, amenda să fie impusă de instanțele naționale competente ca sancțiune penală, iar în Estonia amenda să fie impusă de autoritatea de supraveghere în cadrul unei proceduri privind delictele, cu condiția ca o astfel de aplicare a normelor în statele membre respective să aibă un efect echivalent cu cel al amenzilor administrative impuse de autoritățile de supraveghere. Prin urmare, instanțele naționale competente ar trebui să țină seama de recomandarea autorității de supraveghere care a inițiat amenda. În orice caz, amenzile impuse ar trebui să fie eficace, proporționale și disuasive.(152) În cazul în care prezentul regulament nu armonizează sancțiunile administrative sau în alte cazuri, acolo unde este necesar, de exemplu în cazul unor încălcări grave ale prezentului regulament, statele membre ar trebui să pună în aplicare un sistem care să prevadă sancțiuni eficace, proporționale și disuasive. Natura unor astfel de sancțiuni, penale sau administrative, ar trebui stabilită în dreptul intern.(153) Dreptul statelor membre ar trebui să stabilească un echilibru între normele care reglementează libertatea de exprimare și de informare, inclusiv exprimarea jurnalistică, academică, artistică și/sau literară, și dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament. Prelucrarea datelor cu caracter personal exclusiv în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare ar trebui să facă obiectul unor derogări sau al unor excepții de la anumite dispoziții ale prezentului regulament în cazul în care este necesară stabilirea unui echilibru între dreptul la protecția datelor cu caracter personal și dreptul la libertatea de exprimare și de informare, astfel cum este prevăzut în [articolul 11 din cartă](#). Acest lucru ar trebui să se aplice în special prelucrării datelor cu caracter personal în domeniul audiovizualului, precum și în arhivele de știri și în bibliotecile ziarelor. Prin urmare, statele membre ar trebui să adopte măsuri legislative care să prevadă excepțiile și derogările necesare în vederea asigurării echilibrului între aceste drepturi fundamentale. Statele membre ar trebui să adopte astfel de excepții și derogări în ceea ce privește principiile generale, drepturile persoanelor vizate, operatorul și persoana împuternicită de operator, transferul de date cu caracter personal către țări terțe sau organizații internaționale, autoritățile de supraveghere independente, cooperarea și coerența, precum și în ceea ce privește situații specifice de prelucrare a datelor. În cazul în care aceste excepții sau derogări

diferă de la un stat membru la altul, ar trebui să se aplice dreptul statului membru sub incidența căruia intră operatorul. Pentru a ține seama de importanța dreptului la libertatea de exprimare în fiecare societate democratică, este necesar ca noțiunile legate de această libertate, cum ar fi jurnalismul, să fie interpretate în sens larg.(154) Prezentul regulament permite luarea în considerare a principiului accesului public la documente oficiale în aplicarea prezentului regulament. Accesul public la documente oficiale poate fi considerat a fi în interes public. Datele cu caracter personal din documentele deținute de o autoritate publică sau de un organism public ar trebui să poată fi divulgate de autoritatea respectivă sau de organismul respectiv în cazul în care dreptul Uniunii sau dreptul intern sub incidența căruia intră autoritatea publică sau organismul public prevede acest lucru. Dreptul Uniunii și dreptul intern ar trebui să asigure un echilibru între accesul public la documentele oficiale și reutilizarea informațiilor din sectorul public, pe de o parte, și dreptul la protecția datelor cu caracter personal, pe de altă parte, și ar putea prin urmare să prevadă echilibrul necesar cu dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament. Trimiterea la autoritățile și organisme publice ar trebui, în acest context, să includă toate autoritățile sau alte organisme reglementate de dreptul intern privind accesul public la documente. [Directiva 2003/98/CE](#) a Parlamentului European și a Consiliului \*14) lasă intact și nu aduce atingere în niciun fel nivelului de protecție a persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal în conformitate cu dreptul Uniunii și cu cel intern și, în special, nu modifică drepturile și obligațiile prevăzute de prezentul regulament. În special, directiva sus-menționată nu se aplică documentelor la care accesul este exclus sau restrâns în temeiul regimurilor de acces din motive legate de protecția datelor cu caracter personal și nici părților din documente accesibile în temeiul respectivelor regimuri care conțin date cu caracter personal a căror reutilizare a fost stabilită prin lege ca fiind incompatibilă cu dreptul privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.(155) Dreptul intern sau acordurile colective, inclusiv "acordurile de muncă", pot prevedea norme specifice care să reglementeze prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă, în special condițiile în care datele cu caracter personal în contextul ocupării unui loc de muncă pot fi prelucrate pe baza consimțământului angajatului, în scopul recrutării, al respectării clauzelor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii, al egalității și diversității la locul de muncă, al asigurării sănătății și securității la locul de muncă, precum și în scopul exercitării și beneficierei, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și în scopul încetării raporturilor de muncă.(156) Prelucrarea datelor cu caracter personal în scopuri de arhivare

În interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ar trebui să facă obiectul unor garanții adecvate pentru drepturile și libertățile persoanei vizate în temeiul prezentului regulament. Respectivetele garanții ar trebui să asigure faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, principiul reducerii la minimum a datelor. Prelucrarea ulterioară a datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice se efectuează atunci când operatorul a evaluat fezabilitatea pentru îndeplinirea acestor obiective prin prelucrarea unor date cu caracter personal care nu permit sau nu mai permit identificarea persoanelor vizate, cu condiția să existe garanții adecvate (cum ar fi pseudonimizarea datelor cu caracter personal). Statele membre ar trebui să prevadă garanții adecvate pentru prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. Statele membre ar trebui să fie autorizate să ofere, în anumite condiții și sub rezerva unor garanții adecvate pentru persoanele vizate, precizări și derogări în ceea ce privește cererile de informații și dreptul la rectificare, dreptul la ștergere, dreptul de a fi uitat, dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, precum și dreptul la opoziție în cazul prelucrării datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. Condițiile și garanțiile în cauză pot genera proceduri specifice astfel încât persoanele vizate să își exercite respectivele drepturi dacă acest lucru este adecvat în contextul scopurilor vizate de prelucrarea specifică, precum și măsuri tehnice și organizaționale vizând reducerea la minimum a prelucrării datelor cu caracter personal, în conformitate cu principiile proporționalității și necesității. Prelucrarea datelor cu caracter personal în scopuri științifice ar trebui să fie, de asemenea, conformă cu alte acte legislative relevante, cum ar fi cele privind studiile clinice.(157) Prin combinarea informațiilor din registre, cercetătorii pot obține noi cunoștințe de mare valoare în ceea ce privește bolile cu largă răspândire, cum ar fi bolile cardiovasculare, cancerul și depresia. Pe baza registrelor, rezultatele cercetărilor pot fi întărite, întrucât acestea se bazează pe o populație mai mare. În domeniul științelor sociale, cercetarea pe baza registrelor le permite cercetătorilor să obțină informații esențiale despre corelarea pe termen lung a unei serii de condiții sociale, precum șomajul sau educația, cu alte condiții de viață. Rezultatele cercetărilor obținute pe baza registrelor furnizează cunoștințe solide, de înaltă calitate, care pot constitui baza pentru elaborarea și punerea în aplicare a unor politici bazate pe cunoaștere și care pot îmbunătăți calitatea vieții pentru un număr de persoane, eficiența serviciilor sociale. Pentru a facilita cercetarea științifică, datele cu caracter personal pot fi prelucrate în scopuri de cercetare științifică, sub rezerva condițiilor și a garanțiilor corespunzătoare stabilite în dreptul

Uniunii sau în dreptul intern.(158) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare, prezentul regulament ar trebui să se aplice și prelucrării respective, ținând seama de faptul că prezentul regulament nu ar trebui să se aplice persoanelor decedate. Autoritățile publice sau organismele publice sau private care dețin evidențe de interes public ar trebui, în temeiul dreptului Uniunii sau al dreptului național, să aibă o obligație legală de a dobândi, a păstra, a evalua, a pregăti, a descrie, a comunica, a promova, a disemina și a asigura accesul la evidențe de valoare durabilă de interes public general. Statele membre ar trebui, de asemenea, să poată să prevadă prelucrarea ulterioară a datelor cu caracter personal în scopuri de arhivare, de exemplu cu scopul de a furniza informații specifice referitoare la comportamentul politic în perioada fostelor regimuri de stat totalitare, la genociduri, la crime împotriva umanității, în special holocaustul, sau la crime de război.(159) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică, prezentul regulament ar trebui să se aplice și prelucrării respective. În sensul prezentului regulament, prelucrarea datelor cu caracter personal în scopuri de cercetare științifică ar trebui să fie interpretată în sens larg, incluzând de exemplu dezvoltarea tehnologică și activitățile demonstrative, cercetarea fundamentală, cercetarea aplicată și cercetarea finanțată din surse private. Ar trebui, în plus, luat în considerare obiectivul Uniunii de creare a unui Spațiu european de cercetare, astfel cum este menționat la [articolul 179 alineatul \(1\) din TFUE](#). Scopurile de cercetare științifică ar trebui să includă, de asemenea, studii efectuate în interes public în domeniul sănătății publice. Pentru a îndeplini caracteristicile specifice ale prelucrării datelor cu caracter personal în scopuri de cercetare științifică, ar trebui să se aplice condiții specifice, în special în ceea ce privește publicarea sau divulgarea într-un alt mod a datelor cu caracter personal în contextul scopurilor de cercetare științifică. În cazul în care rezultatul cercetării științifice, în special în contextul sănătății, constituie un motiv pentru măsuri suplimentare în interesul persoanei vizate, normele generale ale prezentului regulament ar trebui să se aplice având în vedere aceste măsuri.(160) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare istorică, prezentul regulament ar trebui să se aplice și prelucrării respective. Acest lucru ar trebui să includă, de asemenea, cercetarea istorică și cercetarea în scopuri genealogice, ținând seama de faptul că prezentul regulament nu ar trebui să se aplice persoanelor decedate.(161) În scopul acordării consimțământului de a participa la activități de cercetare științifică în cadrul testelor clinice, ar trebui să se aplice dispozițiile relevante ale [Regulamentului \(UE\) nr. 536/2014](#) al Parlamentului European și al Consiliului \*15).(162) În cazul în care datele cu caracter personal sunt prelucrate în scopuri statistice, prezentul regulament ar trebui să se aplice prelucrării respective. Dreptul Uniunii sau dreptul intern ar trebui, în limitele prezentului regulament, să determine conținutul statistic,

controlul accesului, specificațiile pentru prelucrarea datelor cu caracter personal în scopuri statistice și măsurile adecvate pentru a proteja drepturile și libertățile persoanelor vizate și pentru a asigura confidențialitatea datelor statistice. Aceste rezultate statistice pot fi utilizate ulterior în diferite scopuri, inclusiv în scopuri de cercetare științifică. Scopuri statistice înseamnă orice operațiune de colectare și prelucrare de date cu caracter personal necesară pentru anchetele statistice sau pentru producerea de rezultate statistice. Scopurile statistice presupun că rezultatul prelucrării în scopuri statistice nu constituie date cu caracter personal, ci date agregate și că acest rezultat sau datele cu caracter personal nu sunt utilizate în sprijinul unor măsuri sau decizii privind o anumită persoană fizică.(163) Informațiile confidențiale pe care autoritățile statistice de la nivelul Uniunii și de la nivel național le colectează în vederea elaborării de statistici europene și naționale oficiale ar trebui să fie protejate. Statisticile europene ar trebui concepute, elaborate și difuzate în conformitate cu principiile statistice prevăzute la [articolul 338 alineatul \(2\) din TFUE](#), în timp ce statisticile naționale ar trebui, de asemenea, să fie în conformitate cu dreptul intern. [Regulamentul \(CE\) nr. 223/2009](#) al Parlamentului European și al Consiliului \*16) prevede specificații suplimentare privind confidențialitatea datelor statistice pentru statisticile europene.(164) În ceea ce privește competențele autorităților de supraveghere de a obține de la operator sau de la persoana împuternicită de operator accesul la datele cu caracter personal și accesul în clădirile lor, statele membre pot adopta, pe cale legislativă și în limitele stabilite de prezentul regulament, norme specifice pentru protejarea secretului profesional sau a altor obligații echivalente, în măsura în care acest lucru este necesar pentru a asigura un echilibru între dreptul la protecția datelor cu caracter personal și obligația de păstrare a secretului profesional. Aceasta nu aduce atingere obligațiilor existente ale statelor membre de a adopta norme privind secretul profesional în situațiile cerute de dreptul Uniunii.(165) Prezentul regulament respectă și nu aduce atingere statutului de care beneficiază, în temeiul dreptului constituțional existent, bisericile și asociațiile sau comunitățile religioase din statele membre, astfel cum este recunoscut în [articolul 17 din TFUE](#).(166) În vederea îndeplinirii obiectivelor prezentului regulament, și anume protejarea drepturilor și libertăților fundamentale ale persoanelor fizice și, în special, a dreptului acestora la protecția datelor cu caracter personal, și pentru a se garanta libera circulație a datelor cu caracter personal pe teritoriul Uniunii, competența de a adopta acte în conformitate cu [articolul 290 din TFUE](#) ar trebui să fie delegată Comisiei. În special, ar trebui adoptate acte delegate în ceea ce privește criteriile și cerințele privind mecanismele de certificare, informațiile care trebuie prezentate prin pictograme standardizate și procedurile pentru furnizarea unor astfel de pictograme. Este deosebit de important ca, în cadrul activității sale pregătitoare, Comisia să organizeze consultări adecvate,

inclusiv la nivel de experți. Atunci când pregătește și elaborează acte delegate, Comisia ar trebui să asigure transmiterea simultană, la timp și în mod corespunzător a documentelor relevante către Parlamentul European și către Consiliu.(167) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentului regulament, Comisia ar trebui investită cu competențe de executare în situațiile stabilite de prezentul regulament. Competențele respective ar trebui să fie exercitate în conformitate cu [Regulamentul \(UE\) nr. 182/2011](#). În acest context, Comisia ar trebui să ia în considerare măsuri specifice pentru microîntreprinderi și pentru întreprinderile mici și mijlocii.(168) Procedura de examinare ar trebui utilizată pentru adoptarea de acte de punere în aplicare privind: clauzele contractuale standard dintre operatori și persoanele împuternicite de operatori, precum și dintre persoanele împuternicite de operatori; codurile de conduită; standardele tehnice și mecanismele de certificare; nivelul adecvat de protecție oferit de o țară terță, de un teritoriu sau de un anumit sector de prelucrare din țara terță respectivă, sau de o organizație internațională; clauzele standard de protecție a datelor; formatele și procedurile pentru schimbul electronic de informații între operatori, persoanele împuternicite de operatori și autoritățile de supraveghere pentru regulile corporatiste obligatorii; asistența reciprocă; precum și modalitățile de realizare a schimbului electronic de informații între autoritățile de supraveghere, precum și între autoritățile de supraveghere și comitetul.(169) Comisia ar trebui să adopte acte de punere în aplicare imediat aplicabile atunci când dovezile disponibile arată că o țară terță, un teritoriu sau un anumit sector de prelucrare din țara terță respectivă, sau o organizație internațională nu asigură un nivel de protecție adecvat, precum și din motive imperative de urgență.(170) Deoarece obiectivul prezentului regulament, și anume asigurarea unui nivel echivalent de protecție a persoanelor fizice și libera circulație a datelor cu caracter personal în întreaga Uniune, nu poate fi realizat în mod satisfăcător de către statele membre dar, având în vedere amploarea sau efectele acțiunii, poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este definit la [articolul 5 din Tratatul](#) privind Uniunea Europeană ("[Tratatul UE](#)"). În conformitate cu principiul proporționalității, astfel cum este definit la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivelor menționate.(171) [Directiva 95/46/CE](#) ar trebui să fie abrogată prin prezentul regulament. Prelucrările în derulare la data aplicării prezentului regulament ar trebui să fie aduse în conformitate cu prezentul regulament în termen de doi ani de la data intrării în vigoare a prezentului regulament. În cazul în care prelucrările se bazează pe consimțământ în temeiul [Directivei 95/46/CE](#), nu este necesar ca persoana vizată să își dea încă o dată consimțământul în cazul în care modul în care consimțământul a fost dat este în conformitate cu condițiile din prezentul regulament, astfel încât operatorului să i se permită

să continue o astfel de prelucrare după data aplicării prezentului regulament. Deciziile adoptate ale Comisiei și autorizațiile autorităților de supraveghere emise pe baza [Directivei 95/46/CE](#) rămân în vigoare până când vor fi modificate, înlocuite sau abrogate.(172) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu [articolul 28 alineatul \(2\) din Regulamentul \(CE\) nr. 45/2001](#) și a emis un aviz la 7 martie 2012 \*17).(173) Prezentul regulament ar trebui să se aplice tuturor aspectelor referitoare la protecția drepturilor și libertăților fundamentale legate de prelucrarea datelor cu caracter personal, care nu fac obiectul unor obligații specifice cu același obiectiv ca cel stabilit în [Directiva 2002/58/CE](#) a Parlamentului European și a Consiliului \*18), inclusiv obligațiile privind operatorul și drepturile persoanelor fizice. Pentru a se clarifica relația dintre prezentul regulament și [Directiva 2002/58/CE](#), respectiva directivă ar trebui să fie modificată în consecință. După adoptarea prezentului regulament, [Directiva 2002/58/CE](#) ar trebui să fie revizuită în special pentru a se asigura coerența cu prezentul regulament,ADOPTĂ PREZENTUL REGULAMENT:☐

## Capitolul I Dispoziții generale

☐ **Articolul 1 Obiect și obiective****Articolul 2 Domeniul de aplicare material**(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.(2) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal: **(a)** în cadrul unei activități care nu intră sub incidența dreptului Uniunii; **(b)** de către statele membre atunci când desfășoară activități care intră sub incidența [capitolului 2 al titlului V din Tratatul UE](#); **(c)** de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice; **(d)** de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor, sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.(3) Pentru prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii, se aplică [Regulamentul \(CE\) nr. 45/2001](#).[Regulamentul \(CE\) nr. 45/2001](#) și alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal se adaptează la principiile și normele din prezentul regulament în conformitate cu articolul 98.(4) Prezentul regulament nu aduce atingere aplicării [Directivei 2000/31/CE](#), în special normelor privind răspunderea furnizorilor de servicii intermediari, prevăzute la articolele 12-15 din directiva menționată.**Articolul 3 Domeniul de aplicare teritorial**(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de

operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.(2) Prezentul regulament se aplică prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activitățile de prelucrare sunt legate de: **(a)** oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată; sau **(b)** monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.(3) Prezentul regulament se aplică prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internațional public.**Articolul 4 Definiții**În sensul prezentului regulament: **1.** "date cu caracter personal" înseamnă orice informații privind o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale; **2.** "prelucrare" înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea; **3.** "restricționarea prelucrării" înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora; **4.** "creare de profiluri" înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia; **5.** "pseudonimizare" înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile; **6.** "sistem de evidență a datelor" înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau

geografice;**7.** "operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;**8.** "persoană împuternicită de operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;**9.** "destinatar" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;**10.** "parte terță" înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;**11.** "consimțământ" al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;**12.** "încălcarea securității datelor cu caracter personal" înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;**13.** "date genetice" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;**14.** "date biometrice" înseamnă o date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;**15.** "date privind sănătatea" înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;**16.** "sediul principal" înseamnă: **(a)** în cazul unui operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a

acestui în Uniune, cu excepția cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are competența de a dispune punerea în aplicare a acestor decizii, caz în care sediul care a luat deciziile respective este considerat a fi sediul principal; **(b)** în cazul unei persoane împuternicite de operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acesteia în Uniune, sau, în cazul în care persoana împuternicită de operator nu are o administrație centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activitățile principale de prelucrare, în contextul activităților unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligații specifice în temeiul prezentului regulament; **17.** "reprezentant" înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul [articolului 27](#), care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul prezentului regulament; **18.** "întreprindere" înseamnă o persoană fizică sau juridică ce desfășoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații care desfășoară în mod regulat o activitate economică; **19.** "grup de întreprinderi" înseamnă o întreprindere care exercită controlul și întreprinderile controlate de aceasta; **20.** "reguli corporatiste obligatorii" înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună; **21.** "autoritate de supraveghere" înseamnă o autoritate publică independentă instituită de un stat membru în temeiul [articolului 51](#); **22.** "autoritate de supraveghere vizată" înseamnă o autoritate de supraveghere care este vizată de procesul de prelucrare a datelor cu caracter personal deoarece: **(a)** operatorul sau persoana împuternicită de operator este stabilită pe teritoriul statului membru al autorității de supraveghere respective; **(b)** persoanele vizate care își au reședința în statul membru în care se află autoritatea de supraveghere respectivă sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare; sau **(c)** la autoritatea de supraveghere respectivă a fost depusă o plângere; **23.** "prelucrare transfrontalieră" înseamnă: **(a)** fie prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre; sau **(b)** fie prelucrarea datelor cu caracter

personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre;

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

**25.** "serviciile societății informaționale" înseamnă un serviciu astfel cum este definit la articolul 1 alineatul (1) litera (b) din [Directiva 2015/1535/CE](#) a Parlamentului European și a Consiliului (\*19);

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

## **Capitolul II Principii** **Articolul 5 Principii legate de prelucrarea datelor cu caracter personal**

(1) Datele cu caracter personal sunt: **(a)** prelucrate în mod legal, echitabil și transparent față de persoana vizată ("legalitate, echitate și transparență"); **(b)** colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89 alineatul (1) ("limitări legate de scop"); **(c)** adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate ("reducerea la minimum a datelor"); **(d)** exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere ("exactitate"); **(e)** păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu [articolul 89 alineatul \(1\)](#), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate ("limitări legate de stocare"); **(f)** prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării

neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("integritate și confidențialitate").(2) Operatorul este responsabil de respectarea [alineatului \(1\)](#) și poate demonstra această respectare ("responsabilitate").**Articolul 6 Legalitatea prelucrării**(1) Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții: **(a)** persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice; **(b)** prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract; **(c)** prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului; **(d)** prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice; **(e)** prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul; **(f)** prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.Litera (f) din primul paragraf nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor.(2) Statele membre pot menține sau introduce dispoziții mai specifice de adaptare a aplicării normelor prezentului regulament în ceea ce privește prelucrarea în vederea respectării [alineatului \(1\) literele \(c\) și \(e\)](#) prin definirea unor cerințe specifice mai precise cu privire la prelucrare și a altor măsuri de asigurare a unei prelucrări legale și echitabile, inclusiv pentru alte situații concrete de prelucrare, astfel cum este prevăzut în [capitolul IX](#).(3) Temeiul pentru prelucrarea menționată la [alineatul \(1\) literele \(c\) și \(e\)](#) trebuie să fie prevăzut în: **(a)** dreptul Uniunii; sau **(b)** dreptul intern care se aplică operatorului.Scopul prelucrării este stabilit pe baza respectivului temei juridic sau, în ceea ce privește prelucrarea menționată la [alineatul \(1\) litera \(e\)](#), este necesar pentru îndeplinirea unei sarcini efectuate în interes public sau în cadrul exercitării unei funcții publice atribuite operatorului. Respectivul temei juridic poate conține dispoziții specifice privind adaptarea aplicării normelor prezentului regulament, printre altele: condițiile generale care reglementează legalitatea prelucrării de către operator; tipurile de date care fac obiectul prelucrării; persoanele vizate; entitățile cărora le pot fi divulgate datele și scopul pentru care respectivele date cu caracter personal pot fi divulgate; limitările legate de scop; perioadele de stocare; și operațiunile și procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale și echitabile cum sunt cele pentru alte situații concrete de prelucrare astfel cum sunt prevăzute

în [capitolul IX](#). Dreptul Uniunii sau dreptul intern urmărește un obiectiv de interes public și este proporțional cu obiectivul legitim urmărit.(4) În cazul în care prelucrarea în alt scop decât cel pentru care datele cu caracter personal au fost colectate nu se bazează pe consimțământul persoanei vizate sau pe dreptul Uniunii sau dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja obiectivele menționate la [articolul 23 alineatul \(1\)](#), operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial, ia în considerare, printre altele: **(a)** orice legătură dintre scopurile în care datele cu caracter personal au fost colectate și scopurile prelucrării ulterioare preconizate; **(b)** contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește relația dintre persoanele vizate și operator; **(c)** natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date cu caracter personal, în conformitate cu [articolul 9](#), sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale și infracțiuni, în conformitate cu [articolul 10](#); **(d)** posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate; **(e)** existența unor garanții adecvate, care pot include criptarea sau pseudonimizarea. **Articolul 7 Condiții privind consimțământul**(1) În cazul în care prelucrarea se bazează pe consimțământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal.(2) În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Nicio parte a respectivei declarații care constituie o încălcare a prezentului regulament nu este obligatorie.(3) Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragera consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragera consimțământului se face la fel de simplu ca acordarea acestuia.(4) Atunci când se evaluează dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract. **Articolul 8 Condiții aplicabile în ceea ce privește consimțământul copiilor în legătură cu serviciile societății informaționale**(1) În cazul în care se aplică [articolul 6 alineatul \(1\) litera \(a\)](#), în ceea ce privește oferirea de servicii ale societății informaționale în mod direct unui copil, prelucrarea datelor cu caracter personal ale unui copil este legală dacă copilul are cel puțin vârsta de 16 ani.

Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului. Statele membre pot prevedea prin lege o vârstă inferioară în aceste scopuri, cu condiția ca acea vârstă inferioară să nu fie mai mică de 13 ani. (2) Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile. (3) [Alineatul \(1\)](#) nu afectează dreptul general al contractelor aplicabil în statele membre, cum ar fi normele privind valabilitatea, încheierea sau efectele unui contract în legătură cu un copil.

**Articolul 9 Prelucrarea de categorii speciale de date cu caracter personal** (1) Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice. (2) [Alineatul \(1\)](#) nu se aplică în următoarele situații: **(a)** persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicția prevăzută la [alineatul \(1\)](#) să nu poată fi ridicată prin consimțământul persoanei vizate; **(b)** prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate; **(c)** prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul; **(d)** prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate; **(e)** prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată; **(f)** prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare; **(g)** prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu

obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate; **(h)** prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la [alineatul \(3\)](#); **(i)** prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional; sau **(j)** prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu [articolul 89 alineatul \(1\)](#), în baza dreptului Uniunii sau al dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate.

(3) Datele cu caracter personal menționate la [alineatul \(1\)](#) pot fi prelucrate în scopurile menționate la [alineatul \(2\) litera \(h\)](#) în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naționale competente.

(4) Statele membre pot menține sau introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea de date genetice, date biometrice sau date privind sănătatea.

**Articolul 10 Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni**

Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni sau la măsuri de securitate conexe în temeiul [articolului 6 alineatul \(1\)](#) se efectuează numai sub controlul unei autorități de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorități de stat.

**Articolul 11 Prelucrarea care nu necesită identificare**(1) În cazul în care scopurile pentru care un operator prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate

de către operator, operatorul nu are obligația de a păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizată în scopul unic al respectării prezentului regulament.(2) Dacă, în cazurile menționate la [alineatul \(1\)](#) din prezentul articol, operatorul poate demonstra că nu este în măsură să identifice persoana vizată, operatorul informează persoana vizată în mod corespunzător, în cazul în care este posibil. În astfel de cazuri, [articolele 15-20](#) nu se aplică, cu excepția cazului în care persoana vizată, în scopul exercitării drepturilor sale în temeiul respectivelor articole, oferă informații suplimentare care permit identificarea sa.

### **Capitolul III Drepturile persoanei vizate** **Secțiunea 1 Transparență și**

#### **modalități** **Articolul 12 Transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate**

(1) Operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informații menționate la [articolele 13 și 14](#) și orice comunicări în temeiul [articolelor 15-22 și 34](#) referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil. Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.(2) Operatorul facilitează exercitarea drepturilor persoanei vizate în temeiul [articolelor 15-22](#). În cazurile menționate la [articolul 11 alineatul \(2\)](#), operatorul nu refuză să dea curs cererii persoanei vizate de a-și exercita drepturile în conformitate cu [articolele 15-22](#), cu excepția cazului în care operatorul demonstrează că nu este în măsură să identifice persoana vizată.(3) Operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri în temeiul [articolelor 15-22](#), fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.(4) Dacă nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoana vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară.(5) Informațiile furnizate în temeiul [articolelor 13 și 14](#) și orice comunicare și orice măsuri luate în temeiul [articolelor 15-22 și 34](#) sunt oferite gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul

poate: **(a)** fie să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate; **(b)** fie să refuze să dea curs cererii. În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii. (6) Fără a aduce atingere [articolului 11](#), în cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea menționată la [articolele 15-21](#), operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate. (7) Informațiile care urmează să fie furnizate persoanelor vizate în temeiul [articolelor 13 și 14](#) pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea trebuie să poată fi citite automat. (8) Comisia este împuternicită să adopte acte delegate în conformitate cu [articolul 92](#) în vederea determinării informațiilor care urmează să fie prezentate de pictograme și a procedurilor pentru furnizarea de pictograme standardizate.

**Secțiunea 2 Informare și acces la date cu caracter personal**

**Articolul 13 Informații care se furnizează în cazul în care datele cu caracter personal sunt colectate de la persoana vizată** (1) În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obținerii acestor date cu caracter personal, furnizează persoanei vizate toate informațiile următoare: **(a)** identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia; **(b)** datele de contact ale responsabilului cu protecția datelor, după caz; **(c)** scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării; **(d)** în cazul în care prelucrarea se face în temeiul [articolului 6 alineatul \(1\) litera \(f\)](#), interesele legitime urmărite de operator sau de o parte terță; **(e)** destinatarii sau categoriile de destinatari ai datelor cu caracter personal; **(f)** dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menționate la [articolul 46](#) sau [47](#) sau la [articolul 49 alineatul \(1\) al doilea paragraf](#), o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție. (2) În plus față de informațiile menționate la [alineatul \(1\)](#), în momentul în care datele cu caracter personal sunt obținute, operatorul furnizează persoanei vizate următoarele informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă: **(a)** perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă; **(b)** existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau

ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor; **(c)** atunci când prelucrarea se bazează pe [articolul 6 alineatul \(1\) litera \(a\)](#) sau pe [articolul 9 alineatul \(2\) litera \(a\)](#), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia; **(d)** dreptul de a depune o plângere în fața unei autorități de supraveghere; **(e)** dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații; **(f)** existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la [articolul 22 alineatele \(1\) și \(4\)](#), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată. (3) În cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu [alineatul \(2\)](#). (4) [Alineatele \(1\), \(2\) și \(3\)](#) nu se aplică dacă și în măsura în care persoana vizată deține deja informațiile respective. **Articolul 14 Informații care se furnizează în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată** (1) În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informații: **(a)** identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia; **(b)** datele de contact ale responsabilului cu protecția datelor, după caz; **(c)** scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării; **(d)** categoriile de date cu caracter personal vizate; **(e)** destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz; **(f)** dacă este cazul, intenția operatorului de a transfera date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menționate la [articolul 46](#) sau [47](#) sau la [articolul 49 alineatul \(1\) al doilea paragraf](#), o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție. (2) Pe lângă informațiile menționate la [alineatul \(1\)](#), operatorul furnizează persoanei vizate următoarele informații necesare pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată: **(a)** perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă; **(b)** în cazul în care prelucrarea se face în

temeiul [articolului 6 alineatul \(1\) litera \(f\)](#), interesele legitime urmărite de operator sau de o parte terță; **(c)** existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării și a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor; **(d)** atunci când prelucrarea se bazează pe [articolul 6 alineatul \(1\) litera \(a\)](#) sau pe [articolul 9 alineatul \(2\) litera \(a\)](#), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia; **(e)** dreptul de a depune o plângere în fața unei autorități de supraveghere; **(f)** sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public; **(g)** existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la [articolul 22 alineatele \(1\) și \(4\)](#), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată. (3) Operatorul furnizează informațiile menționate la [alineatele \(1\) și \(2\)](#): **(a)** într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal; **(b)** dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă; sau **(c)** dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară. (4) În cazul în care operatorul intenționează să prelucrez ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obținute, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu [alineatul \(2\)](#). (5) [Alineatele \(1\)-\(4\)](#) nu se aplică dacă și în măsura în care: **(a)** persoana vizată deține deja informațiile; **(b)** furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva condițiilor și a garanțiilor prevăzute la [articolul 89 alineatul \(1\)](#), sau în măsura în care obligația menționată la [alineatul \(1\)](#) din prezentul articol este susceptibilă să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective. În astfel de cazuri, operatorul ia măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate, inclusiv punerea informațiilor la dispoziția publicului; **(c)** obținerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern sub incidența căruia intră operatorul și care prevede măsuri adecvate pentru a proteja interesele

legitime ale persoanei vizate; sau **(d)** în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligații legale de a păstra secretul. **Articolul 15 Dreptul de acces al persoanei vizate** (1) Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații: **(a)** scopurile prelucrării; **(b)** categoriile de date cu caracter personal vizate; **(c)** destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale; **(d)** acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă; **(e)** existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării; **(f)** dreptul de a depune o plângere în fața unei autorități de supraveghere; **(g)** în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora; **(h)** existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la [articolul 22 alineatele \(1\) și \(4\)](#), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată. (2) În cazul în care datele cu caracter personal sunt transferate către o țară terță sau o organizație internațională, persoana vizată are dreptul să fie informată cu privire la garanțiile adecvate în temeiul articolului 46 referitoare la transfer. (3) Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative. În cazul în care persoana vizată introduce cererea în format electronic și cu excepția cazului în care persoana vizată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent. (4) Dreptul de a obține o copie menționată la [alineatul \(3\)](#) nu aduce atingere drepturilor și libertăților altora. **Secțiunea 3 Rectificare și ștergere** **Articolul 16 Dreptul la rectificare** Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare. **Articolul 17 Dreptul la ștergerea datelor ("dreptul de a fi uitat")** (1) Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri

nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive: **(a)** datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate; **(b)** persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea, în conformitate cu [articolul 6 alineatul \(1\) litera \(a\)](#) sau cu [articolul 9 alineatul \(2\) litera \(a\)](#), și nu există niciun alt temei juridic pentru prelucrarea; **(c)** persoana vizată se opune prelucrării în temeiul [articolului 21 alineatul \(1\)](#) și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării în temeiul [articolului 21 alineatul \(2\)](#); **(d)** datele cu caracter personal au fost prelucrate ilegal; **(e)** datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul; **(f)** datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la [articolul 8 alineatul \(1\)](#).

(2) În cazul în care operatorul a făcut publice datele cu caracter personal și este obligat, în temeiul [alineatului \(1\)](#), să le șteargă, operatorul, ținând seama de tehnologia disponibilă și de costul implementării, ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

(3) [Alineatele \(1\) și \(2\)](#) nu se aplică în măsura în care prelucrarea este necesară: **(a)** pentru exercitarea dreptului la liberă exprimare și la informare; **(b)** pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul; **(c)** din motive de interes public în domeniul sănătății publice, în conformitate cu [articolul 9 alineatul \(2\) literele \(h\) și \(i\)](#) și cu [articolul 9 alineatul \(3\)](#); **(d)** în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu [articolul 89 alineatul \(1\)](#), în măsura în care dreptul menționat la [alineatul \(1\)](#) este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau **(e)** pentru constatarea, exercitarea sau apărarea unui drept în instanță.

**Articolul 18 Dreptul la restricționarea prelucrării**

(1) Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării în cazul în care se aplică unul din următoarele cazuri: **(a)** persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor; **(b)** prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor; **(c)** operatorul nu

mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță; sau **(d)** persoana vizată s-a opus prelucrării în conformitate cu [articolul 21 alineatul \(1\)](#), pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate. (2) În cazul în care prelucrarea a fost restricționată în temeiul [alineatului \(1\)](#), astfel de date cu caracter personal pot, cu excepția stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru. (3) O persoană vizată care a obținut restricționarea prelucrării în temeiul [alineatului \(1\)](#) este informată de către operator înainte de ridicarea restricției de prelucrare.

**Articolul 19 Obligația de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării** Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate în conformitate cu [articolul 16](#), [articolul 17 alineatul \(1\)](#) și [articolul 18](#), cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

**Articolul 20 Dreptul la portabilitatea datelor** (1) Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, în cazul în care: **(a)** prelucrarea se bazează pe consimțământ în temeiul [articolului 6 alineatul \(1\) litera \(a\)](#) sau al [articolului 9 alineatul \(2\) litera \(a\)](#) sau pe un contract în temeiul [articolului 6 alineatul \(1\) litera \(b\)](#); și **(b)** prelucrarea este efectuată prin mijloace automate. (2) În exercitarea dreptului său la portabilitatea datelor în temeiul [alineatului \(1\)](#), persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic. (3) Exercitarea dreptului menționat la [alineatul \(1\)](#) din prezentul articol nu aduce atingere [articolului 17](#). Respectivul drept nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este investit operatorul. (4) Dreptul menționat la [alineatul \(1\)](#) nu aduce atingere drepturilor și libertăților altora.

**Secțiunea 4 Dreptul la opoziție și procesul decizional individual automatizat**

**Articolul 21 Dreptul la opoziție** (1) În orice moment, persoana vizată are dreptul să se opună, din motive legate de situația particulară în care se află, prelucrării în temeiul [articolului 6 alineatul \(1\) litera \(e\)](#) sau [\(f\)](#), a datelor cu caracter personal care o privesc, inclusiv

creării de profiluri pe baza respectivelor dispoziții. Operatorul nu mai prelucrează datele cu caracter personal, cu excepția cazului în care operatorul demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.(2) Atunci când prelucrarea datelor cu caracter personal are drept scop marketingul direct, persoana vizată are dreptul de a se opune în orice moment prelucrării în acest scop a datelor cu caracter personal care o privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv.(3) În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.(4) Cel târziu în momentul primei comunicări cu persoana vizată, dreptul menționat la [alineatele \(1\) și \(2\)](#) este adus în mod explicit în atenția persoanei vizate și este prezentat în mod clar și separat de orice alte informații.(5) În contextual utilizării serviciilor societății informaționale și în pofida [Directivei 2002/58/CE](#), persoana vizată își poate exercita dreptul de a se opune prin mijloace automate care utilizează specificații tehnice.(6) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică sau în scopuri statistice în conformitate cu [articolul 89 alineatul \(1\)](#), persoana vizată, din motive legate de situația sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepția cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.**Articolul 22 Procesul decizional individual automatizat, inclusiv crearea de profiluri**(1) Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.(2) [Alineatul \(1\)](#) nu se aplică în cazul în care decizia: **(a)** este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date; **(b)** este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului și care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate; sau **(c)** are la bază consimțământul explicit al persoanei vizate.(3) În cazurile menționate la [alineatul \(2\) literele \(a\) și \(c\)](#), operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia.(4) Deciziile menționate la [alineatul \(2\)](#) nu au la bază categoriile speciale de date cu caracter personal menționate la [articolul 9 alineatul \(1\)](#), cu excepția cazului în care se aplică [articolul 9 alineatul \(2\) litera \(a\)](#) sau [\(g\)](#) și în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei

vizate. **Secțiunea 5 Restricții** **Articolul 23 Restricții** (1) Dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la [articolele 12-22](#) și [34](#), precum și la [articolul 5](#) în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la [articolele 12-22](#), atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura: **(a)** securitatea națională; **(b)** apărarea; **(c)** securitatea publică; **(d)** prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora; **(e)** alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale; **(f)** protejarea independenței judiciare și a procedurilor judiciare; **(g)** prevenirea, investigarea, depistarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate; **(h)** funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale în cazurile menționate la [literele \(a\)-\(e\)](#) și [\(g\)](#); **(i)** protecția persoanei vizate sau a drepturilor și libertăților altora; **(j)** punerea în aplicare a pretențiilor de drept civil. (2) În special, orice măsură legislativă menționată la [alineatul \(1\)](#) conține dispoziții specifice cel puțin, dacă este cazul, în ceea ce privește: **(a)** scopurile prelucrării sau ale categoriilor de prelucrare; **(b)** categoriile de date cu caracter personal; **(c)** domeniul de aplicare al restricțiilor introduse; **(d)** garanțiile pentru a preveni abuzurile sau accesul sau transferul ilegal; **(e)** menționarea operatorului sau a categoriilor de operatori; **(f)** perioadele de stocare și garanțiile aplicabile având în vedere natura, domeniul de aplicare și scopurile prelucrării sau ale categoriilor de prelucrare; **(g)** riscurile pentru drepturile și libertățile persoanelor vizate; și **(h)** dreptul persoanelor vizate de a fi informate cu privire la restricție, cu excepția cazului în care acest lucru poate aduce atingere scopului restricției.

## **Capitolul IV Operatorul și persoana împuternicită de operator** **Secțiunea**

**1 Obligații generale** **Articolul 24 Responsabilitatea operatorului** (1) Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar. (2) Atunci când sunt proporționale în raport cu operațiunile de prelucrare, măsurile menționate la [alineatul \(1\)](#) includ punerea în aplicare de

către operator a unor politici adecvate de protecție a datelor.(3) Aderarea la coduri de conduită aprobate, menționate la [articolul 40](#), sau la un mecanism de certificare aprobat, menționat la [articolul 42](#), poate fi utilizată ca element care să demonstreze respectarea obligațiilor de către operator.**Articolul 25 Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit**(1) Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.(2) Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane.(3) Un mecanism de certificare aprobat în conformitate cu [articolul 42](#) poate fi utilizat drept element care să demonstreze îndeplinirea cerințelor prevăzute la [alineatele \(1\) și \(2\)](#) ale prezentului articol.**Articolul 26 Operatori asociați**(1) În cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați. Ei stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul prezentului regulament, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute la [articolele 13 și 14](#), prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.(2) Acordul menționat la [alineatul \(1\)](#) reflectă în mod adecvat rolurile și raporturile respective ale operatorilor asociați față de persoanele vizate. Esența acestui acord este făcută cunoscută persoanei vizate.(3) Indiferent de clauzele acordului menționat la [alineatul \(1\)](#), persoana vizată își poate exercita drepturile în temeiul prezentului regulament cu privire la și în raport cu fiecare dintre operatori.**Articolul 27 Reprezentanții operatorilor sau ai persoanelor împuternicite de operatori care nu își au sediul în Uniune**(1) În cazul în care se aplică [articolul 3 alineatul \(2\)](#), operatorul sau persoana împuternicită de

operator desemnează în scris un reprezentant în Uniune.(2) Obligația prevăzută la [alineatul \(1\)](#) din prezentul articol nu se aplică: **(a)** prelucrării care are un caracter ocazional, care nu include, pe scară largă, prelucrarea unor categorii speciale de date, astfel cum se prevede la [articolul 9 alineatul \(1\)](#), sau prelucrarea unor date cu caracter personal referitoare la condamnări penale și infracțiuni menționată la [articolul 10](#), și care este puțin susceptibilă de a genera un risc pentru drepturile și libertățile persoanelor, ținând cont de natura, contextul, domeniul de aplicare și scopurile prelucrării; sau **(b)** unei autorități sau unui organism public.(3) Reprezentantul își are sediul în unul dintre statele membre în care se află persoanele vizate ale căror date cu caracter personal sunt prelucrate în legătură cu furnizarea de bunuri și servicii sau al căror comportament este monitorizat.(4) Reprezentantul primește din partea operatorului sau a persoanei împuternicite de operator un mandat prin care autoritățile de supraveghere și persoanele vizate, în special, se pot adresa reprezentantului, în plus față de operator sau persoana împuternicită de operator sau în locul acestora, cu privire la toate chestiunile legate de prelucrarea, în scopul asigurării respectării prezentului regulament.(5) Desemnarea unui reprezentant de către operator sau persoana împuternicită de operator nu aduce atingere acțiunilor în justiție care ar putea fi introduse împotriva operatorului sau persoanei împuternicite de operator înseși.**Articolul 28 Persoana împuternicită de operator**(1) În cazul în care prelucrarea urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate.(2) Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecții față de aceste modificări.(3) Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoană împuternicită de operator: **(a)** prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, inclusiv în ceea ce privește transferurile de date cu caracter personal către o țară terță sau o organizație internațională, cu excepția

cazului în care această obligație îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public; **(b)** se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație statutară adecvată de confidențialitate; **(c)** adoptă toate măsurile necesare în conformitate cu [articolul 32](#); **(d)** respectă condițiile menționate la [alineatele \(2\) și \(4\)](#) privind recrutarea unei alte persoane împuternicite de operator; **(e)** ținând seama de natura prelucrării, oferă asistență operatorului prin măsuri tehnice și organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligației operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute în [capitolul III](#); **(f)** ajută operatorul să asigure respectarea obligațiilor prevăzute la [articolele 32-36](#), ținând seama de caracterul prelucrării și informațiile aflate la dispoziția persoanei împuternicite de operator; **(g)** la alegerea operatorului, șterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal; **(h)** pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute la prezentul articol, permite desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea. În ceea ce privește primul paragraf [litera \(h\)](#), persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucțiune încalcă prezentul regulament sau alte dispoziții din dreptul intern sau din dreptul Uniunii referitoare la protecția datelor. (4) În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator, astfel cum se prevede la [alineatul \(3\)](#), revin celei de a doua persoane împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul dreptului Uniunii sau al dreptului intern, în special furnizarea de garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentului regulament. În cazul în care această a doua persoană împuternicită nu își respectă obligațiile privind protecția datelor, persoana împuternicită inițială rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor acestei a doua persoane împuternicite. (5) Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, menționat la [articolul 40](#), sau la un mecanism de

certificare aprobat, menționat la [articolul 42](#), poate fi utilizată ca element prin care să se demonstreze existența garanțiilor suficiente menționate la [alineatele \(1\) și \(4\)](#) din prezentul articol.(6) Fără a aduce atingere unui contract individual încheiat între operator și persoana împuternicită de operator, contractul sau celălalt act juridic menționat la [alineatele \(3\) și \(4\)](#) din prezentul articol se poate baza, integral sau parțial, pe clauze contractuale standard menționate la [alineatele \(7\) și \(8\)](#) din prezentul articol, inclusiv atunci când fac parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator în temeiul [articolelor 42 și 43](#).(7) Comisia poate să prevadă clauze contractuale standard pentru aspectele menționate la [alineatele \(3\) și \(4\)](#) din prezentul articol și în conformitate cu procedura de examinare menționată la [articolul 93 alineatul \(2\)](#).(8) O autoritate de supraveghere poate să adopte clauze contractuale standard pentru aspectele menționate la [alineatele \(3\) și \(4\)](#) din prezentul articol și în conformitate cu mecanismul pentru asigurarea coerenței menționat la [articolul 63](#).(9) Contractul sau celălalt act juridic menționat la [alineatele \(3\) și \(4\)](#) se formulează în scris, inclusiv în format electronic.(10) Fără a aduce atingere [articolelor 82, 83 și 84](#), în cazul în care o persoană împuternicită de operator încalcă prezentul regulament, prin stabilirea scopurilor și mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă.**Articolul 29 Desfășurarea activității de prelucrare sub autoritatea operatorului sau a persoanei împuternicite de operator**Persoana împuternicită de operator și orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru.**Articolul 30 Evidențele activităților de prelucrare**(1) Fiecare operator și, după caz, reprezentantul acestuia păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor. Respectiva evidență cuprinde toate următoarele informații: **(a)** numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor; **(b)** scopurile prelucrării; **(c)** o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal; **(d)** categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale; **(e)** dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor menționate la [articolul 49 alineatul \(1\) al doilea paragraf](#), documentația care dovedește existența unor garanții adecvate; **(f)** acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date; **(g)** acolo unde este posibil, o descriere generală a măsurilor tehnice și

organizatorice de securitate menționate la [articolul 32 alineatul \(1\)](#).(2) Fiecare persoană împuternicită de operator și, după caz, reprezentantul persoanei împuternicite de operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind: **(a)** numele și datele de contact ale persoanei sau persoanelor împuternicite de operator și ale fiecărui operator în numele căruia acționează această persoană (aceste persoane), precum și, după caz, ale reprezentantului operatorului sau ale reprezentantului persoanei împuternicite de operator, și ale responsabilului cu protecția datelor; **(b)** categoriile de activități de prelucrare desfășurate în numele fiecărui operator; **(c)** dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor prevăzute la [articolul 49 alineatul \(1\) al doilea paragraf](#), documentația care dovedește existența unor garanții adecvate; **(d)** acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la [articolul 32 alineatul \(1\)](#).(3) Evidențele menționate la [alineatele \(1\) și \(2\)](#) se formulează în scris, inclusiv în format electronic.(4) Operatorul sau persoana împuternicită de acesta, precum și, după caz, reprezentantul operatorului sau al persoanei împuternicite de operator pun evidențele la dispoziția autorității de supraveghere, la cererea acesteia.(5) Obligațiile menționate la [alineatele 1 și 2](#) nu se aplică unei întreprinderi sau organizații cu mai puțin de 250 de angajați, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la [articolul 9 alineatul \(1\)](#), sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează la articolul 10.

**Articolul 31 Cooperarea cu autoritatea de supraveghere** Operatorul și persoana împuternicită de operator și, după caz, reprezentantul acestora cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor acesteia.

**Secțiunea 2 Securitatea datelor cu caracter personal**

**Articolul 32 Securitatea prelucrării** (1) Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz: **(a)** pseudonimizarea și criptarea datelor cu caracter personal; **(b)** capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare; **(c)** capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident

de natură fizică sau tehnică; **(d)** un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.(2) La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.(3) Aderarea la un cod de conduită aprobat, menționat la [articolul 40](#), sau la un mecanism de certificare aprobat, menționat la [articolul 42](#), poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute la [alineatul \(1\)](#) din prezentul articol.(4) Operatorul și persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.**Articolul 33 Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal**(1) În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere competente în temeiul [articolului 55](#), fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea către autoritatea de supraveghere nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată pentru întârziere.(2) Persoana împuternicită de operator înștiințează operatorul fără întârzieri nejustificate după ce ia cunoștință de o încălcare a securității datelor cu caracter personal.(3) Notificarea menționată la [alineatul \(1\)](#) cel puțin: **(a)** descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză; **(b)** comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații; **(c)** descrie consecințele probabile ale încălcării securității datelor cu caracter personal; **(d)** descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.(4) Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.(5) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor

acestea și a măsurilor de remediere întreprinse. Această documentație permite autorității de supraveghere să verifice conformitatea cu prezentul articol.

**Articolul 34 Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal**(1) În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.(2) În informarea transmisă persoanei vizate prevăzută la [alineatul \(1\)](#) din prezentul articol se include o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile și măsurile menționate la [articolul 33 alineatul \(3\) literele \(b\), \(c\) și \(d\)](#).(3) Informarea persoanei vizate menționată la [alineatul \(1\)](#) nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită: **(a)** operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea; **(b)** operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate menționat la [alineatul \(1\)](#) nu mai este susceptibil să se materializeze; **(c)** ar necesita un efort disproporționat. În această situație, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.(4) În cazul în care operatorul nu a comunicat deja încălcarea securității datelor cu caracter personal către persoana vizată, autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securității datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condițiile menționate la [alineatul \(3\)](#) sunt îndeplinite.

**Secțiunea 3 Evaluarea impactului asupra protecției datelor și consultarea prealabilă**

**Articolul 35 Evaluarea impactului asupra protecției datelor**(1) Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.(2) La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat.(3) Evaluarea impactului asupra protecției datelor menționată la [alineatul \(1\)](#) se impune mai ales în cazul: **(a)** unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se

bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă; **(b)** prelucrării pe scară largă a unor categorii speciale de date, menționată la [articolul 9 alineatul \(1\)](#), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la [articolul 10](#); sau **(c)** unei monitorizări sistematice pe scară largă a unei zone accesibile publicului. (4) Autoritatea de supraveghere întocmește și publică o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor, în conformitate cu [alineatul \(1\)](#). Autoritatea de supraveghere comunică aceste liste comitetului menționat la [articolul 68](#). (5) Autoritatea de supraveghere poate, de asemenea, să stabilească și să pună la dispoziția publicului o listă a tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor. Autoritatea de supraveghere comunică aceste liste comitetului. (6) Înainte de adoptarea listelor menționate la [alineatele \(4\) și \(5\)](#), autoritatea de supraveghere competentă aplică mecanismul pentru asigurarea coerenței menționat la articolul 63 în cazul în care aceste liste implică activități de prelucrare care presupun furnizarea de bunuri sau prestarea de servicii către persoane vizate sau monitorizarea comportamentului acestora în mai multe state membre ori care pot afecta în mod substanțial libera circulație a datelor cu caracter personal în cadrul Uniunii. (7) Evaluarea conține cel puțin: **(a)** o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator; **(b)** o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri; **(c)** o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la [alineatul \(1\)](#); și **(d)** măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate. (8) La evaluarea impactului operațiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatorii relevante, se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate menționate la [articolul 40](#), în special în vederea unei evaluări a impactului asupra protecției datelor. (9) Operatorul solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare. (10) Atunci când prelucrarea în temeiul [articolului 6 alineatul \(1\) litera \(c\)](#) sau [\(e\)](#) are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidența căruia intră operatorul, iar dreptul respectiv

reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, [alineatele \(1\)-\(7\)](#) nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.(11) Acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.**Articolul 36 Consultarea prealabilă**(1) Operatorul consultă autoritatea de supraveghere înainte de prelucrarea atunci când evaluarea impactului asupra protecției datelor prevăzută la [articolul 35](#) indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.(2) Atunci când consideră că prelucrarea prevăzută menționată la [alineatul \(1\)](#) ar încălca prezentul regulament, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris operatorului și, după caz, persoanei împuternicite de operator, în cel mult opt săptămâni de la primirea cererii de consultare, și își poate utiliza oricare dintre competențele menționate la [articolul 58](#). Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute. Autoritatea de supraveghere informează operatorul și, după caz, persoana împuternicită de operator, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când autoritatea de supraveghere a obținut informațiile pe care le-a solicitat în scopul consultării.(3) Atunci când consultă autoritatea de supraveghere în conformitate cu [alineatul \(1\)](#), operatorul îi furnizează acesteia: **(a)** dacă este cazul, responsabilitățile respective ale operatorului, ale operatorilor asociați și ale persoanelor împuternicite de operator implicate în activitățile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi; **(b)** scopurile și mijloacele prelucrării preconizate; **(c)** măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților persoanelor vizate, în conformitate cu prezentul regulament; **(d)** dacă este cazul, datele de contact ale responsabilului cu protecția datelor; **(e)** evaluarea impactului asupra protecției datelor prevăzută la [articolul 35](#); și **(f)** orice alte informații solicitate de autoritatea de supraveghere.(4) Statele membre consultă autoritatea de supraveghere în cadrul procesului de pregătire a unei propuneri de măsură legislativă care urmează să fie adoptată de un parlament național sau a unei măsuri de reglementare întemeiate pe o astfel de măsură legislativă, care se referă la prelucrarea.(5) În pofida [alineatului \(1\)](#), dreptul intern poate impune operatorilor să se consulte cu autoritatea de supraveghere și să obțină în

prealabil autorizarea din partea acestora în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecția socială și sănătatea publică.

**Secțiunea 4 Responsabilul cu protecția datelor****Articolul 37 Desemnarea responsabilului cu protecția datelor**

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

- (a) prelucrarea este efectuată de o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;
- (b) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă;
- sau (c) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date în temeiul [articolului 9](#) sau a unor date cu caracter personal referitoare la condamnări penale și infracțiuni, menționată la [articolul 10](#).

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

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

(4) În alte cazuri decât cele menționate la [alineatul \(1\)](#), operatorul sau persoana împuternicită de operator ori asociațiile și alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot desemna sau, acolo unde dreptul Uniunii sau dreptul intern solicită acest lucru, desemnează un responsabil cu protecția datelor. Responsabilul cu protecția datelor poate să acționeze în favoarea unor astfel de asociații și alte organisme care reprezintă operatori sau persoane împuternicite de operatori.

(5) Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la [articolul 39](#).

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

(7) Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecția datelor și le comunică autorității de supraveghere.

**Articolul 38 Funcția responsabilului cu protecția datelor**

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

(2) Operatorul și persoana împuternicită de operator sprijină responsabilul cu protecția datelor în

îndeplinirea sarcinilor menționate la [articolul 39](#), asigurându-i resursele necesare pentru executarea acestor sarcini, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate.(3) Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini. Acesta nu este demis sau sancționat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.(4) Persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentului regulament.(5) Responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.(6) Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese.**Articolul 39 Sarcinile responsabilului cu protecția datelor**(1) Responsabilul cu protecția datelor are cel puțin următoarele sarcini:**(a)** informarea și consilierea operatorului, sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;**(b)** monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;**(c)** furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu [articolul 35](#);**(d)** cooperarea cu autoritatea de supraveghere;**(e)** asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la [articolul 36](#), precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.(2) În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.**Secțiunea 5 Coduri de conduită și certificare****Articolul 40 Coduri de conduită**(1) Statele membre, autoritățile de supraveghere, comitetul și Comisia încurajează elaborarea de coduri de conduită menite să contribuie la buna aplicare a prezentului regulament, ținând seama de caracteristicile specifice ale diverselor sectoare de prelucrare

și de nevoile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii.(2) Asociațiile și alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot pregăti coduri de conduită sau le pot modifica sau extinde pe cele existente, în scopul de a specifica modul de aplicare a prezentului regulament, cum ar fi în ceea ce privește:(a) prelucrarea în mod echitabil și transparent;(b) interesele legitime urmărite de operatori în contexte specifice;(c) colectarea datelor cu caracter personal;(d) pseudonimizarea datelor cu caracter personal;(e) informarea publicului și a persoanelor vizate;(f) exercitarea drepturilor persoanelor vizate;(g) informarea și protejarea copiilor și modalitatea în care trebuie obținut consimțământul titularilor răspunderii părintești asupra copiilor;(h) măsurile și procedurile menționate la [articolele 24 și 25](#) și măsurile de asigurare a securității prelucrării, menționate la [articolul 32](#);(i) notificarea autorităților de supraveghere cu privire la încălcările securității datelor cu caracter personal și informarea persoanelor vizate cu privire la aceste încălcări;(j) transferul de date cu caracter personal către țări terțe sau organizații internaționale; sau(k) proceduri extrajudiciare și alte proceduri de soluționare a litigiilor pentru soluționarea litigiilor între operatori și persoanele vizate în ceea ce privește prelucrarea, fără a aduce atingere drepturilor persoanelor vizate, în temeiul [articolelor 77 și 79](#).(3) La codurile de conduită aprobate în temeiul [alineatului \(5\)](#) din prezentul articol și care au o valabilitate generală în temeiul [alineatului \(9\)](#) din prezentul articol pot adera nu numai operatorii sau persoanele împuternicite de operatori care fac obiectul prezentului regulament, ci și operatorii sau persoanele împuternicite de operatori care nu fac obiectul prezentului regulament în temeiul [articolului 3](#), în scopul de a oferi garanții adecvate în cadrul transferurilor de date cu caracter personal către țări terțe sau organizații internaționale în condițiile menționate la [articolul 46 alineatul \(2\) litera \(e\)](#). Acești operatori sau persoane împuternicite de operatori își asumă angajamente cu caracter obligatoriu și executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, în scopul aplicării garanțiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.(4) Codul de conduită prevăzut la [alineatul \(2\)](#) din prezentul articol cuprinde mecanisme care permit organismului menționat la [articolul 41 alineatul \(1\)](#) să efectueze monitorizarea obligatorie a respectării dispozițiilor acestuia de către operatorii sau persoanele împuternicite de operatori care se angajează să îl aplice, fără a aduce atingere sarcinilor și competențelor autorităților de supraveghere care sunt competente în temeiul [articolului 55](#) sau [56](#).(5) Asociațiile și alte organisme menționate la [alineatul \(2\)](#) din prezentul articol care intenționează să pregătească un cod de conduită sau să modifice sau să extindă un cod existent transmit proiectul de cod, de modificare sau de extindere autorității de supraveghere care este competentă în temeiul [articolului 55](#). Autoritatea

de supraveghere emite un aviz cu privire la conformitatea cu prezentul regulament a proiectului de cod, de modificare sau de extindere și îl aprobă în cazul în care se constată că acesta oferă garanții adecvate suficiente.(6) În cazul în care proiectul de cod, de modificare sau de extindere este aprobat în conformitate cu [alineatul \(5\)](#), iar codul de conduită în cauză nu are legătură cu activitățile de prelucrare din mai multe state membre, autoritatea de supraveghere înregistrează și publică codul.(7) În cazul în care un proiect de cod de conduită, de modificare sau de extindere are legătură cu activitățile de prelucrare din mai multe state membre, înainte de aprobare, autoritatea de supraveghere competentă în temeiul [articolului 55](#) îl transmite, prin procedura menționată la [articolul 63](#), comitetului, care emite un aviz cu privire la conformitatea cu prezentul regulament a proiectului respectiv, sau, în situația menționată la [alineatul \(3\)](#) din prezentul articol, oferă garanții adecvate.(8) În cazul în care avizul menționat la [alineatul \(7\)](#) confirmă conformitatea cu prezentul regulament a proiectului de cod, de modificare sau de extindere sau în cazul în care, în situația menționată la [alineatul \(3\)](#), oferă garanții adecvate, comitetul transmite avizul său Comisiei.(9) Comisia poate adopta acte de punere în aplicare pentru a decide că codul de conduită, modificarea sau extinderea aprobate care i-au fost prezentate în temeiul alineatului (8) din prezentul articol au valabilitate generală în Uniune. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la [articolul 93 alineatul \(2\)](#).(10) Comisia asigură publicitatea adecvată pentru codurile aprobate asupra cărora s-a decis că au valabilitate generală în conformitate cu [alineatul \(9\)](#).(11) Comitetul regroupează toate codurile de conduită, modificările și extinderile aprobate într-un registru și le pune la dispoziția publicului prin mijloace corespunzătoare.**Articolul 41 Monitorizarea codurilor de conduită aprobate**(1) Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente în temeiul [articolelor 57](#) și [58](#), monitorizarea respectării unui cod de conduită în temeiul [articolului 40](#) poate fi realizată de un organism care dispune de un nivel adecvat de expertiză în legătură cu obiectul codului și care este acreditat în acest scop de autoritatea de supraveghere competentă.(2) Un organism menționat la [alineatul \(1\)](#) poate fi acreditat pentru monitorizarea respectării unui cod de conduită dacă: **(a)** a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, independența și expertiza sa în legătură cu obiectul codului; **(b)** a instituit proceduri care îi permit să evalueze eligibilitatea operatorilor și a persoanelor împuternicite de operatori în vederea aplicării codului, să monitorizeze respectarea de către aceștia a dispozițiilor codului și să revizuiască periodic funcționarea acestuia; **(c)** a instituit proceduri și structuri pentru tratarea plângerilor privind încălcări ale codului sau privind modul în care codul a fost sau este pus în aplicare de un operator sau o persoană împuternicită de operator, precum și pentru asigurarea transparenței acestor proceduri și

structuri pentru persoanele vizate și pentru public; și **(d)** a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, că sarcinile și atribuțiile sale nu creează conflicte de interese. (3) Autoritatea de supraveghere competentă transmite proiectul de cerințe pentru acreditarea unui organism menționat la [alineatul \(1\)](#) din prezentul articol comitetului, în conformitate cu mecanismul pentru asigurarea coerenței menționat la [articolul 63](#). (4) Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente și dispozițiilor [capitolului VIII](#), un organism menționat la [alineatul \(1\)](#) din prezentul articol ia măsuri corespunzătoare, sub rezerva unor garanții adecvate, în cazul încălcării codului de către un operator sau o persoană împuternicită de operator, inclusiv prin suspendarea sau excluderea respectivului operator sau a respectivei persoane din cadrul codului. Organismul în cauză informează autoritatea de supraveghere competentă cu privire la aceste măsuri și la motivele care le-au determinat. (5) Autoritatea de supraveghere competentă revocă acreditarea unui organism menționat la [alineatul \(1\)](#) în cazul în care nu mai sunt îndeplinite cerințele pentru acreditare sau măsurile luate de organismul în cauză încalcă prezentul regulament. (6) Prezentul articol nu se aplică prelucrării efectuate de autorități și organisme publice. **Articolul**

**42 Certificare** (1) Statele membre, autoritățile de supraveghere, comitetul și Comisia încurajează, în special la nivelul Uniunii, instituirea de mecanisme de certificare în domeniul protecției datelor, precum și de sigilii și mărci în acest domeniu, care să permită demonstrarea faptului că operațiunile de prelucrare efectuate de operatori și de persoanele împuternicite de operatori respectă prezentul regulament. Sunt luate în considerare necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii. (2) Mecanismele de certificare din domeniul protecției datelor, sigiliile sau mărcile aprobate în temeiul [alineatului \(5\)](#) din prezentul articol sunt instituite nu numai pentru a fi respectate de operatorii sau de persoanele împuternicite de operatori care fac obiectul prezentului regulament, ci și pentru a demonstra existența unor garanții adecvate oferite de operatorii sau de persoanele împuternicite de operatori care nu fac obiectul prezentului regulament, în temeiul [articolului 3](#), în cadrul transferurilor de date cu caracter personal către țări terțe sau organizații internaționale în condițiile menționate la [articolul 46 alineatul \(2\) litera \(f\)](#). Acești operatori sau persoane împuternicite de operatori își asumă angajamente cu caracter obligatoriu și executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, în scopul aplicării garanțiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate. (3) Certificarea este voluntară și disponibilă prin intermediul unui proces transparent. (4) Certificarea în conformitate cu prezentul articol nu reduce responsabilitatea operatorului sau a persoanei împuternicite de operator de a respecta prezentul regulament și nu aduce atingere sarcinilor și competențelor autorităților de supraveghere

care sunt competente în temeiul [articolului 55](#) sau [56](#).(5) Organismele de certificare menționate la [articolul 43](#) sau autoritatea de supraveghere competentă emit o certificare în temeiul prezentului articol, pe baza criteriilor aprobate de către autoritatea de supraveghere competentă respectivă în temeiul [articolului 58 alineatul \(3\)](#), sau de către comitet în temeiul [articolului 63](#). În cazul în care criteriile sunt aprobate de comitet, aceasta poate duce la o certificare comună, și anume sigiliul european privind protecția datelor.(6) Operatorul sau persoana împuternicită de operator care supune activitățile sale de prelucrare mecanismului de certificare oferă organismului de certificare menționat la [articolul 43](#) sau, după caz, autorității de supraveghere competente, toate informațiile necesare pentru desfășurarea procedurii de certificare, precum și accesul la activitățile de prelucrare respective.(7) Certificarea este eliberată unui operator sau unei persoane împuternicite de operator pentru o perioadă maximă de trei ani și poate fi reînnoită în aceleași condiții, cu condiția ca criteriile relevante să fie îndeplinite în continuare. Certificarea este retrasă, după caz, de către organismele de certificare menționate la [articolul 43](#) sau de către autoritatea de supraveghere competentă în cazul în care nu mai sunt îndeplinite criteriile pentru certificare.(8) Comitetul regroupează toate mecanismele de certificare și sigiliile și mărcile de protecție a datelor într-un registru și le pune la dispoziția publicului prin orice mijloc corespunzător.**Articolul 43 Organisme de certificare**(1) Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente, prevăzute la [articolele 57 și 58](#), organismele de certificare care dispun de un nivel adecvat de competență în domeniul protecției datelor, după ce informează autoritatea de supraveghere pentru a-i permite să își exercite competențele în temeiul [articolului 58 alineatul \(2\) litera \(h\)](#), emit și reînnoiesc certificarea. Statele membre se asigură că aceste organisme de certificare sunt acreditate de către una sau amândouă dintre următoarele entități: **(a)** autoritatea de supraveghere care este competentă în temeiul [articolului 55](#) sau [56](#); **(b)** organismul național de acreditare desemnat în conformitate cu [Regulamentul \(CE\) nr. 765/2008](#) al Parlamentului European și al Consiliului \*20) în conformitate cu standardul EN-ISO/IEC 17065/2012 și cu cerințele suplimentare stabilite de autoritatea de supraveghere care este competentă în temeiul [articolului 55](#) sau [56](#).(2) Un organism de certificare menționat la [alineatul \(1\)](#) este acreditat în conformitate cu alineatul respectiv numai dacă: **(a)** a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, independența și expertiza sa în legătură cu obiectul certificării; **(b)** s-a angajat să respecte criteriile menționate la [articolul 42 alineatul \(5\)](#) și aprobate de autoritatea de supraveghere care este competentă în temeiul [articolului 55](#) sau [56](#), sau de către comitet în temeiul [articolului 63](#); **(c)** a instituit proceduri pentru emiterea, revizuirea periodică și retragerea certificării, a sigiliilor și mărcilor din domeniul protecției datelor; **(d)** a instituit proceduri și structuri pentru

tratarea plângerilor privind încălcări ale certificării sau privind modul în care certificarea a fost sau este pusă în aplicare de un operator sau o persoană împuternicită de operator, precum și pentru asigurarea transparenței acestor proceduri și structuri pentru persoanele vizate și pentru public; și **(e)** a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, că sarcinile și atribuțiile sale nu creează conflicte de interese.(3) Acreditarea organismelor de certificare menționate la [alineatele \(1\) și \(2\)](#) din prezentul articol se realizează pe baza cerințelor aprobate de către autoritatea de supraveghere care este competentă în temeiul [articolului 55](#) sau [56](#), sau de către comitet în temeiul articolului 63. În cazul unei acreditări în temeiul [alineatului \(1\) litera \(b\)](#) din prezentul articol, aceste cerințe le completează pe cele prevăzute în [Regulamentul \(CE\) nr. 765/2008](#) și normele tehnice care descriu metodele și procedurile organismelor de certificare.(4) Organismele de certificare menționate la [alineatul \(1\)](#) sunt responsabile cu realizarea unei evaluări adecvate în vederea certificării sau retragerii acestei certificări, fără a aduce atingere responsabilității operatorului sau a persoanei împuternicite de operator de a respecta prezentul regulament. Acreditarea se eliberează pentru o perioadă maximă de cinci ani și poate fi reînnoită în aceleași condiții, cu condiția ca organismul de certificare să îndeplinească cerințele prevăzute în prezentul articol.(5) Organismele de certificare menționate la [alineatul \(1\)](#) transmite autorităților de supraveghere competente motivele acordării sau retragerii certificării solicitate.(6) Cerințele menționate la [alineatul \(3\)](#) din prezentul articol și criteriile menționate la [articolul 42 alineatul \(5\)](#) se publică de către autoritatea de supraveghere într-o formă ușor de accesat. Autoritățile de supraveghere transmit, de asemenea, aceste cerințe și criterii comitetului.(7) Fără a aduce atingere dispozițiilor [capitolului VIII](#), autoritatea de supraveghere competentă sau organismul național de acreditare revocă acreditarea acordată unui organism de certificare în temeiul [alineatului \(1\)](#) din prezentul articol în cazul în care nu sunt sau nu mai sunt îndeplinite condițiile pentru acreditare sau măsurile luate de organismul de acreditare încalcă prezentul regulament.(8) Comisia este împuternicită să adopte acte delegate în conformitate cu [articolul 92](#), în scopul specificării cerințelor care trebuie luate în considerare pentru mecanismele de certificare din domeniul protecției datelor, menționate la [articolul 42 alineatul \(1\)](#).(9) Comisia poate adopta acte de punere în aplicare pentru a stabili standarde tehnice pentru mecanismele de certificare și pentru sigiliile și mărcile din domeniul protecției datelor, precum și mecanisme de promovare și recunoaștere a acelor mecanisme de certificare, sigilii și mărci. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la [articolul 93 alineatul \(2\)](#).