Consiliul
Uniunii Europene

Bruxelles, 11 iunie 2015
(OR. en)

9565/15

Dosar interinstituțional:
2012/0011 (COD)

DATAPROTECT 97
JAI 420
MI 369
DIGIT 49
DAPIX 94
FREMP 133
COMIX 259
CODEC 823

NOTĂ

Sursă:	Președinția
Destinatar:	Consiliul
Nr. doc. ant.:	9398/15
Subiect:	Propunere de regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor) - Pregătirea abordării generale

Introducere

La 25 ianuarie 2012, Comisia și-a adoptat propunerea de regulament general privind protecția datelor (5853/12). Noul regulament este menit să înlocuiască Directiva 95/46/CE. Dublul obiectiv al regulamentului este de a consolida drepturile persoanelor fizice în materie de protecție a datelor și de a îmbunătăți oportunitățile de afaceri prin facilitarea liberei circulații a datelor cu caracter personal în cadrul pieței unice digitale.

În paralel cu propunerea de regulament general privind protecția datelor, Comisia a adoptat o comunicare generală care expune obiectivele Comisiei (5852/12) și o directivă privind prelucrarea datelor în scopul aplicării legii (5833/12). Noua directivă este menită să înlocuiască Decizia-cadru privind protecția datelor din 2008.

Parlamentul European și-a adoptat pozițiile în primă lectură cu privire la propunerile de regulament privind protecția datelor și de directivă privind protecția datelor la 12 martie 2014.

Textul de compromis

Mai multe abordări generale parțiale au contribuit esențial la existența unor opinii convergente în cadrul Consiliului privind propunerea de regulament general privind protecția datelor în toate elementele sale. Textul regulamentului pe care Președinția îl înaintează spre aprobare ca abordare generală este redat în anexă. Toate modificările față de propunerea inițială a Comisiei sunt indicate prin caractere subliniate; porțiunile de text eliminate sunt marcate cu (…). În cazurile în care porțiuni de text existente au fost mutate, acestea sunt indicate prin *caractere cursive*. Observațiile delegațiilor cu privire la textul regulamentului - care nu conținea încă noile propuneri ale Președinției privind considerentele 118 și 134 - sunt prezentate în rezultatul lucrărilor reuniunii Comitetului Reprezentanților Permanenți din 9 iunie 2015 (9788/15).

În urma reuniunii Comitetului Reprezentanților Permanenți din 9 iunie 2015, Președinția a efectuat două modificări.

Dreptul la despăgubiri și răspunderea - articolul 77 și considerentul (118)

Președinția propune modificarea considerentului (118) pentru a clarifica faptul că obiectivul principal al articolul 77 și al considerentului (118) este de a garanta despăgubirea integrală și efectivă a persoanei vizate pentru daunele suferite. Ținând seama de faptul că sistemele juridice pentru tratarea cazurilor de răspundere diferă de la un stat membru la altul, persoana vizată poate primi astfel despăgubiri de la un operator sau o persoană împuternicită de operator care este considerat(ă) răspunzător (răspunzătoare) pentru întreaga daună sau, în statele membre al căror sistem juridic prevede proceduri conexate, despăgubirile pot fi împărțite între mai mulți operatori sau mai multe persoane împuternicite de operator.

Aplicarea regulamentului - considerentul (134)

Pentru a asigura un nivel suficient de securitate juridică pentru operatorii și persoanele împuternicite de operatori ale căror operațiuni de prelucrare a datelor cu caracter personal sunt conforme cu Directiva 95/46/CE, Președinția propune clarificarea domeniului de aplicare al regulamentului în cadrul considerentului (134).

Concluzie

Pentru a oferi Președinției un mandat de a se angaja în negocieri cu reprezentanții Parlamentului European, Consiliul este invitat să aprobe textul Regulamentului general privind protecția datelor, astfel cum figurează în anexă ca abordare generală.

ANEXĂ

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor)

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European,

după consultarea Autorității Europene pentru Protecția Datelor,

hotărând în conformitate cu procedura legislativă ordinară,

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 și articolul 16 alineatul (1) din tratat prevăd că orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.

2) Principiile (…) și normele privind protecția persoanelor fizice referitor la 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. Aceasta ar trebui 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 din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date vizează armonizarea nivelului de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește activitățile de prelucrare și garantarea liberei circulații a datelor cu caracter personal între statele membre.

(3a) 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 principiile recunoscute în Carta drepturilor fundamentale a Uniunii Europene consacrată în tratate, în special dreptul la respectarea vieții private și de familie, a reședinței și a secretului comunicațiilor, dreptul la protecția datelor cu caracter personal, libertatea de gândire, de conștiință și de religie, libertatea de exprimare și de informare, libertatea 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.

4) Integrarea economică și socială care rezultă din funcționarea pieței interne a condus la o creștere substanțială a fluxurilor transfrontaliere. Schimbul de date între (…) actori publici și privați, inclusiv persoane fizice și întreprinderi, s-a intensificat în întreaga Uniune. Conform dreptului Uniunii, autoritățile naționale 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.

5) Evoluțiile tehnologice rapide și globalizarea au generat noi provocări pentru protecția datelor cu caracter personal. Amploarea schimbului și a colectării de date a crescut spectaculos. 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 multe persoane 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 în cadrul Uniunii și transferul către țări terțe și organizații internaționale, asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal.

6) 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.

(6a) În cazul în care prezentul regulament prevede specificări sau restricționări ale normelor sale în temeiul dreptului statelor membre, statele membre pot, în măsura în care acest lucru este necesar pentru coerență și pentru a asigura înțelegerea dispozițiilor naționale de către persoanele cărora acestea li se aplică, să încorporeze elemente din regulament în dreptul lor intern respectiv.

7) 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, incertitudinea juridică și percepția publică larg răspândită conform căreia există riscuri semnificative pentru protecția persoanelor fizice care au legătură, în special, 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 permisă în 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.

8) 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 învestit 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. În limitele acestei marje de manevră, legile sectoriale pe care statele membre le-au emis în punerea în aplicare a Directivei 95/46/CE ar trebui să poată fi admise.

9) Protecția efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea și detalierea 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 autorii infracțiunilor în statele membre.

10) Articolul 16 alineatul (2) din tratat 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.

11) 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 garantate din punct de vedere juridic, de obligații și de responsabilități 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 efectivă 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 mai multe derogări. În plus, instituțiile și organismele Uniunii, 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 Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii.

12) Protecția conferită de prezentul regulament vizează persoanele fizice, indiferent de cetățenia sau de locul de reședință al acestora, în ceea ce privește prelucrarea datelor cu caracter personal. Referitor la prelucrarea datelor care privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și detaliile de contact ale persoanei juridice, protecția conferită de prezentul regulament nu ar trebui să poată fi invocată de nicio asemenea persoană. (…).

13) Protecția persoanelor fizice ar trebui să fie neutră din punct de vedere tehnologic și să nu depindă de tehnicile utilizate, în caz contrar creându-se un risc serios de eludare. 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 sunt cuprinse sau destinate să fie cuprinse într-un sistem de evidență. Dosarele sau seturile de dosare, precum și copertele acestora, care nu sunt structurate în conformitate cu criterii specifice, nu ar trebui să intre în domeniul de aplicare a prezentului regulament.

14) Prezentul regulament nu se referă nici la chestiuni de protecție a drepturilor și libertăților fundamentale, nici la libera circulație a datelor referitoare la activități care nu intră în domeniul de aplicare al dreptului Uniunii, de exemplu activități privind securitatea națională, (…) nici nu reglementează prelucrarea datelor cu caracter personal de către statele membre atunci când acestea desfășoară activități legate de politica externă și de securitate comună a Uniunii.

(14a) Regulamentul (CE) nr. 45/2001 se aplică prelucrării datelor cu caracter personal de către instituțiile, organismele, oficiile și agențiile Uniunii. Regulamentul (CE) nr. 45/2001 și alte instrumente juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal ar trebui adaptate la principiile și normele din prezentul regulament.

15) Prezentul regulament nu ar trebui să se aplice prelucrării datelor cu caracter personal de către o persoană fizică în cadrul unei activități personale sau domestice și care, prin urmare, nu are legătură cu o activitate profesională sau comercială. Activitățile personale și domestice includ activitățile în cadrul rețelelor sociale și activitățile online desfășurate în contextul respectivelor activități personale sau domestice. Cu toate acestea, prezentul regulament ar trebui (…) să se aplice operatorilor sau persoanelor împuternicite de către operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activități personale sau domestice.

16) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, identificării sau urmăririi penale a infracțiunilor**,** al executării pedepselor, al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, precum și al liberei circulații a acestor date face obiectul unui instrument juridic specific la nivelul Uniunii.

Prin urmare, prezentul regulament nu ar trebui să se aplice activităților de prelucrare în aceste scopuri. Cu toate acestea, datele prelucrate de către autoritățile publice în temeiul prezentului regulament, în cazul în care sunt utilizate în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor ar trebui să fie reglementate de respectivul instrument juridic mai specific la nivelul Uniunii (Directiva XX/YYY). Statele membre pot încredința autorităților competente în sensul Directivei XX/YYY alte sarcini care nu sunt neapărat îndeplinite în scopul prevenirii, identificării, investigării, detectării sau urmăririi penale a infracțiunilor sau 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, intră 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 Regulamentului general privind protecția datelor, statele membre pot menține sau introduce dispoziții mai concrete pentru a adapta aplicarea normelor din Regulamentul general privind protecția datelor. 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, incluzând siguranța publică și prevenirea, identificarea, investigarea și urmărirea penală a infracțiunilor. Acest lucru este relevant, de exemplu, în contextul combaterii spălării de bani sau al activităților laboratoarelor criminalistice.

(16a) *Deşi prezentul regulament se aplică şi în cazul activităţilor instanţelor* şi ale altor autorităţi judiciare, dreptul Uniunii sau al statelor membre ar putea să precizeze operaţiunile şi procedurile de prelucrare în ceea ce priveşte prelucrarea datelor cu caracter personal de către instanţe şi alte autorităţi judiciare. *Prelucrarea datelor cu caracter personal nu ar trebui să fie de competenţa autorităţilor de supraveghere în cazul în care instanţele îşi exercită atribuţiile judiciare*, în scopul garantării independenţei sistemului judiciar în îndeplinirea sarcinilor sale judiciare, inclusiv în luarea deciziilor. Supravegherea unor astfel de operaţiuni de prelucrare a datelor poate fi încredinţată unor organisme specifice din cadrul sistemului judiciar al statului membru, care ar trebui să verifice în special respectarea normelor prevăzute de prezentul regulament, să promoveze conştientizarea de către sistemul judiciar a obligaţiilor care îi revin în temeiul prezentului regulament şi să se ocupe de plângeri în legătură cu astfel de operaţiuni de prelucrare.

17) Directiva 2000/31/CE nu se aplică chestiunilor referitoare la serviciile societăţii informaţionale care fac obiectul prezentului regulament. Respectiva directivă îşi propune să contribuie la buna funcţionare a pieţei interne, prin asigurarea liberei circulaţii a serviciilor societăţii informaţionale între statele membre. Aplicarea sa nu ar trebui să fie afectată de prezentul regulament. Prezentul regulament nu ar trebui, prin urmare, să aducă atingere aplicării Directivei 2000/31/CE, în special normelor privind răspunderea furnizorilor intermediari de servicii, prevăzute la articolele 12 - 15 din directiva menţionată.

18) (…)

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

20) 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 își au reședința în Uniune de către un operator 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 care are loc în Uniune. Pentru a determina dacă un asemenea operator oferă bunuri sau servicii unor astfel de persoane vizate în Uniune, ar trebui să se stabilească dacă reiese că operatorul intenționează să desfășoare activități comerciale cu persoanele vizate care își au reședința în unul sau mai multe state membre în Uniune. Întrucât simplul fapt că există acces la un site internet al operatorului sau al unui intermediar în Uniune sau că este disponibilă o adresă de e-mail și alte date de contact sau că este utilizată o limbă utilizată 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 și/sau menționarea unor clienți sau utilizatori care își au reședința în Uniune pot conduce la concluzia că operatorul intenționează să ofere bunuri sau servicii unor astfel de persoane vizate în Uniune.

21) Prelucrarea datelor cu caracter personal ale persoanelor vizate care își au reședința în Uniune de către un operator 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 respectivelor persoane care are loc pe teritoriul Uniunii Europene. 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 cu tehnici de prelucrare a datelor 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.

22) În cazul în care dreptul intern al 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.

23) Principiile protecției datelor ar trebui să se aplice oricărei informații referitoare la o persoană fizică identificată sau identificabilă. Datele care includ date pseudonimizate, 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 este identificabilă, ar trebui să se ia în considerare toate mijloacele care pot fi utilizate în mod rezonabil fie de operator, fie de orice altă persoană în scopul identificării persoanei fizice respective, în mod direct sau indirect. Pentru a se determina ce mijloace este posibil, în mod rezonabil, să fie utilizate 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 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 pentru cercetare. .

(23aa)Principiile protecției datelor nu ar trebui să se aplice datelor referitoare la persoane decedate. Dreptul intern al unui stat membru poate să prevadă norme privind prelucrarea datelor referitoare la persoane decedate.

(23a)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 diverse articole din prezentul regulament nu este, așadar, destinată să împiedice alte eventuale măsuri de protecție a datelor.

(23b)(...)

(23c) Pentru a crea stimulente pentru aplicarea pseudonimizării atunci când sunt prelucrate date cu caracter personal, ar trebui să fie posibile măsuri de pseudonimizare, permiţând, în acelaşi timp, analiza generală, în cadrul aceluiaşi operator atunci când operatorul a luat măsurile tehnice şi organizatorice necesare pentru a se asigura că dispoziţiile prezentului regulament sunt puse în aplicare, ţinând seama de respectiva prelucrare a datelor şi asigurând faptul că informaţiile suplimentare pentru atribuirea datelor cu caracter personal unei anumite persoane vizate sunt păstrate separat. Operatorul care prelucrează datele se referă, de asemenea, la persoanele autorizate din cadrul aceluiaşi operator. Totuşi, într-un asemenea caz, operatorul se asigură că persoana (persoanele) care efectuează pseudonimizarea nu este (nu sunt) menţionată (menţionate) în metadate.

24) Atunci când utilizează servicii online, persoanele fizice pot fi asociate cu identificatorii online furnizaţi de dispozitivele, aplicaţiile, instrumentele şi protocoalele lor, cum ar fi adresele IP sau identificatorii cookie. Aceştia pot lăsa urme care, atunci când sunt combinate cu identificatorii unici şi alte informaţii primite de servere, pot fi utilizate pentru crearea de profiluri ale persoanelor fizice şi pentru identificarea lor. Numerele de identificare, datele de localizare, identificatorii online sau alţi factori specifici nu ar trebui (…) să fie consideraţi ca atare date cu caracter personal, dacă aceştia nu identifică o persoană sau nu fac identificabilă o persoană.

25) Consimţământul ar trebui acordat în mod explicit prin orice metodă corespunzătoare care permite manifestarea liberă, specifică şi informată a voinţei persoanei vizate, fie printr-o declaraţie scrisă, inclusiv electronică, fie verbală, fie, dacă acest lucru este necesar în anumite circumstanţe, prin orice altă acţiune neechivocă a persoanei vizate, care să însemne consimţământul său pentru prelucrarea datelor sale cu caracter personal. Acesta ar putea include bifarea unei căsuţe atunci când persoana vizitează un site internet sau orice altă declaraţie sau acţiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absenţa unui răspuns sau a unei acţiuni nu ar trebui să constituie un consimţământ. Dacă este fezabil şi eficient din punct de vedere tehnic, consimţământul persoanei vizate pentru prelucrarea datelor sale cu caracter personal poate fi dat prin utilizarea setărilor corespunzătoare ale unui program de navigare sau ale altei aplicaţii. În astfel de cazuri, este suficient dacă persoana vizată primeşte informaţiile necesare pentru a-şi da consimţământul în mod liber, specific şi informat atunci când începe să utilizeze serviciul. (…). Consimţământul ar trebui să vizeze toate activităţile de prelucrare efectuate în acelaşi scop sau în aceleaşi scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimţământul neechivoc ar trebui dat pentru toate scopurile prelucrării. În cazul în care consimţământul persoanei vizate trebuie acordat în urma unei cereri electronice, aceasta trebuie să fie clară şi concisă şi să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimţământul.

(25a) Datele genetice ar trebui definite drept date cu caracter personal referitoare la caracteristicile genetice ale unei persoane, care au fost moștenite sau dobândite, astfel cum rezultă în urma unei analize a unei mostre de material biologic al persoanei în cauză, în special a unei analize cromozomiale, a unei analize a acidului dezoxiribonucleic (ADN) sau a acidului ribonucleic (ARN) sau a unei analize a oricărui alt element ce permite obţinerea unor informaţii echivalente.

(25aa)Adesea nu este posibil să se identifice pe deplin scopul prelucrării datelor în scopuri ştiinţifice în momentul colectării datelor. Din acest motiv, persoanele vizate pot să își dea consimțământul pentru anumite domenii ale cercetării ştiinţifice atunci când sunt respectate standardele etice recunoscute pentru cercetarea ştiinţifică. Persoanele vizate ar trebui să aibă posibilitatea de a-și exprima consimțământul doar pentru anumite domenii de cercetare sau părți ale proiectelor de cercetare în măsura permisă de scopul preconizat și cu condiția ca acest lucru să nu implice eforturi disproporționate ținând seama de obiectivul de protecție urmărit.

26) Datele cu caracter personal privind sănătatea ar trebui să includă (…) date având legătură cu starea de sănătate a persoanei vizate, care să dezvăluie informații despre starea de sănătate fizică sau mentală trecută, prezentă sau viitoare a persoanei vizate, incluzând informații privind: înscrierea persoanei fizice pentru acordarea de servicii de sănătate (…); un număr, simbol sau semn distinctiv atribuit unei persoane fizice pentru identificarea unică a acesteia în scopuri medicale; (…) informații rezultate din testarea sau examinarea unei părți a corpului sau a unei substanțe corporale, inclusiv date genetice și eșantioane de material biologic; (…) orice informații privind, de exemplu, o boală, un handicap, un risc de îmbolnăvire, istoricul medical, tratamentul clinic sau starea psihologică sau biomedicală efectivă a persoanei vizate, indiferent de sursa acestora, cum ar fi, de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro.

27) 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 privind prelucrarea 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 efectivă a 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, în sine, un astfel de 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 și, 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 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 operatorului 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.

28) 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 centrală care controlează prelucrarea datelor cu caracter personal în întreprinderile afiliate formează, împreună cu acestea din urmă, o entitate care poate fi tratată drept „grup de întreprinderi”.

29) Copiii (...) au nevoie de o protecție specifică a datelor lor cu caracter personal, întrucât pot fi mai puțin conștienți de riscurile, consecințele, garanțiile și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal. (…). Această protecție se referă în special la utilizarea datelor cu caracter personal ale copiilor în scopuri de marketing sau pentru crearea de profiluri de personalitate sau de utilizator și la colectarea datelor copiilor în momentul utilizării serviciilor oferite direct copiilor.

30) Orice prelucrare de date cu caracter personal ar trebui să fie legală și echitabilă. (…). Ar trebui să fie transparent pentru persoane faptul că datele cu caracter personal care le privesc sunt colectate, utilizate, consultate sau prelucrate în alt mod și în ce măsură datele sunt sau urmează a fi prelucrate. Principiul transparenței prevede că orice informații și comunicări referitoare la prelucrarea respectivelor date ar trebui să fie ușor accesibile și ușor de înțeles și că se utilizează un limbaj simplu și clar. Acest lucru 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 vizate și dreptul acestora de a li se confirma și comunica datele cu caracter personal prelucrate care le privesc. Persoanele 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 respective. În special, scopurile specifice în care datele sunt prelucrate ar trebui să fie explicite și legitime și să fie determinate la momentul colectării datelor. Datele ar trebui să fie adecvate și relevante (…) pentru scopurile în care sunt prelucrate; aceasta necesită, în special, asigurarea faptului că datele colectate nu sunt excesive și că perioada pentru care datele sunt stocate este limitată strict la minimum. (…). Datele cu caracter personal ar trebui prelucrate doar în cazul în care scopul prelucrării nu poate fi îndeplinit, în mod rezonabil, prin alte mijloace. În vederea asigurării faptului că datele nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ștergere sau revizuire periodică.

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 prevenirea accesului neautorizat la acestea sau utilizarea neautorizată a datelor și a echipamentului utilizat pentru prelucrare.

31) 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 juridic legitim, prevăzut de lege, fie în prezentul regulament, fie în alt act legislativ al Uniunii sau al unui stat membru la care se face referire 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.

(31a) 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, însă un astfel de temei juridic sau o astfel de măsură legislativă ar trebui să fie clară și precisă, iar aplicarea acesteia să fie previzibilă pentru cei vizați, în conformitate cu jurisprudența Curții de Justiție a Uniunii Europene și a Curții Europene a Drepturilor Omului.

(32) 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. 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 conținutul acesteia nu ar trebui să fie ieșit din comun, în contextul general. 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 și nu este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată.

(33) (...)

34) Pentru a garanta faptul că s-a 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 și dacă acest dezechilibru 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, deși acest lucru este adecvat în cazul particular, sau dacă executarea unui contract este condiționată de consimțământ, în ciuda faptului că acest lucru nu este necesar pentru executarea contractului și persoana vizată nu poate obține, în mod rezonabil, servicii echivalente din altă sursă fără consimțământ.

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

(35a) Prezentul regulament prevede norme generale privind protecția datelor și faptul că, în anumite cazuri, statele membre sunt, de asemenea, împuternicite să stabilească norme naționale privind protecția datelor. Prin urmare, prezentul regulament nu exclude legislația statelor membre care definește 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. Dreptul intern poate, de asemenea, să prevadă condiții de prelucrare speciale pentru sectoare specifice și pentru prelucrarea unor categorii speciale de date.

(36) 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 de interes public sau pentru exercitarea unei funcții publice, prelucrarea ar trebui să aibă un temei (…) în dreptul Uniunii sau în dreptul intern al unui stat membru. (…). De asemenea, ar trebui ca scopul prelucrării să fie stabilit în legislația Uniunii sau în cea națională. Mai mult decât atât, acest temei (…) ar putea să specifice condițiile generale ale regulamentului care reglementează legalitatea prelucrării datelor, să determine specificațiile pentru stabilirea operatorului, a tipului de date care fac obiectul prelucrării, a persoanelor vizate, a entităților cărora le pot fi dezvăluite datele, 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 legislația Uniunii sau în cea națională dacă operatorul care îndeplinește o sarcină de interes public sau exercită o funcție publică ar trebui să fie o autoritate publică sau o altă persoană fizică sau juridică de drept public sau privat, cum ar fi o asociație profesională, 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.

37) 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. (…). Unele tipuri de *prelucrare a datelor 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*.

38) Interesele legitime ale unui operator, inclusiv ale unui operator căruia îi pot fi dezvăluite datele 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. Interesul legitim poate exista, de exemplu, în cazul în care există o legătură relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată ar fi un client al operatorului sau ar fi în serviciul acestuia. (...) În orice caz, existența unui interes legitim ar necesita o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată se poate aștepta în momentul și în contextul colectării datelor la posibilitatea prelucrării în acest scop. În special, o astfel de evaluare trebuie să țină seama de cazul în care persoana vizată este un minor, întrucât minorii necesită o protecție specifică. Persoana vizată ar trebui să aibă dreptul gratuit la opoziție în ceea ce privește prelucrarea, din motive legate de situația sa particulară. Pentru a se asigura transparența, operatorul ar trebui să aibă obligația de a informa în mod explicit persoana vizată cu privire la interesele legitime urmărite și dreptul la opoziție și, de asemenea, ar trebui să aibă obligația de a documenta aceste interese legitime. (...)

(38a) Operatorii care fac parte dintr-un grup de întreprinderi sau o instituție afiliată 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 datelor cu caracter personal, în cadrul unui grup de întreprinderi, către o întreprindere situată într-o țară terță (...) rămân neschimbate.

39) Prelucrarea datelor în măsura strict necesară 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 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 (CERT), echipele de intervenție în cazul producerii unor incidente care afectează securitatea informatică (CSIRT), 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. 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.

40) Prelucrarea datelor cu caracter personal în alte scopuri decât scopurile pentru care datele au fost inițial colectate ar trebui să fie permisă doar atunci când prelucrarea este compatibilă cu scopurile respective pentru care datele au fost inițial colectate. În acest caz nu este necesar niciun temei juridic separat în afară de cel pe baza căruia a fost permisă colectarea datelor. (...) În cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice cu care este învestit operatorul, dreptul Uniunii sau al statelor membre poate stabili și specifica sarcinile și scopurile pentru care prelucrarea ulterioară este considerată a fi legală. Prelucrarea ulterioară (...) în scopuri de arhivare în interes public sau în scopuri (...) statistice, științifice sau istorice (...) sau în vederea soluționării unor litigii viitoare ar trebui considerată ca reprezentând operațiuni de prelucrare legale compatibile. Temeiul juridic prevăzut în legislația Uniunii sau a statelor membre pentru colectarea și prelucrarea datelor cu caracter personal poate constitui, de asemenea, temeiul juridic pentru prelucrarea ulterioară în alte scopuri, în cazul în care aceste scopuri sunt în conformitate cu sarcina atribuită și operatorul are dreptul legal să colecteze datele în respectivele scopuri diferite.

Pentru a stabili dacă scopul prelucrării ulterioare este compatibil cu scopul pentru care au fost colectate inițial datele, 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, inclusiv de așteptările rezonabile ale persoanei vizate în ceea ce privește utilizarea ulterioară a acestora, 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 celor preconizate. În cazul în care celălalt scop preconizat nu este compatibil cu scopul inițial în care datele sunt colectate, operatorul ar trebui să obțină consimțământul persoanei vizate cu privire la acest alt scop sau ar trebui să întemeieze prelucrarea legală pe un alt motiv legitim, în special în cazul în care acest fapt este prevăzut de dreptul Uniunii sau al statului membru care se aplică operatorului. (…).

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 acestor date către o autoritate competentă 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.

41) 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 poate genera riscuri importante la adresa drepturilor și libertăților fundamentale. Ar trebui incluse în această categorie și datele cu caracter personal care dezvăluie originea rasială sau etnică, utilizarea termenului „origine rasială” în prezentul regulament neimplicând o acceptare de către Uniunea Europeană a teoriilor care urmăresc să stabilească existența unor rase umane separate. Asemenea date nu ar trebui prelucrate, cu excepția cazului în care prelucrarea este permisă în cazuri specifice prevăzute de prezentul regulament, ținând seama de faptul că legislația statelor membre poate prevedea dispoziții specifice cu privire la protecția datelor în scopul adaptării aplicării normelor din prezentul regulament, în ceea ce privește respectarea unei obligații legale sau îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice cu care este învestit 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.

De asemenea, anumite categorii speciale de date cu caracter personal pot fi prelucrate în cazul în care datele au fost făcute publice în mod manifest sau pot fi transferate operatorului, în mod voluntar și la solicitarea persoanei vizate, într-un scop specific precizat de către persoana vizată, în cazul în care prelucrarea este efectuată în interesul persoanei vizate.
Dreptul statelor membre și al Uniunii poate prevedea ca, în anumite cazuri, interdicția generală privind prelucrarea acestor categorii speciale de date cu caracter personal să nu poată fi ridicată prin consimțământul explicit al persoanei vizate.

42) Derogarea de la interdicția privind prelucrarea categoriilor sensibile de date ar trebui să fie permisă, de asemenea, în cazul în care legislația Uniunii sau a statelor membre 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 prin motive de interes public, în special în cazul *prelucrării datelor* în domeniul legislației privind ocuparea forței de muncă, securitatea socială și 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 sau pentru asigurarea unor standarde ridicate de calitate și siguranță a asistenței medicale, a serviciilor de sănătate și a medicamentelor sau dispozitivelor medicale ori pentru evaluarea politicilor publice adoptate în domeniul sănătății, inclusiv prin elaborarea de indicatori privind calitatea și activitatea*.
Această derogare poate fi acordată în scopuri medicale, inclusiv sănătatea publică (...) și pentru gestionarea serviciilor de asistență medicală, în special în scopul 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 vederea arhivării în interes public sau în scopuri (...) istorice, statistice și științifice.
De asemenea, prelucrarea unor asemenea date 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 judiciare sau în cadrul unei proceduri administrative sau a oricărei proceduri extrajudiciare.

(42a) *Categoriile speciale de date cu caracter personal care necesită un nivel mai ridicat de protecție pot fi prelucrate doar în scopuri legate de sănătate atunci când este necesar pentru realizarea acestor scopuri în beneficiul persoanelor 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 sau în scopuri de securitate, supraveghere și alertă în materie de sănătate ori în vederea arhivării* în interes public, în scopuri *istorice, statistice sau științifice, 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 (...). Legislația Uniunii sau a statelor membre ar trebui să prevadă măsuri specifice și adecvate pentru a proteja drepturile fundamentale și datele cu caracter personal ale persoanelor fizice. (...).*

(42b) *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 este condiționată de măsuri adecvate și specifice destinate să protejeze drepturile și libertățile persoanelor. 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 din 16 decembrie 2008 privind statisticile comunitare referitoare la sănătatea publică, precum și la sănătatea și siguranța la locul de muncă, adică 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 cu caracter personal 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, societățile de asigurări și băncile.*

43) 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.

44) În cazul în care, în cadrul activităților electorale, funcționarea sistemului democratic necesită, într-un stat membru, ca partidele politice să colecteze date 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.

45) Dacă datele 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.

46) Principiul transparenței prevede că orice informații care se adresează publicului sau persoanei vizate ar trebui să fie ușor accesibile și ușor de înțeles și că ar trebui să se utilizeze un limbaj simplu și clar, precum și vizualizare acolo unde este cazul. Aceste informații ar putea fi furnizate și în format electronic, de exemplu atunci când sunt adresate publicului, prin intermediul unui site internet. Acesta este important în special în cazul în care, în situații cum ar fi publicitatea online, multitudinea actorilor și complexitatea, 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. Întrucât minorii necesită o protecție specifică, orice informații și orice comunicare, în cazul în care prelucrarea vizează (…) un minor, ar trebui să fie exprimate într-un limbaj simplu și clar, astfel încât acesta să îl poată înțelege cu ușurință.

47) Ar trebui prevăzute modalități de facilitare a exercitării de către persoana vizată a drepturile sale stipulate de prezentul regulament, inclusiv mecanismele de a solicita, (…) în special, accesul la date, rectificarea și ștergerea acestora, precum și exercitarea dreptului la opoziție. Astfel, 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 fac obiectul unei prelucrări automate. Operatorul ar trebui să aibă obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate și cel mai târziu într-un termen fix de o lună și, în cazul în care nu intenționează să se conformeze cererii persoanei vizate, să motiveze acest refuz.

Cu toate acestea, în cazul în care cererile sunt în mod vădit nefondate sau excesive, de exemplu atunci când persoana vizată solicită informații în mod nejustificat și repetat sau atunci când persoana vizată abuzează de dreptul său de a primi informații, de exemplu prin furnizarea de informații false sau înșelătoare în momentul efectuării cererii, operatorul ar putea refuza să dea curs cererii.

48) Conform principiilor prelucrării echitabile și transparente, persoana vizată ar trebui să fie 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 garanta o prelucrare echitabilă și transparentă. În plus, persoana vizată ar trebui informată cu privire la crearea de profiluri, precum și la consecințele acesteia. Atunci când datele sunt colectate de la persoana vizată, aceasta ar trebui, de asemenea, să fie informată dacă are obligația de a furniza datele și care sunt consecințele în cazul nerespectării acestei obligații.

49) Informațiile în legătură cu prelucrarea datelor cu caracter personal referitoare la persoana vizată ar trebui furnizate acesteia la momentul colectării sau, în cazul în care datele nu sunt colectate de la persoana vizată, într-o perioadă rezonabilă, în funcție de circumstanțele cazului. În cazul în care datele pot fi divulgate în mod legitim unui alt destinatar, persoana vizată ar trebui informată atunci când datele sunt divulgate pentru prima dată destinatarului. În cazul în care operatorul intenționează să prelucreze datele 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 nu a putut fi comunicată persoanei vizate din cauză că au fost utilizate surse diverse, informațiile ar trebui furnizate în manieră generală.

50) Cu toate acestea, nu este necesară impunerea obligației respective în cazul în care persoana vizată deține deja aceste informații sau în cazul în care înregistrarea sau divulgarea datelor 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 vederea arhivării în interes public, în scopuri istorice, statistice sau științifice (...); în această privință, pot fi luate în considerare numărul persoanelor vizate, vechimea datelor și orice garanții adecvate adoptate.

51) O persoană fizică ar trebui să aibă drept de acces la datele colectate care o privesc și ar trebui să își exercite acest drept cu ușurință și la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia. *Acest lucru include dreptul persoanelor de a avea acces la datele lor cu caracter personal 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 în ce scopuri sunt prelucrate datele, dacă este posibil pentru ce perioadă, identitatea destinatarilor datelor, care este logica de prelucrare automată a datelor și care ar putea fi, cel puțin în cazul în care se bazează pe crearea de profiluri, consecințele unei astfel de prelucrări. Acest drept nu ar trebui să aducă atingere drepturilor și 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 poate solicita ca, înainte de a îi fi furnizate informațiile, persoana vizată să precizeze la ce informații sau la ce activități de prelucrare se referă cererea sa.

52) 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 identificatorilor online. (...) 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. Un operator nu ar trebui să rețină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacționeze la cereri potențiale.

53) O persoană fizică ar trebui să aibă dreptul de rectificare a datelor cu caracter personal care o privesc și „dreptul de a fi uitată”, în cazul în care păstrarea acestor date nu este în conformitate cu prezentul regulament sau cu legislația Uniunii sau a statului membru sub incidența căreia 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 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 minoră 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 își exercita acest drept în pofida faptului că nu mai este minoră. Cu toate acestea, păstrarea în continuare a datelor ar trebui să fie conformă cu legislația 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 executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul, *din motive de interes public în domeniul sănătății publice,* în vederea arhivării în interes public, în scopuri istorice, statistice și științifice (...) sau pentru constatarea, exercitarea sau apărarea unui drept în instanță.

54) Pentru a se consolida „dreptul de a fi uitat” în mediul online, dreptul de ștergere ar trebui, de asemenea, să fie extins astfel încât un operator care a făcut publice date cu caracter personal să aibă obligația de a informa operatorii care prelucrează astfel de date **(...)** să șteargă orice linkuri către datele cu caracter personal respective sau copii sau reproduceri ale acestora.

În scopul asigurării informațiilor sus-menționate, operatorul ar trebui să ia (…) măsuri rezonabile, ținând seama de tehnologia disponibilă și de mijloacele aflate la dispoziția lui, inclusiv măsuri tehnice, în ceea ce privește datele de a căror publicare operatorul este responsabil. (…).

(54a) Metodele de restricționare a prelucrării de date cu caracter personal ar putea include, printre altele, mutarea temporară a datelor selectate în alt sistem de prelucrare sau anularea accesului utilizatorilor la datele selectate sau înlăturarea temporară a datelor publicate de pe un site internet. În ceea ce privește sistemele automatizate de evidență a datelor, restricționarea prelucrării de date cu caracter personal ar trebui, în principiu, asigurată prin mijloace tehnice; faptul că prelucrarea datelor cu caracter personal este restricționată ar trebui indicat în sistem în așa fel încât să se înțeleagă clar că această restricționare are loc.

55) 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 și prelucrabil automat, și să le poată transmite unui alt operator.

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 cadrul executării 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 în cadrul exercitării funcțiilor lor publice. Prin urmare, 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 pentru efectuarea unei sarcini îndeplinite în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul.

Dreptul persoanei vizate de a transmite date cu caracter personal nu creează pentru operatori obligația de a adopta sau de a menține sisteme de prelucrare a datelor 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 transmite datele nu ar trebui să aducă atingere cerințelor privind legalitatea prelucrării datelor cu caracter personal referitoare la o altă persoană vizată, 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. (...)

56) 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 pentru exercitarea autorității oficiale cu care este învestit operatorul sau pe baza (...) intereselor legitime ale unui operator sau ale unei părți terțe, orice persoană vizată ar trebui să aibă totuși dreptul de a se opune prelucrării oricăror date care se referă la situația sa particulară. Ar trebui să revină operatorului sarcina de a demonstra că interesele sale legitime și imperioase pot prevala asupra intereselor sau a drepturilor și libertăților fundamentale ale persoanei vizate.

57) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de marketing direct, persoana vizată ar trebui să aibă gratuit dreptul la opoziție cu privire la o astfel de prelucrare, fie ea inițială sau ulterioară, care să poată fi invocat cu ușurință și în mod efectiv.

58) Persoana vizată ar trebui să aibă dreptul de a nu face obiectul unei decizii care evaluează aspecte personale referitoare la persoana vizată (...), care se bazează exclusiv pe prelucrarea automată *şi care produce efecte juridice care privesc persoana vizată* sau o afectează în mod semnificativ, cum ar fi refuzul automat al unei cereri de credit online sau practicile de recrutare pe cale electronică, fără intervenţie umană. O astfel de prelucrare include de asemenea „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 legate de performanţa la locul de muncă, situaţia economică, sănătate, preferinţe personale sau interese, fiabilitate sau comportament, locaţie sau deplasări, atât timp cât aceasta produce efecte juridice care privesc persoana vizată sau o afectează în mod semnificativ. Cu toate acestea, luarea de decizii pe baza unei astfel de prelucrări, inclusiv creare de profiluri, ar trebui permisă în cazul în care este autorizată de legislaţia Uniunii sau a statului membru care se aplică operatorului, inclusiv în scopul monitorizării şi prevenirii fraudei şi a evaziunii fiscale şi în scopul asigurării securităţii şi fiabilităţii unui serviciu oferit de operator, sau în cazul în care este necesară pentru încheierea sau executarea unui contract între persoana vizată şi un operator sau în cazul în care persoana vizată şi-a dat în mod explicit consimţământul. În orice caz, o astfel de prelucrare ar trebui să facă obiectul unor garanţii corespunzătoare, inclusiv o informare specifică a persoanei vizate şi dreptul acesteia de a obţine intervenţie umană, de a-şi exprima punctul de vedere, de a primi o explicaţie privind decizia luată în urma unei astfel de evaluări, precum şi dreptul de a contesta decizia. Pentru a asigura o prelucrare echitabilă şi transparentă în ceea ce priveşte persoana vizată, având în vedere circumstanţele specifice şi contextul în care sunt prelucrate datele cu caracter personal, operatorul ar trebui să utilizeze proceduri matematice sau statistice adecvate pentru crearea de profiluri, să pună în aplicare măsuri tehnice şi organizatorice adecvate pentru a asigura în special faptul că factorii care duc la inexactităţi ale datelor sunt corectaţi şi că riscul de erori este redus la minimum, precum şi să securizeze datele cu caracter personal într-un mod care să ţină seama de pericolele potenţiale la adresa intereselor şi drepturilor persoanei vizate şi care să prevină, printre altele, efectele discriminatorii împotriva persoanelor pe motiv de rasă sau origine etnică, opinii politice, religie sau convingeri, apartenenţă sindicală, caracteristici genetice, stare de sănătate sau orientare sexuală sau care să ducă la măsuri care să aibă astfel de efecte. Procesul decizional automatizat şi crearea de profiluri pe baza unor categorii speciale de date cu caracter personal ar trebui permise numai în condiţii specifice.

(58a) Crearea de profiluri face în sine obiectul normelor (generale) ale prezentului regulament care reglementează prelucrarea datelor cu caracter personal (temeiurile juridice ale prelucrării, principiile de protecție a datelor etc.), cu garanții specifice (de exemplu, obligația de a efectua o evaluare a impactului în unele cazuri sau dispoziții privind informațiile specifice care trebuie furnizate persoanei vizate). Comitetul european pentru protecția datelor ar trebui să aibă posibilitatea de a emite orientări în acest context.

59) Dreptul Uniunii sau dreptul unui stat membru poate impune restricții ale unor principii specifice, ale drepturilor de informare, acces, rectificare și ștergere sau ale dreptului la portabilitatea datelor, ale dreptului la opoziție, ale măsurilor bazate pe crearea de profiluri, precum și ale comunicării unei încălcări a securității datelor cu caracter personal persoanei vizate și ale 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 a încălcării eticii în cazul profesiilor reglementate, alte interese publice 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, cum ar fi îndeplinirea unei sarcini care revine Mișcării Internaționale de Cruce Roșie și Semilună Roșie (...). Aceste restricții ar trebui să fie conforme cu cerințele prevăzute de Carta drepturilor fundamentale a Uniunii Europene și de Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale.

(59a) Nicio dispoziție din prezentul regulament nu ar trebui să deroge de la (...) privilegiul nedivulgării de informații confidențiale al Comitetului Internațional al Crucii Roșii în temeiul dreptului internațional, care este aplicabil în proceduri judiciare și administrative. (…).

60) Ar trebui să se stabilească responsabilitatea și răspunderea operatorului pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său. În special, operatorul ar trebui (…) să fie obligat să pună în aplicare măsuri adecvate și să fie în măsură să demonstreze conformitatea (…) activităților de prelucrare cu prezentul regulament (…). Aceste măsuri ar trebui să țină seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul la adresa drepturilor și libertăților persoanelor fizice.

(60a) Astfel de riscuri, prezentând grade diferite de probabilitate și gravitate, pot fi rezultatul unei prelucrări a datelor care ar putea genera daune 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 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 de capacitatea de a-și exercita controlul asupra datelor lor cu caracter personal; datele cu caracter personal prelucrate sunt date care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența sindicală; sunt prelucrate date genetice sau date privind sănătatea, viața sexuală sau condamnările penale și infracțiunile sau măsurile de securitate conexe; sunt evaluate aspecte de natură personală, în special analizarea și 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 minori; prelucrarea implică un volum mare de date cu caracter personal și afectează un număr larg de persoane vizate; (...).

(60b) *Probabilitatea de a se materializa și gravitatea riscului ar trebui să fie determinate în funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor. Riscul ar trebui să facă obiectul unei evaluări obiective, prin care să se stabilească dacă operațiunile de prelucrare a datelor prezintă un risc ridicat. Un risc ridicat este un risc deosebit de prejudiciere a drepturilor și libertăților persoanelor fizice* (...).

(60c) Orientări pentru punerea în aplicare a 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 european pentru protecția datelor sau prin indicații furnizate de un responsabil cu protecția datelor. Comitetul european pentru protecția datelor poate, de asemenea, să emită orientări cu privire la operațiunile de prelucrare care sunt considerate puțin susceptibile de a genera un risc ridicat la adresa drepturilor și libertăților persoanelor fizice și să indice măsurile care se pot dovedi suficiente în asemenea cazuri pentru a aborda un astfel de risc. (...)

61) 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 corespunzătoare, care să respecte, în special, principiul luării în considerare a 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 fie se bazează pe prelucrarea datelor cu caracter personal, fie 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 tehnologiei, să se asigure că operatorii și persoanele împuternicite de operatori sunt în măsură să își îndeplinească obligațiile referitoare la protecția datelor.

62) Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și a persoane**lor** 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.

63) Atunci când un operator care nu este stabilit în Uniune prelucrează date cu caracter personal ale unor persoane vizate care își au reședința în Uniune, iar activitățile sale de prelucrare au legătură cu oferirea de bunuri sau servicii unor astfel de persoane vizate sau cu monitorizarea comportamentului acestora în Uniune, (...) operatorul ar trebui să desemneze un reprezentant, în afara cazului în care (...) *prelucrarea pe care o efectuează are* caracter ocazional şi este puţin susceptibilă *să genereze un risc la adresa drepturilor şi libertăţilor persoanelor vizate, având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării,* sau a cazului în care operatorul este o autoritate publică ori un organism public (…). Reprezentantul ar trebui să acționeze în numele operatorului, putând fi contactat de orice autoritate de supraveghere. Reprezentantul ar trebui desemnat în mod explicit, printr-un mandat scris al operatorului, să acţioneze în numele acestuia în ceea ce priveşte obligaţiile operatorului în temeiul prezentului regulament. Desemnarea unui astfel de reprezentant nu aduce atingere responsabilităţii şi răspunderii operatorului în temeiul prezentului regulament. Un astfel de reprezentant ar trebui să își îndeplinească sarcinile în conformitate cu mandatul primit de la operator, inclusiv să coopereze cu autoritățile de supraveghere competente cu privire la orice acțiune întreprinsă pentru a asigura respectarea dispozițiilor prezentului regulament. Reprezentantul desemnat ar trebui să fie supus unor acțiuni executorii în cazul nerespectării prezentului regulament de către operator.

(63a) 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 pune în aplicare 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 un 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 legislației Uniunii sau a unui stat membru, care creează obligații pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopu**rile** prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate, ținând seama de sarcinile și responsabilitățile specifice ale persoanei împuternicite de operator în contextul prelucrării care trebuie efectuată, precum și de riscul la adresa drepturilor și libertăților persoanei vizate.

Operatorii și persoanele împuternicite de operatori 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 ori care fac parte dintr-o certificare acordată în cadrul mecanismului de certificare. După finalizarea prelucrării în numele operatorului, persoana împuternicită de operator ar trebui să returneze sau să șteargă datele cu caracter personal, cu excepția cazului în care există o cerință de stocare a datelor în temeiul legislației Uniunii sau a unui stat membru care instituie obligații pentru persoana împuternicită de operator.

64) (...)

65) În vederea demonstrării conformității cu prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să păstreze evidențe ale tuturor categoriilor de activități 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.

66) În vederea menținerii securității și a prevenirii prelucrărilor care încalcă dispozițiile prezentului regulament, operatorul sau persoana împuternicită de operator ar trebui să evalueze riscul (...) inerent prelucrării și să pună în aplicare măsuri pentru atenuarea acestui risc. Măsurile respective ar trebui să asigure un nivel corespunzător de securitate, inclusiv confidențialitatea, luând în considerare tehnologia disponibilă și costurile punerii (…) în aplicare în raport cu riscul și natura datelor cu caracter personal a căror protecție trebuie asigurată. (…). La evaluarea riscului pentru securitatea datelor, ar trebui să se acorde atenție riscuri**lor** 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 daune fizice, materiale sau morale.

(66a) Pentru a favoriza respectarea dispozițiilor prezentului regulament în cazurile în care operațiunile de prelucrare sunt susceptibile să genereze un risc ridicat la adresa drepturilor și libertăților 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 dispozițiile prezentului 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 punerii în aplicare, ar trebui să aibă loc o consultare a autorității de supraveghere înainte de prelucrare.

67) Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate conduce la (...) daune 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 protejate prin secret profesional sau orice alt dezavantaj de natură economică sau socială adus persoanei fizice vizate. (…). Prin urmare, de îndată ce a luat cunoștință de producerea unei (…) încălcări a securității datelor cu caracter personal care poate conduce la (...) daune fizice, materiale sau morale, operatorul ar trebui să o notifice autorității de supraveghere, fără întârziere nejustificată și, dacă este posibil, în termen de 72 de ore. În cazul în care termenul de 72 de ore nu poate fi respectat, notificarea ar trebui să fie însoțită de o explicație a motivelor întârzierii. Persoanele fizice ale căror drepturi și libertăți ar putea fi afectate grav de încălcare ar trebui să fie notificate fără întârziere nejustificată, pentru a putea să ia măsurile de precauție necesare. (…). Notificarea ar trebui să descrie natura încălcării securității datelor cu caracter personal și să formuleze recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative. Notificările 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 unor daune ar presupune notificarea cu promptitudine a persoanelor vizate, în timp ce necesitatea de a pune în aplicare măsuri corespunzătoare împotriva încălcării în continuare a securității datelor sau împotriva unor încălcări similare ale securității datelor ar putea justifica un termen mai îndelungat.

68) (...) Trebuie să se stabilească dacă au fost puse în aplicare 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.

(68a) Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal nu ar trebui să fie necesară în cazul în care operatorul a pus în aplicare măsuri tehnologice adecvate de protecție și respectivele măsuri au fost aplicate în cazul datelor afectate de încălcarea securității datelor cu caracter personal. Aceste măsuri tehnologice de protecție ar trebui să includă măsurile prin care se asigură că datele devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, în special prin criptarea datelor cu caracter personal (...).

69) 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.

70) 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 la adresa drepturilor și libertăților 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 .

(70a) 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, evaluare care ar trebui să includă, în special, măsurile avute în vedere, precum și garanții și mecanisme pentru atenuarea riscului respectiv, pentru asigurarea protecției datelor cu caracter personal și pentru demonstrarea conformității cu prezentul regulament.

71) 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 la adresa drepturilor și libertăților 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 sunt prelucrate în scopul luării de decizii care vizează anumite persoane 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 la adresa drepturilor și libertăților 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, indiferent de volumul sau de natura acestora, nu ar trebui considerată a fi la scară largă în cazul în care prelucrarea acestor date este protejată prin secret profesional (...), cum ar fi prelucrarea de date cu caracter personal de la pacienți sau clienți de către un anumit medic, profesionist în domeniul sănătății, spital sau avocat. În aceste cazuri, o evaluare a impactului asupra protecției datelor nu ar trebui să fie obligatorie.*

72) În unele circumstanțe ar putea fi judicios și 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.

73) Evaluările impactului asupra protecției datelor pot fi efectuate de o autoritate publică sau un organism public în cazul în care o astfel de evaluare nu a fost deja realizată 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.

74) În cazul în care o evaluare a impactului asupra protecției datelor arată că prelucrarea ar genera, în pofida garanțiilor, măsurilor de securitate și mecanismelor de atenuare a riscului prevăzute, un risc ridicat la adresa drepturilor și libertăților persoanelor fizice (...), iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile și al costurilor punerii în aplicare, autoritatea de supraveghere ar trebui să fie consultată, înainte de începerea operațiunilor de prelucrare. Un astfel de risc (...) ridicat este susceptibil să fie generat de anumite tipuri de prelucrare a datelor, precum și de o anumită amploare și o anumită frecvență ale prelucrării, care pot duce și la producerea unor daune (...) sau (...) pot atinge drepturile și libertățile persoanei vizate. 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 în conformitate cu articolul 33 poate fi transmis autorității de supraveghere, în special măsurile avute în vedere pentru a atenua riscul la adresa drepturilor și libertăților persoanelor fizice.

(74a) 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.

(74b) 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.

75) În cazul în care prelucrarea este efectuată în sectorul public sau în cazul în care, în sectorul privat, prelucrarea este efectuată de o întreprindere de mari dimensiuni sau în cazul în care activitățile de bază ale întreprinderii, indiferent de dimensiunea acesteia, implică operațiuni de prelucrare care necesită o monitorizare regulată și sistematică, o persoană care deține cunoștințe de specialitate în materie de legislație și practici privind protecția datelor poate să acorde asistență operatorului sau persoanei împuternicite de operator pentru monitorizarea conformității, la nivel intern, cu prezentul regulament. 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.

76) 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 la adresa drepturilor și libertăților persoanelor fizice.

(76a) 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.

77) 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.

78) Fluxurile transfrontaliere 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 garantat 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 poate avea loc numai dacă, sub rezerva respectării celorlalte dispoziții ale prezentului regulament, operatorul sau persoana împuternicită de operator îndeplinește condițiile prevăzute la capitolul V.

79) 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 legislația UE și includ garanții pentru protejarea drepturilor persoanelor vizate.

80) Comisia poate (...) decide, cu efect în întreaga Uniune, că anumite țări terțe sau un teritoriu sau un sector specificat, precum sectorul privat sau unul sau mai multe sectoare economice specifice, dintr-o țară terță sau o organizație internațională oferă un nivel adecvat de protecție a datelor, furnizând astfel securitate juridică și uniformitate în Uniune în ceea ce privește țările terțe sau organizațiile internaționale care sunt considerate a furniza un astfel de nivel de protecție. În aceste cazuri, transferurile de date cu caracter personal către țările respective pot avea loc fără a fi necesar să se obțină o autorizație specifică.

81) În conformitate cu valorile fundamentale pe care se întemeiază Uniunea, în special protecția drepturilor omului, Comisia ar trebui, în evaluarea sa referitoare la o țară 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 a standardelor juridice aplicabile și legislația în vigoare în țara terță respectivă. Țara terță ar trebui să ofere garanții care asigură un nivel adecvat de protecție, în special atunci când datele sunt prelucrate în unul sau mai multe sectoare specifice. În special, țara terță ar trebui să asigure o supraveghere efectivă în materie de protecție a datelor și să prevadă mecanisme de cooperare cu autoritățile europene de protecție a datelor, iar persoanele vizate ar trebui să beneficieze de drepturi efective și opozabile și căi de atac administrative și judiciare efective.

(81a) Pe lângă angajamentele internaționale asumate de țara terță sau de organizația internațională, Comisia ar trebui să țină seama și de obligațiile care decurg din participarea țării terțe sau a organizației internaționale la sistemele multilaterale sau regionale, în special în ceea ce privește protecția datelor cu caracter personal, precum și de punerea în aplicare a unor astfel de obligații. În special, *ar trebui să fie luată în considerare* aderarea țării terțe la Convenția Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal şi protocolul adiţional la aceasta. Comisia ar trebui să consulte Comitetul european pentru protecția datelor atunci când evaluează nivelul de protecție din țările terțe sau din organizațiile internaționale.

(81b) Comisia ar trebui să monitorizeze funcționarea deciziilor privind nivelul de protecție dintr-o țară terță sau un teritoriu sau un sector specificat dintr-o țară terță sau dintr-o organizație internațională, inclusiv a deciziilor adoptate în temeiul articolului 25 alineatul (6) sau al articolului 26 alineatul (4) din Directiva 95/46/CE. Comisia ar trebui să evalueze, într-un termen rezonabil, funcționarea deciziilor din urmă și să raporteze toate constatările pertinente comitetului în sensul Regulamentului (UE) nr. 182/2011, după cum s-a stabilit în temeiul prezentului regulament.

82) Comisia poate (...) să recunoască faptul că o țară terță sau 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 când sunt îndeplinite cerințele prevăzute la articolele 42 - 44. 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.

83) În absența unei decizii privind caracterul adecvat al protecției, 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 în materie de protecție a datelor adoptate de o autoritate de supraveghere sau a clauzelor contractuale ad-hoc autorizate de o autoritate de supraveghere sau a altor măsuri adecvate și proporționale care sunt justificate având în vedere toate circumstanțele aferente unei operațiuni de transfer de date sau unui set de operațiuni de transfer de date și în cazurile autorizate de o autoritate de supraveghere. Respectivele garanții ar trebui să asigure respectarea cerințelor în materie de protecție a datelor și drepturi ale persoanelor vizate, inclusiv dreptul de acces la căi de atac administrative sau judiciare efective. Acestea ar trebui să se refere în special la respectarea principiilor generale referitoare la prelucrarea datelor cu caracter personal, la disponibilitatea drepturilor executorii ale persoanelor vizate și a căilor de atac eficiente și la principiul luării în considerare a protecției datelor începând cu momentul conceperii și al 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 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.

84) 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, inclusiv 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.

85) Un grup corporativ 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 corporativ sau grup de întreprinderi, atât timp cât astfel de reguli corporatiste includ principii esențiale și drepturi exercitabile în scopul asigurării unor garanții adecvate pentru transferurile sau categoriile de transferuri de date cu caracter personal.

86) 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 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 legislația Uniunii sau a unui stat membru impun acest lucru sau 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 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.

87) Aceste norme 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, între 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 contacților 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 persona vizată nu are capacitatea să își dea consimțământul. În absența unei decizii privind caracterul adecvat al nivelului de protecție, dreptul Uniunii sau al unui stat membru 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, cum ar fi Societatea Națională a Crucii Roșii (...) sau Comitetul Internațional al Crucii Roșii, al datelor cu caracter personal ale unei persoane vizate care se află în incapacitate fizică sau juridică de a-și da consimțământul, în vederea îndeplinirii unei sarcini care revine Mișcării Internaționale de Cruce Roșie și Semilună Roșie în temeiul Convențiilor de la Geneva și/sau în vederea punerii în aplicare cu fidelitate a dreptului internațional umanitar aplicabil în conflictele armate, ar putea fi considerat necesar pentru un motiv important de interes public sau ca fiind în interesul vital al persoanei vizate.

88) Transferurile care nu pot fi considerate ca fiind pe scară largă sau frecvente, ar putea, de asemenea, să fie efectuate în scopul realizării intereselor legitime urmărite de operator sau de persoana împuternicită de operator, atunci când asupra respectivelor interese nu prevalează interesele sau drepturile şi libertăţile persoanei vizate şi atunci când operatorul sau persoana împuternicită de operator a evaluat toate circumstanţele aferente transferului de date. Operatorul sau persoana împuternicită de către operator ar trebui să acorde atenţie deosebită naturii datelor, scopului şi duratei operaţiunii sau operaţiunilor propuse de prelucrare, situaţiei din ţara de origine, din ţara terţă şi din ţara de destinaţie finală şi garanţiilor adecvate oferite pentru protecţia drepturilor şi libertăţilor fundamentale ale persoanelor fizice în ceea ce priveşte prelucrarea datelor lor cu caracter personal. Pentru prelucrarea datelor în scopuri de cercetare istorică, statistică şi ştiinţifică, ar trebui să se ia în considerare aşteptările legitime ale societăţii cu privire la creşterea nivelului de cunoştinţe. Pentru a evalua dacă un transfer este la scară largă sau frecvent, ar trebui luate în considerare volumul de date cu caracter personal şi numărul de persoane vizate, precum şi dacă transferul are loc ocazional sau cu regularitate.

89) În orice caz, atunci când Comisia nu a luat o decizie cu privire la nivelul adecvat de protecție a datelor într-o țară terță, operatorul sau persoana împuternicită de operator ar trebui să utilizeze soluții care să ofere persoanelor vizate garanția că vor continua să beneficieze de drepturi fundamentale și garanții în ceea ce privește prelucrarea datelor lor în Uniune, odată ce aceste date au fost transferate.

90) Unele țări terțe au adoptat legi, regulamente și alte instrumente legislative care au drept obiectiv să reglementeze în mod direct activitățile de prelucrare a datelor ale persoanelor fizice și juridice aflate sub jurisdicția statelor membre. Aplicarea extrateritorială a acestor legi, regulamente și alte instrumente legislative poate încălca dreptul internațional și poate împiedica asigurarea protecției persoanelor fizice garantată 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 al unui stat membru care se aplică operatorului. (...)

91) Fluxul transfrontalier de date cu caracter personal <u>în afara Uniunii</u> 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. <u>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 dispozițiile prezentului regulament, inclusiv dispozițiile prevăzute la capitolul V.</u>

92) 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 pot institui mai multe autorități de supraveghere, pentru a reflecta structura lor constituțională, organizatorică și administrativă.

(92a) Independența autorităților de supraveghere nu ar trebui să însemne că autoritățile de supraveghere nu pot face obiectul unui mecanism de control sau monitorizare în ceea ce privește cheltuielile acestora. De asemenea, aceasta nu înseamnă că autoritățile de supraveghere nu pot face obiectul unui control jurisdicțional.

93) 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 european pentru protecția datelor și cu Comisia.

94) Fiecare autoritate de supraveghere ar trebui să beneficieze de resurse financiare și umane (…), de localuri și de infrastructura necesare pentru îndeplinirea cu eficacitate a sarcinilor lor, inclusiv a celor legate de asistența reciprocă și cooperarea cu alte autorități de supraveghere în întreaga Uniune. Fiecare autoritate de supraveghere ar trebui să aibă un buget anual separat, care poate face parte din bugetul general de stat sau național.

95) 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 ar trebui să fie numiți de parlamentul și/sau de guvernul ori șeful de stat al statului membru ori de către un organism independent împuternicit prin legislația statului membru să facă numirea prin intermediul unei proceduri transparente. În vederea asigurării independenței autorității de supraveghere, membrul sau membrii acesteia ar trebui să nu întreprindă acțiuni incompatibile cu îndatoririle lor, iar, pe durata mandatului, ar trebui să nu desfășoare activități incompatibile, remunerate sau nu. (…).

(95a) Fiecare autoritate de supraveghere ar trebui să aibă, pe teritoriul statului membru de care aparține, competența 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 Uniunea Europeană 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 regulamentului, promovarea informării publicului cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal.

96) Autoritățile de supraveghere ar trebui să monitorizeze aplicarea dispozițiilor prevăzute de prezentul regulament și să contribuie la aplicarea consecventă 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, prezentul regulament ar trebui să oblige și să împuternicească autoritățile de supraveghere 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.

(97) 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 care sunt 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 european pentru protecția datelor poate 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.

(97a) Autoritatea principală ar trebui să aibă competența de a adopta decizii obligatorii privind măsurile de punere în aplicare a competențelor care îi sunt conferite în conformitate cu dispozițiile prezentului 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 deciziile constau în respingerea 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.

(97b) 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.

(97c) 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 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 cadrul mecanismului 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 principală de supraveghere 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 mecanismului ghișeului unic.

(98) Normele privind autoritatea de supraveghere principală și mecanismul ghișeului unic nu ar trebui să se aplice în cazul în care prelucrarea este efectuată de către autorități publice sau organisme private care acționează 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.

(99) (...)

(100) 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, corective și de sancționare, precum și competențe de autorizare și de consultare, în special în cazul plângerilor depuse de persoane fizice, precum și, fără a aduce atingere competențelor autorităților de urmărire penală în temeiul legislației naționale, de a aduce în atenția autorităților judiciare cazurile de încălcare a prezentului regulament și/sau de a se implica în proceduri judiciare. Aceste competențe ar trebui să includă și competența de a interzice prelucrarea cu privire la care este consultată autoritatea. 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 legislația procedurală națională. 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.

(101) (…).

(101a)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 în cel mai înalt grad 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 competentă.

(101b)Autoritatea de supraveghere care a primit o plângere sau a identificat ori a fost informată în alt mod asupra unor situații de posibile încălcări ale regulamentului ar trebui să încerce o soluționare pe cale amiabilă și, în cazul în care aceasta eșuează, să își exercite plenitudinea competențelor 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 acel stat membru în care a fost depusă plângerea sau a fost identificată posibila încălcare, iar chestiunea nu afectează în mod substanțial sau nu este de natură să afecteze în mod substanțial persoane vizate din alte state membre. 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 acelui stat membru sau 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 legislației naționale.

(102) 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.

(103) Autoritățile de supraveghere ar trebui să își acorde reciproc asistență în îndeplinirea sarcinilor care le revin, pentru a se asigura consecvența aplicării prezentului regulament pe piața internă. Dacă o autoritate de supraveghere care solicită asistență reciprocă, în cazul absenței unui răspuns din partea autorității de supraveghere căreia i s-a adresat cererea în termen de o lună de la primirea cererii, adoptă o măsură provizorie, respectiva măsură provizorie ar trebui să fie justificată în mod corespunzător și să aibă doar un caracter temporar.

(104) Fiecare autoritate de supraveghere ar trebui să aibă dreptul de a participa 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.

(105) Pentru a se asigura aplicarea consecventă 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 abordat 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.

(106) În aplicarea mecanismului pentru asigurarea coerenței, Comitetul european pentru protecția datelor 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 european pentru protecția datelor 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.

(107) (...)

(108) 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, atunci când aplică mecanismul pentru asigurarea coerenței, o autoritate de supraveghere ar trebui să poată adopta măsuri provizorii, cu o anumită perioadă de valabilitate.

(109) Aplicarea acestui 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.

(110) Cu scopul de a promova aplicarea consecventă a prezentului regulament, Comitetul european pentru protecția datelor ar trebui instituit ca organism independent al Uniunii. Pentru a-și îndeplini obiectivele, Comitetul european pentru protecția datelor ar trebui să aibă personalitate juridică. Comitetul european pentru protecția datelor 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. Comitetul ar trebui să fie format din șefii autorităților de supraveghere din fiecare stat membru ori reprezentanții acestora(...). Comisia și *Autoritatea Europeană pentru Protecția Datelor* ar trebui să participe la activitățile sale, fără a avea drept de vot. Comitetul european pentru protecția datelor ar trebui să contribuie la aplicarea consecventă a prezentului regulament în întreaga Uniune, inclusiv prin oferirea de consultanță Comisiei, în special la nivelul protecției în țările terțe și în cadrul organizațiilor internaționale, și prin promovarea cooperării autorităților de supraveghere în întreaga Uniune. Comitetul european pentru protecția datelor ar trebui să acționeze în mod independent în exercitarea sarcinilor sale.

(110a) Comitetul european pentru protecția datelor ar trebui să fie asistat de un secretariat asigurat de secretariatul Autorității Europene pentru Protecția Datelor. Personalul secretariatului Autorității Europene pentru Protecția Datelor implicat în îndeplinirea sarcinilor conferite Comitetului european pentru protecția datelor în temeiul prezentului regulament ar trebui să își îndeplinească sarcinile exclusiv conform instrucțiunilor președintelui Comitetului european pentru protecția datelor și să raporteze acestuia. Separarea personalului din punct de vedere organizațional ar trebui să vizeze toate serviciile necesare pentru funcționarea independentă a Comitetului european pentru protecția datelor.

(111) Orice persoană vizată ar trebui să aibă dreptul de a depune o plângere la o 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 Carta drepturilor fundamentale, 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 pe suport electronic, fără a exclude alte mijloace de comunicare.

(112) În cazul în care persoana vizată consideră că drepturile sale în temeiul prezentului regulament sunt încălcate, aceasta ar trebui să aibă dreptul să mandateze un organism, o organizație sau o asociație care are drept obiectiv asigurarea protecției drepturilor și a intereselor persoanelor vizate în ceea ce privește protecția datelor acestora și este constituit(ă) în conformitate cu legislația unui stat membru, să depună o plângere în numele său la o autoritate de supraveghere sau să exercite dreptul la o cale de atac în numele persoanelor vizate. Statele membre pot prevedea ca un astfel de organism, organizație sau asociație să aibă dreptul, în statul membru respectiv, de a depune o plângere, independent de mandatul acordat de o persoană vizată, și/sau să aibă dreptul la o cale de atac eficace 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 nu este în conformitate cu prezentul regulament. Acest organism, organizație sau asociație nu poate pretinde despăgubiri în numele unei persoane vizate.

(113)Orice persoană fizică sau juridică are dreptul de a introduce o acțiune în anulare îndreptată împotriva deciziilor Comitetului european pentru protecția datelor în fața Curții de Justiție a Uniunii Europene (denumită în continuare „Curtea de Justiție”), în conformitate cu condițiile prevăzute la articolul 263 din TFUE. În calitate de destinatare 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 european pentru protecția datelor vizează în mod direct și individual un operator, o persoană împuternicită de operator sau reclamantul, aceștia din urmă pot introduce o acțiune în anulare împotriva acestor decizii și ar trebui să facă acest lucru în termen de două luni de la publicarea deciziilor respective pe site-ul internet al Comitetului european pentru protecția datelor, 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 această 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, acest drept nu include alte măsuri ale autorităților de supraveghere care nu sunt obligatorii din punct de vedere juridic, cum ar fi avizele emise de autoritatea de supraveghere sau consultanța furnizată de aceasta. Acțiunile inițiate împotriva unei autorități de supraveghere ar trebui să fie aduse în fața instanțelor statului membru în care este stabilită autoritatea de supraveghere și ar trebui să se desfășoare în conformitate cu dreptul procesual național al statului membru respectiv. Respectivele instanțe ar trebui să își exercite competența deplină, care ar trebui să includă competența de a examina toate aspectele de fapt sau de drept care au relevanță pentru litigiul cu care acestea sunt sesizate. 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 european pentru protecția datelor este contestată în fața unei instanțe naționale și validitatea deciziei Comitetului european pentru protecția datelor este în discuție, respectiva instanță națională nu are competența de a declara nulă decizia Comitetului european pentru protecția datelor, 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 în cauza *Foto-Frost*[1], 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 european pentru protecția datelor 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.

(113a) Atunci când o instanță sesizată cu o procedură împotriva unei decizii a unei autorități de supraveghere are motive să creadă că au fost introduse proceduri în fața unei instanțe competente dintr-un alt stat membru cu privire la aceeași prelucrare, cum ar fi același obiect - în ceea ce privește activitățile de prelucrare ale aceluiași operator sau ale aceleiași persoane împuternicite 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, să își poată declina competența în favoarea instanței sesizate inițial, cu condiția ca aceasta din urmă să aibă competența de a soluționa procedurile în cauză și ca legislația aplicabilă 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.

(114) (...)

(115) (...)

---

[1] Cauza C-314/85

(116) 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 ce acționează în exercitarea competențelor sale publice.

(117) (…).

(118) Orice daună pe care o persoană o poate suferi ca urmare a unei prelucrări care nu este în conformitate cu prezentul regulament ar trebui să fie compensată de operator sau de persoana împuternicită de operator, care ar trebui să fie exonerați de răspundere dacă dovedesc că nu sunt în niciun fel răspunzători pentru daună (...). Conceptul de daune ar trebui interpretat, în sens larg, din perspectiva jurisprudenței Curții de Justiție a Uniunii Europene, într-un mod care să reflecte pe deplin obiectivele prezentului regulament. Această dispoziție nu aduce atingere niciunei cereri de despăgubiri care rezultă din încălcarea altor norme din dreptul Uniunii sau al statelor membre. (…)

Atunci când se face trimitere la o prelucrare care nu este în conformitate cu prezentul regulament, trimiterea vizează și prelucrarea care nu este în conformitate cu 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 daunele pe care le-au suferit. În cazul în care operatorii sau persoanele împuternicite de operatori sunt implicate în aceeași prelucrare, fiecare operator sau persoană împuternicită de operator ar trebui să fie considerat(ă) răspunzător (răspunzătoare) pentru întreaga daună. Cu toate acestea, atunci când procedurile juridice care le vizează sunt conexate, 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 daunele. 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.

(118a) 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 nu ar trebui să aducă atingere aplicării unor astfel de norme specifice.

(118b) Pentru a consolida punerea în aplicare a normelor prevăzute în prezentul regulament, pot fi impuse sancțiuni și amenzi administrative pentru orice încălcare a regulamentului, 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 daunele cauzate, 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 și amenzi administrative ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu Carta drepturilor fundamentale, inclusiv o protecție judiciară eficientă și un proces echitabil. În cazul în care dreptul intern al unui stat membru nu prevede amenzi administrative, statul membru în cauză poate să se abțină de la a prevedea amenzi administrative pentru încălcări ale prezentului regulament care fac deja obiectul sancțiunilor penale în dreptul său intern, asigurându-se că aceste sancțiuni penale sunt eficace, proporționate și disuasive, având în vedere nivelul amenzilor administrative prevăzute în prezentul regulament.

119) Statele membre pot stabili normele privind sancțiunile penale pentru încălcările prezentului regulament, inclusiv pentru încălcarea normelor naționale adoptate în temeiul și în limitele prezentului regulament. Aceste 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 naționale 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.

120) 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 infracțiunile, limita maximă și criteriile pentru stabilirea amenzilor administrative aferente, care ar trebui să fie stabilite de autoritatea de supraveghere competentă în fiecare caz particular, ținându-se 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 regulamentului și pentru a se preveni sau atenua consecințele încălcării. În cazul în care se impun amenzi unor persoane care nu sunt întreprinderi comerciale, autoritatea de supraveghere ar trebui să țină seama de nivelul general al veniturilor în statul membru respectiv atunci când estimează cuantumul adecvat al amenzii. Mecanismul pentru asigurarea coerenței poate fi, de asemenea, utilizat pentru a promova aplicarea consecventă a amenzilor administrative. Ar trebui să le revină statelor membre competența de a stabili dacă și în ce măsură autoritățile publice ar trebui să facă obiectul unor amenzi administrative. 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.

(120a) 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 regulamentului, 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 de dreptul intern.

(121) Legislația statelor membre ar trebui să stabilească un echilibru între normele care reglementează libertatea de exprimare şi de informare, inclusiv exprimarea jurnalistică, academică, artistică şi/sau literară, şi dreptul la protecţia datelor cu caracter personal în temeiul prezentului regulament. Prelucrarea datelor cu caracter personal în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare ar trebui să facă obiectul unor derogări sau al unor excepţii de la anumite dispoziţii ale prezentului regulament, în cazul în care este necesară stabilirea unui echilibru între dreptul la protecţia datelor cu caracter personal şi dreptul la libertatea de exprimare şi de informare, astfel cum este garantat prin articolul 11 din Carta drepturilor fundamentale a Uniunii Europene. Acest lucru ar trebui să se aplice în special prelucrării datelor cu caracter personal din domeniul audiovizualului, precum şi din arhivele de ştiri şi din bibliotecile ziarelor. Prin urmare, statele membre ar trebui să adopte măsuri legislative care să prevadă excepţiile şi derogările necesare în vederea asigurării echilibrului între aceste drepturi fundamentale. Astfel de excepţii şi derogări ar trebui să fie adoptate de statele membre în ceea ce privește principiile generale, drepturile persoanelor vizate, operatorul şi persoana împuternicită de operator, transferul de date cu caracter personal către țări terțe sau organizații internaționale, autoritățile de supraveghere independente, cooperarea și coerența. În cazul în care aceste excepții sau derogări diferă de la un stat membru la altul, ar trebui să se aplice legislația națională a 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. (...)

(121a) *Prezentul regulament permite luarea în considerare a principiului accesului publicului la documente oficiale, în aplicarea dispozițiilor prevăzute de acesta. Accesul public la documente oficiale poate fi considerat drept interes public. Datele cu caracter personal din documentele deținute de o autoritate publică sau de un organism public ar trebui să poată fi făcute publice de autoritatea sau organismul respectiv în cazul în care dreptuș Uniunii sau cel al statului membru sub incidența căruia intră autoritatea publică sau organismul public prevede acest lucru. O astfel de legislație 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 derogările necesare de la normele prezentului regulament. Trimiterea la autoritățile și organismele publice ar trebui, în acest context, să includă toate autoritățile sau alte organisme reglementate de legislația statelor membre privind accesul public la documente. Directiva 2003/98/CE a Parlamentului European și a Consiliului din 17 noiembrie 2003 privind reutilizarea informațiilor din sectorul public 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 legislația Uniunii și cu legislația națională 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 definită prin lege ca fiind incompatibilă cu legislația privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.*

(122) (…).

(123) (…).

(124) Legislația națională 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 în scopul recrutării, îndeplinirii prevederilor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii, al asigurării sănătății și securității la locul de muncă, precum și în scopul exercitării și beneficierii, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și în scopul încetării raporturilor de muncă.*

(125) Prelucrarea datelor cu caracter personal în scopuri (...) istorice, statistice sau științifice și în scopuri de arhivare în interes public (...) ar trebui, în plus față de principiile generale și normele specifice din prezentul regulament, în special în ceea ce privește condițiile pentru prelucrarea legală, să fie în conformitate și cu alte acte legislative relevante, cum ar fi cele privind studiile clinice. Prelucrarea ulterioară a datelor cu caracter personal în scopuri istorice, statistice sau științifice și în scopuri de arhivare în interes public (...) nu ar trebui să fie considerată incompatibilă cu scopurile pentru care datele au fost colectate inițial și pot fi prelucrate în respectivele scopuri mai mult timp decât este necesar pentru scopul inițial (…). Statele membre ar trebui să fie autorizate să ofere, în anumite condiții și în prezența unor garanții adecvate pentru persoanele vizate, precizări și derogări în ceea ce privește cererile de informații și drepturile de acces, de rectificare, de ștergere, de a fi uitat, restricții de prelucrare și dreptul la portabilitatea datelor, precum și dreptul la opoziție în cazul prelucrării datelor cu caracter personal în scopuri istorice, statistice sau științifice și în scopuri de arhivare (…). Condițiile și garanțiile în cauză pot genera proceduri specifice astfel încât persoanele vizate să își exercite respectivele drepturi, dacă acest lucru este corespunzător în contextul scopurilor vizate de către 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.

(125a) (…).

(125aa) Prin combinarea informațiilor din registre, cercetătorii pot obține noi cunoștințe de mare valoare în ceea ce privește, de exemplu, bolile cu largă răspândire, cum ar fi bolile cardiovasculare, cancerul, depresia etc. 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 impactul pe termen lung al unei serii de condiții sociale, precum șomajul, educația, și despre combinarea acestor informații 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, pot îmbunătăți calitatea vieții pentru un număr de persoane și eficiența serviciilor sociale etc.
Pentru a facilita cercetarea științifică, datele cu caracter personal pot fi prelucrate în scopuri științifice, sub rezerva condițiilor și a garanțiilor corespunzătoare stabilite de dreptului statului membru sau al Uniunii. De aceea, consimțământul persoanei vizate nu ar trebui să fie necesar pentru fiecare prelucrare ulterioară în scopuri științifice.

(125b) Rezoluția Consiliului din 6 mai 2003 privind arhivele în statele membre[2] a subliniat „importanța arhivelor pentru înțelegerea istoriei și a culturii Europei” și „faptul că arhivele accesibile și păstrate în condiții bune contribuie la funcționarea democratică a societăților noastre”. În cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare, prezentul regulament ar trebui să se aplice 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 să fie serviciile care, în conformitate cu legislația Uniunii sau a statului membru, au 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 fie autorizate să prevadă faptul că datele cu caracter personal pot fi prelucrate suplimentar în scopuri de arhivare, de exemplu cu scopul de a furniza informații specifice referitoare la comportamentul politic în perioada regimurilor fostelor state totalitare.

[2] JO C 113, 13.5.2003, p. 2.

Codurile de conduită pot să contribuie la aplicarea corespunzătoare a prezentului regulament, inclusiv în cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare în interes public, prin detalierea suplimentară a garanțiilor adecvate pentru drepturile și libertățile persoanelor vizate. Aceste coduri ar trebui să fie elaborate de arhivele oficiale ale statelor membre sau de către Grupul Arhivelor Europene. În ceea ce privește transferurile internaționale de date cu caracter personal incluse în arhive, acestea trebuie să aibă loc fără a aduce atingere normelor europene și naționale în vigoare privind circulația bunurilor culturale și a tezaurelor naționale.

(126) În cazul în care datele cu caracter personal sunt prelucrate în scopuri științifice, prezentul regulament ar trebui să se aplice și prelucrării respective. În sensul prezentului regulament, prelucrarea datelor cu caracter personal în scopuri științifice ar trebui să includă cercetarea fundamentală, cercetarea aplicată, cercetarea finanțată din surse private și ar trebui, în plus, să ia în considerare obiectivul Uniunii de creare a unui spațiu european de cercetare, astfel cum este menționat la articolul 179 alineatul (1) din Tratatul privind funcționarea Uniunii Europene. Scopurile științifice ar trebui să includă, de asemenea, studii efectuate în interes public în domeniul sănătății publice. Pentru a îndeplini caracteristicile de prelucrare a datelor cu caracter personal în scopuri științifice ar trebui să se aplice condiții specifice în special în ceea ce privește publicarea sau divulgarea datelor cu caracter personal în contextul scopurilor științifice. 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.

(126a)În cazul în care datele cu caracter personal sunt prelucrate în scopuri istorice, 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.

(126b)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.

(126c) 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 al statului membru 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 garanta confidențialitatea datelor statistice.*

(126d) *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 Tratatul privind funcționarea Uniunii Europene, în timp ce statisticile naționale ar trebui, de asemenea, să fie în conformitate cu legislația națională.*

Regulamentul (CE) nr. 223/2009 al Parlamentului European și al Consiliului din 11 martie 2009 privind statisticile europene și de abrogare a Regulamentului (CE, Euratom) nr. 1101/2008 al Parlamentului European și al Consiliului privind transmiterea de date statistice confidențiale Biroului Statistic al Comunităților Europene, a Regulamentului (CE) nr. 322/97 al Consiliului privind statisticile comunitare și a Deciziei 89/382/CEE, Euratom a Consiliului de constituire a Comitetului pentru programele statistice ale Comunităților Europene prevede specificații suplimentare privind confidențialitatea datelor statistice pentru statisticile europene.

(127) 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 sale, statele membre pot adopta, pe cale legislativă și în limitele stabilite de prezentul regulament, norme specifice pentru garantarea 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 secretul profesional în situațiile cerute de dreptul Uniunii.

(128) Conform articolului 17 din Tratatul privind funcționarea Uniunii Europene, 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. (…).

129) Pentru a se realiza obiectivele 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 Tratatul privind funcționarea Uniunii Europene ar trebui să fie delegată Comisiei. În special, ar trebui adoptate acte delegate în ceea ce privește **(...)** criteriile și cerințele privind mecanismele de certificare (...) (...). Este deosebit de important ca, pe durata activităților pregătitoare, Comisia să desfășoare 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.

130) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentului regulament, Comisia ar trebui investită cu competențe de executare pentru a stabili: **(…);** clauze contractuale standard între operatori și persoanele împuternicite de operatori, precum și între persoanele împuternicite de operatori; coduri de conduită; (…) standarde tehnice și mecanisme de certificare; nivelul adecvat de protecție oferit de o țară terță, de un teritoriu sau de un sector de prelucrare din țara terță respectivă sau de o organizație internațională; clauze standard de protecție a datelor; formatele și procedurile pentru schimbul de informații între operatori, persoanele împuternicite de operatori și autoritățile de supraveghere pentru regulile corporatiste obligatorii; (…) asistența reciprocă; **(…);** modalitățile de realizare a schimbului electronic de informații între autoritățile de supraveghere, precum și între autoritățile de supraveghere și Comitetul european pentru protecția datelor. Competențele respective ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie. În acest context, Comisia ar trebui să ia în considerare măsuri specifice pentru microîntreprinderi și pentru întreprinderi mici și mijlocii.

131) Procedura de examinare ar trebui utilizată pentru adoptarea de acte de punere în aplicare privind: clauze contractuale standard între operatori și persoanele împuternicite de operatori, precum și între persoanele împuternicite de operatori; coduri de conduită; (…) standarde tehnice și mecanisme de certificare; nivelul adecvat de protecție oferit de o țară terță, de un teritoriu sau de un sector de prelucrare din țara terță respectivă sau de o organizație internațională; clauze standard de protecție a datelor; formatul și procedurile pentru schimbul electronic de informații între operatori, persoanele împuternicite de operatori și autoritățile de supraveghere pentru regulile corporatiste obligatorii; asistența reciprocă; (…) modalitățile de realizare a schimbului electronic de informații între autoritățile de supraveghere, precum și între autoritățile de supraveghere și Comitetul european pentru protecția datelor, având în vedere că actele de punere în aplicare respective au un domeniu de aplicare general.

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

133) Dat fiind că obiectivele prezentului regulament, și anume asigurarea unui nivel echivalent de protecție a persoanelor și libera circulație a datelor în întreaga Uniune, nu pot fi realizate în mod satisfăcător de către statele membre și, prin urmare, având în vedere amploarea și efectele acțiunii, pot fi realizate mai bine la nivelul Uniunii, Uniunea poate să adopte măsuri în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este enunțat la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru atingerea acestui obiectiv.

134) Directiva 95/46/CE ar trebui să fie abrogată prin prezentul regulament. **Prelucrările în derulare la data intrării în vigoare a 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. Cu toate acestea, în cazul în care o astfel de prelucrare este în conformitate cu Directiva 95/46/CE, cerințele din prezentul regulament cu privire la efectuarea de evaluări ale impactului asupra protecției datelor și la consultarea prealabilă a autorității de supraveghere nu ar trebui să se aplice operațiunilor de prelucrare aflate deja în derulare înainte de intrarea în vigoare a prezentului regulament, având în vedere că aceste cerințe, prin însăși natura lor, urmează să fie îndeplinite înainte de prelucrare. În cazul în care o astfel de prelucrare este în conformitate cu Directiva 95/46/CE, nu este necesar nici ca persoana vizată să își dea încă o dată consimțământul pentru a permite operatorului să continue o astfel de prelucrare după data aplicării prezentului regulament.** Deciziile Comisiei adoptate și autorizațiile autorităților de supraveghere emise pe baza Directivei 95/46/CE rămân în vigoare **până când vor fi modificate, înlocuite sau abrogate**.

135) 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, inclusiv obligațiile privind operatorul și drepturile persoanelor fizice. Pentru a se clarifica relația dintre prezentul regulament și Directiva 2002/58/CE, aceasta din urmă 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 (...),

136) (...)

137) (...)

138) (…).

139) (...)

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I
DISPOZIȚII GENERALE

Articolul 1

Obiect și obiective

(1) Prezentul regulament stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, precum și normele referitoare la libera circulație a datelor cu caracter personal.

(2) Prezentul regulament asigură protecția drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului acestora la protecția datelor cu caracter personal.

(2a) Statele membre pot menține sau introduce dispoziții mai concrete de adaptare a aplicării normelor prezentului regulament în ceea ce privește prelucrarea datelor cu caracter personal în vederea respectării unei obligații legale, a îndeplinirii unei sarcini care servește unui interes public, în cadrul exercitării unei funcții publice atribuite operatorului sau pentru alte situații specifice de prelucrare, astfel cum este prevăzut la articolul 6 alineatul (1) literele (c) și (e) prin definirea unor cerințe specifice mai precise cu privire la prelucrare și a altor măsuri de asigurare a prelucrării legale și echitabile, inclusiv pentru alte situații concrete de prelucrare, astfel cum este prevăzut în capitolul IX.

(3) Libera circulație a datelor cu caracter personal în interiorul Uniunii nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

Articolul 2

Domeniul de aplicare material

(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuate 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 instituțiile, organele, oficiile și agențiile Uniunii;
(c) de către statele membre atunci când desfășoară activități care intră sub incidența titlului V capitolul 2 din Tratatul privind Uniunea Europeană;
(d) de către o persoană fizică (…) în cadrul unei activități (…) personale sau domestice;
(e) de către autoritățile competente (…) în scopul prevenirii, investigării, identificării sau urmăririi penale a infracțiunilor, al executării pedepselor sau al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.

(3) (…).

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.

(2) Prezentul regulament se aplică prelucrării datelor cu caracter personal ale persoanelor vizate care își au reședința în Uniune de către un operator care nu este stabilit 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 desfășoară în cadrul Uniunii Europene.

(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 legislația națională a unui stat membru 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 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;

2a. (...)

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

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

3b. „pseudonimizare” înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, în măsura în care aceste informații suplimentare sunt stocate separat și fac obiectul unor măsuri de natură tehnică și organizatorică destinate să garanteze neatribuirea unei persoane identificate sau identificabile (...).

4. „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;

5. „operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care, singur sau împreună cu altele, stabilește scopurile (…) și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile (…) și mijloacele de prelucrare sunt stabilite prin dreptul Uniunii sau al unui stat membru, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi stabilite prin dreptul Uniunii sau al statului membru;

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

7. „destinatar” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism (...) căruia îi sunt dezvăluite datele cu caracter personal, indiferent dacă este sau nu o parte terță; cu toate acestea, autoritățile cărora li se pot comunica date în cadrul unei anumite anchete nu sunt considerate destinatari ;

8. „consimțământul persoanei vizate” înseamnă orice manifestare de voință liberă, specifică și informată (…) prin care persoana vizată acceptă, printr-o declarație sau printr-o acțiune pozitivă fără echivoc, ca datele sale cu caracter personal să fie prelucrate;

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

(10) „date genetice” înseamnă toate datele cu caracter personal referitoare la caracteristicile genetice ale unei persoane care au fost moștenite sau dobândite (...) și care oferă informații unice privind fiziologia sau sănătatea persoanei respective, astfel cum rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

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

12. „date privind sănătatea” înseamnă date legate de sănătatea fizică sau mentală a unei persoane, care dezvăluie informații despre starea de sănătate a acesteia;

12a. „creare de profiluri” înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea acestor date pentru a evalua aspecte personale referitoare la o persoană fizică, în special pentru a analiza și a preconiza aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale sau interesele, fiabilitatea sau comportamentul, locația sau deplasările;

12b. (...)

13. „sediu principal” înseamnă

- în cazul unui operator cu sedii în cel puțin două state membre, 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, sediu care are competența de a dispune punerea în aplicare a acestor decizii, caz în care sediul care a luat deciziile respective este considerat ca fiind sediul principal;

- 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, iar 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;

14. „reprezentant” înseamnă orice persoană fizică sau juridică stabilită în Uniune, desemnată (…) de către operator în scris în temeiul articolului 25, care reprezintă operatorul în ceea ce privește obligațiile care îi revin acestuia în temeiul prezentului regulament (…);

15. „întreprindere” înseamnă orice 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;

16. „grup de întreprinderi” înseamnă o întreprindere care exercită controlul și întreprinderile controlate de aceasta;

17. „reguli corporatiste obligatorii” înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau o persoană împuternicită de operator stabilită pe teritoriul unui stat membru al Uniunii, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de societăți implicate într-o activitate economică comună;

18. (...)

19. „autoritate de supraveghere” înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 46;

19a. „autoritate de supraveghere *vizată*” înseamnă

- o autoritate de supraveghere care este vizată de procesul de prelucrare deoarece:

(a) operatorul sau persoana împuternicită de operator este stabilit(ă) pe teritoriul statului membru al acestei autorități de supraveghere;

(b) persoanele vizate care își au reședința în acest stat membru sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare; sau
(c) plângerea aferentă a fost depusă la această autoritate de supraveghere.

19b. „prelucrarea transnațională a datelor cu caracter personal” înseamnă:

(a) fie prelucrarea care are loc în contextul activităților sedi**ilor** din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, operatorul sau persoana împuternicită de operator având sedii în cel puțin două state membre,
(b) fie prelucrarea 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.

19c. „obiecție relevantă și motivată” înseamnă:
o obiecție în scopul de a stabili dacă există sau nu o încălcare a prezentului regulament sau, după caz, dacă măsurile preconizate în ceea ce privește operatorul sau persoana împuternicită de operator sunt în conformitate cu regulamentul. Textul obiecției 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.

20. „serviciile societății informaționale” înseamnă orice servicii definite la articolul 1 alineatul (2) din Directiva 98/34/CE a Parlamentului European și a Consiliului din 22 iunie 1998 de stabilire a unei proceduri pentru furnizarea de informații în domeniul standardelor și reglementărilor tehnice și al normelor privind serviciile societății informaționale.

21. „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 trebuie:

(a) să fie prelucrate în mod legal, echitabil și transparent față de persoana vizată;

(b) să fie colectate în scopuri determinate, explicite și legitime și să nu fie prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară a datelor cu caracter personal în vederea arhivării în interes public sau în scopuri *științifice*, statistice sau istorice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 83;

(c) să fie adecvate, relevante și neexcesive în raport cu scopurile în care sunt prelucrate (…);

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

(e) să fie 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 în scopuri de arhivare în interes public sau în scopuri *științifice*, statistice sau istorice în conformitate cu articolul 83, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în regulament în vederea garantării drepturilor și libertăților persoanei vizate;

(ee) să fie prelucrate într-un mod care să asigure securitatea adecvată a datelor cu caracter personal;

(f) (...)

(2) Operatorul este responsabil de respectarea alineatului (1).

Articolul 6

Legalitatea prelucrării

(1) Prelucrarea datelor cu caracter personal este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

(a) persoana vizată și-a dat consimțământul neechivoc 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 executarea unor măsuri precontractuale la cererea persoanei vizate;

(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;

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

(f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o terță parte, 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 minor. (…) .

(2) Prelucrarea datelor cu caracter personal necesară în vederea arhivării în interes public sau în scopuri istorice, statistice sau științifice este legală, fiind totodată sub rezerva condițiilor și a garanțiilor prevăzute la articolul 83.

(3) Temeiul juridic pentru prelucrarea menționată la alineatul (1) literele (c) și (e) trebuie să fie prevăzut în conformitate cu:

(a) dreptul Uniunii sau

(b) dreptul intern al statului membru care se aplică operatorului.

Scopul prelucrării este stabilit în acest temei juridic sau, în ceea ce privește prelucrarea menționată la alineatul (1) litera (e), trebuie să fie necesar pentru îndeplinirea unei sarcini efectuate în interes public sau în cadrul exercitării unei funcții publice atribuite operatorului. Acest temei juridic poate conține dispoziții specifice privind adaptarea aplicării normelor prezentului regulament, printre altele condițiile generale care reglementează legalitatea prelucrării datelor de către operator, tipul de date care fac obiectul prelucrării, persoanele vizate, entitățile cărora le pot fi dezvăluite datele și scopul pentru care respectivele date pot fi dezvăluite, limitările în funcție de scop, perioadele de stocare, operațiunile și procedurile de prelucrare, inclusiv măsurile de garantare a unei prelucrări legale și echitabile, inclusiv pentru alte situații concrete de prelucrare, astfel cum este prevăzut în capitolul IX.

(3a) Pentru a stabili dacă un scop al prelucrării ulterioare (...) este compatibil cu scopul pentru care datele au fost colectate inițial, cu excepția cazului în care persoana vizată și-a exprimat consimțământul, operatorul ia în considerare, printre altele:

(a) orice legătură dintre scopurile în care datele au fost colectate și scopurile prelucrării ulterioare preconizate;

(b) contextul în care au fost colectate datele;

(c) natura datelor cu caracter personal, în special în cazul prelucrării categoriilor speciale de date cu caracter personal, în conformitate cu articolul 9;

(d) posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;

(e) existența unor garanții adecvate.

(4) În cazul în care scopul prelucrării ulterioare este incompatibil cu scopul pentru care au fost colectate datele cu caracter personal de către același operator, prelucrarea ulterioară trebuie să aibă drept temei juridic cel puțin unul dintre cele menționate la alineatul (1) literele (a)-(e). Prelucrarea ulterioară de către același operator în scopuri incompatibile pe motive de interese legitime ale operatorului respectiv sau ale unei părți terțe este legală în cazul în care aceste interese prevalează asupra intereselor persoanei vizate.

(5) (...)

Articolul 7

Condiții privind consimțământul

(1) În cazul în care se aplică articolul 6 alineatul (1) litera (a), operatorul trebuie să fie în măsură să demonstreze că a fost acordat consimțământul fără echivoc de către persoana vizată.

(1a) În cazul în care se aplică articolul 9 alineatul (2) litera (a), operatorul trebuie să fie în măsură să demonstreze că a fost acordat consimțământul fără echivoc de către persoana vizată.

(2) În cazul în care consimțământul persoanei vizate urmează să fie acordat 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.

(3) Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragerea 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.

(4) (...)

Articolul 8

Condiții aplicabile în ceea ce privește consimțământul minorilor 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 minor, prelucrarea datelor cu caracter personal ale unui minor (...) este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești sau este acordat de minor în așa fel încât să fie considerat valid de legislația Uniunii sau a statelor membre.

(1a) Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri faptul că s-a acordat sau autorizat consimțământul de către titularul răspunderii părinteşti, ținând seama de tehnologiile disponibile.

(2) 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 minor.

(3) (...)

(4) **(…).**

Articolul 9

Prelucrarea de categorii speciale de date cu caracter personal

(1) Prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea datelor genetice sau a datelor privind sănătatea sau viața sexuală (…) este interzisă.

(2) Alineatul (1) nu se aplică în următoarele situații (...):

(a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal (…), cu excepția cazului în care dreptul Uniunii sau cel al statelor membre prevede ca interdicția prevăzută la alineatul (1) să nu poată fi ridicată prin consimțământul persoanei vizate; sau

(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 cel al statelor membre ori de un contract colectiv de muncă încheiat în temeiul dreptul statelor membre, care prevede garanții adecvate; sau

(c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale altei persoane, atunci când persoana vizată se află în incapacitate fizică sau juridică să-și dea consimțământul; sau

(d) prelucrarea este efectuată, în cadrul activităților lor legitime și cu garanții adecvate, de către o fundație, o asociație sau orice alt organism cu scop nelucrativ 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 să nu fie comunicate terților fără consimțământul persoanelor vizate; sau

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

(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; sau

(g) prelucrarea este necesară pentru (...)motive de interes public, în baza dreptului Uniunii sau al dreptului statelor membre, care prevede măsurile corespunzătoare și specifice pentru protejarea intereselor legitime ale persoanei vizate; sau

(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 statelor membre sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la alineatul (4); sau

(ha) (…)**;**

(hb) 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 statelor membre, care prevede măsuri adecvate și specifice pentru garantarea drepturilor și libertăților persoanei vizate; sau

(i) prelucrarea este necesară în vederea arhivării în interes public sau în scopuri istorice, statistice sau științifice (...) și face obiectul condițiilor și garanțiilor prevăzute în dreptul Uniunii sau al statelor membre, inclusiv obiectul condițiilor și garanțiilor menționate la articolul 83.

(j) (...)

(3) (...)

(4) *Datele cu caracter personal menționate la alineatul (1) pot fi prelucrate, în temeiul legislației Uniunii sau a statelor membre, în scopurile menționate la alineatul (2) litera (h) (...) în cazul în care respectivele date sunt prelucrate de către* sau sub responsabilitatea *unui (...) profesionist supus obligației de păstrare a secretului profesional în temeiul legislației Uniunii sau a statelor membre sau în temeiul normelor stabilite de organismele naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate în temeiul legislației Uniunii sau a statelor membre ori al normelor stabilite de organismele naționale competente*.

(4a) **(…)**.

(5) Statele membre pot menține sau introduce dispoziții mai concrete în ceea ce privește datele genetice sau datele privind sănătatea. Acest lucru include posibilitatea introducerii **(...)** de către statele membre a unor condiții suplimentare pentru prelucrarea acestor date**.**

Articolul 9a

Prelucrarea datelor referitoare la condamnări penale și infracțiuni

Prelucrarea datelor referitoare la condamnări penale și infracțiuni sau la măsuri de securitate conexe în temeiul articolului 6 alineatul (1) se poate efectua numai fie sub controlul autorității publice (...), fie atunci când prelucrarea este (...) autorizată de dreptul Uniunii sau de cel al statelor membre care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate. Un registru complet al condamnărilor penale poate fi ținut numai sub controlul autorității publice.

Articolul 10

Prelucrarea care nu necesită identificarea

(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 sau obține (...) informații suplimentare și nici de a efectua o prelucrare suplimentară pentru a identifica persoana vizată în scopul unic al respectării (…) prezentului regulament.(…)

(2) Dacă, în astfel de cazuri, operatorul nu este în măsură să identifice persoana vizată, articolele 15, 16, 17, 17a, 17b și 18 nu se aplică, cu excepția cazului în care persoana vizată, în scopul exercitării drepturilor sale în temeiul acestor articole, oferă informații suplimentare care permit identificarea sa.

CAPITOLUL III

DREPTURILE PERSOANEI VIZATE

SECȚIUNEA 1

TRANSPARENȚĂ ȘI MODALITĂȚI

Articolul 11

Transparența informațiilor și a comunicărilor

(1) (...)

(2) (...)

Articolul 12

Transparența informațiilor, a comunicărilor și a modalităților referitoare la exercitarea drepturilor persoanei vizate

(1) Operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informații menționate la articolele 14 și 14a și orice comunicări în temeiul articolelor 15-19 și 32 referitoare la prelucrarea datelor cu caracter personal, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Informațiile se furnizează în scris sau prin alte mijloace**,** după caz pe cale electronică. În cazul în care persoana vizată introduce cererea în format electronic, informațiile pot, de regulă, să fie furnizate în format electronic, cu excepția cazului în care persoana vizată solicită un alt format. La solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită.

(1a) Operatorul facilitează exercitarea drepturilor persoanei vizate în temeiul articolelor 15-19. (...) În cazurile menționate la articolul 10 alineatul (2), operatorul nu refuză să dea curs cererii persoanei vizate de a-și exercita drepturile în conformitate cu articolele 15-19, cu excepția cazului în care operatorul demonstrează că nu este în măsură să identifice persoana vizată.

(2) Operatorul furnizează persoanei vizate (...) informațiile privind acțiunile întreprinse în urma unei cereri în temeiul articolelor 15 și 16-19, fără întârzieri nejustificate și cel mai târziu în termen de o lună de la primirea cererii (…). Această perioadă poate fi prelungită cu încă două luni atunci când este necesar, ținându-se seama de complexitatea cererii și de numărul de cereri. În cazurile în care se aplică prelungirea, persoana vizată este informată cu privire la motivele amânării în termen de o lună de la primirea cererii.

(3) În cazul în care operatorul nu ia măsuri cu privire la cererea persoanei vizate, acesta informează persoana vizată, fără întârzieri nejustificate și cel mult în termen de 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 (…).

(4) Informațiile furnizate în temeiul articolelor 14 și 14a (…)și orice comunicare în temeiul articolelor 16-19 și 32 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 refuza să le trateze. În acest caz, operatorului îi revine sarcina de a demonstra caracterul *vădit* nefondat sau excesiv al cererii.

(4a) Fără a aduce atingere articolului 10, în cazul în care operatorul are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea menționată la articolele 15-19, acesta poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

(5) (...)

(6) (...)

Articolul 13

Drepturi referitoare la destinatari

(...)

SECȚIUNEA 2

INFORMARE ȘI ACCES LA DATE

Articolul 14

Informații care trebuie furnizate în cazul în care datele 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 următoarele informații:

(a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia; operatorul include, de asemenea, datele de contact ale responsabilului cu protecția datelor, dacă acesta există;

(b) scopurile în care sunt prelucrate datele cu caracter personal (...), precum și temeiul juridic al prelucrării.

(1a) Pe lângă informațiile menționate la alineatul (1), operatorul furnizează persoanei vizate, în momentul obținerii datelor cu caracter personal, informațiile 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:

(a) (…);

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

(d) dacă este cazul, intenția operatorului de a efectua un transfer de date cu caracter personal către un destinatar dintr-o țară terță sau către o organizație internațională;

(e) 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 lor, existența dreptului de a se opune prelucrării acestor date cu caracter personal (…), precum și existența dreptului la portabilitatea datelor;

(ea) 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;

(f) dreptul de a depune o plângere în fața unei autorități de supraveghere (…);

(g) 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 și care sunt eventualele consecințe ale nerespectării acestei obligații;

(h) *existența* unui proces decizional automatizat, incluzând *crearea de profiluri, menționat la articolul 20 alineatele (1) și (3), precum și informații privind* (…) logica utilizată *și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată*.

(1b) În cazul în care operatorul intenționează să prelucreze în mod suplimentar datele **(...)** 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 (1a).

(2) (...)

(3) (...)

(4) (...)

(5) Alineatele (1), (1a) și (1b) nu se aplică dacă și în măsura în care persoana vizată deține deja informațiile respective.

(6) (...)

(7) (...)

(8) (...)

Articolul 14a

Informații care trebuie furnizate în cazul în care datele 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; operatorul include, de asemenea, datele de contact ale responsabilului cu protecția datelor, dacă acesta există;

(b) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării.

(2) Pe lângă informațiile menționate la alineatul (1), operatorul furnizează persoanei vizate informațiile suplimentare care sunt necesare pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată, ținând seama de circumstanțele specifice și de contextul în care sunt prelucrate datele cu caracter personal (…):

(a) categoriile de date cu caracter personal vizate;

(b) (...)

(c) 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;

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

(da) dacă este cazul, intenția operatorului de a efectua un transfer de date cu caracter personal către un destinatar dintr-o țară terță sau către o organizație internațională;

(e) 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 lor, existența dreptului de a se opune prelucrării acestor date cu caracter personal, precum și existența dreptului la portabilitatea datelor (...);

(ea) 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;

(f) dreptul de a depune o plângere în fața unei autorități de supraveghere (…);

(g) sursa din care provin datele cu caracter personal, cu excepția cazului în care acestea provin din surse disponibile public;

(h) existența unui proces decizional automatizat, incluzând *crearea de profiluri, menționat la articolul 20 alineatele (1) și (3), precum și informații 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, dar nu mai mare de o lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele, sau

(b) dacă se intenționează dezvăluirea datelor către un alt destinatar, cel mai târziu la data la care acestea sunt dezvăluite pentru prima oară.

(3a) În cazul în care operatorul intenționează să prelucreze în mod suplimentar datele (...) 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).

(4) Dispozițiile alineatelor (1)-(3a) nu se aplică dacă și în măsura în care:

(a) persoana vizată deține deja informațiile; sau

(b) furnizarea acestor informații (...) se dovedește a fi imposibilă sau ar implica eforturi disproporționate ; în astfel de cazuri, operatorul ia măsurile adecvate pentru a proteja drepturile, libertățile și interesele legitime *ale persoanei vizate*; sau

(c) obținerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de cel al statului membru sub incidența căruia intră operatorul, care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau

(d) (…).

(e) în cazul în care datele trebuie să rămână confidențiale, în conformitate cu dreptul Uniunii sau al statului membru**(...)**.

(5) (...)

(6) (...)

Articolul 15

Dreptul de acces al persoanei vizate

(1) Persoana vizată are dreptul de a obține din partea operatorului, la intervale rezonabile și în mod gratuit (…), o confirmare a prelucrării sau nu a datelor cu caracter personal care o privesc și, în cazul în care aceste date cu caracter personal sunt prelucrate, acces la datele respective și la următoarele informații:

(a) scopurile prelucrării;

(b) (...)

(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) dacă este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal;

(e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării acestor date;

(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) în cazul deciziilor bazate pe prelucrarea automată, inclusiv crearea de profiluri,menționate la articolul 20 alineatele (1) și (3),informații privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări.

(1a) 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 42 referitoare la transfer.

(1b) La cerere şi fără tarife excesive, operatorul furnizează persoanei vizate o copie a datelor cu caracter personal care fac obiectul prelucrării.

(2) (...)

(2a) Dreptul de a obține o copie menționată la alineatul (1b)(...) nu se aplică în cazul în care o astfel de copie nu poate fi furnizată fără a dezvălui date cu caracter personal ale altor persoane vizate sau date confidențiale ale operatorului. Mai mult, acest drept nu se aplică în cazul în care dezvăluirea datelor cu caracter personal ar încălca drepturile de proprietate intelectuală referitoare la prelucrarea datelor cu caracter personal respective.

(3) (...)

(4) (...)

SECȚIUNEA 3

RECTIFICARE ȘI ȘTERGERE

Articolul 16

Dreptul la rectificare

(1) (…) Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal care o privesc și care sunt inexacte. 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.

(2) (...)

Articolul 17

Dreptul la ștergerea datelor și dreptul „de a fi uitat”

(1) (...) Operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate, în special cele colectate când persoana vizată era minoră, iar persoana vizată are dreptul să obțină de la operator ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, în cazul în care se aplică unul dintre motivele următoare:

(a) datele 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 datelor;

(c) persoana vizată se opune prelucrării datelor cu caracter personal în temeiul articolului 19 alineatul (1) și nu există motive legitime care să primeze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării datelor cu caracter personal în temeiul articolului 19 alineatul (2);

(d) datele au fost prelucrate ilegal;

(e) datele trebuie șterse pentru respectarea unei obligații legale care revine operatorului;

(1a) Persoana vizată are, de asemenea, dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, în cazul în care datele au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la articolul 8 alineatul (1).

(…) .

(2) (…) .

(2a) În cazul în care operatorul (...) a făcut publice datele cu caracter personal și este obligat, în temeiul alineatului (1), să le șteargă, o*peratorul, ținând seama de tehnologia disponibilă și de costul implementării*, ia (...) măsuri rezonabile, inclusiv măsuri tehnice, (...) pentru a informa operatorii care prelucrează datele 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), (1a) și (2a) nu se aplică în măsura în care (…) prelucrarea datelor cu caracter personal este necesară:

a. pentru exercitarea dreptului la liberă exprimare și la informare ;

b. pentru respectarea unei obligații legale care prevede prelucrarea *datelor cu caracter personal în temeiul legislației Uniunii sau a statului membru 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 (hb) și cu articolul 9 alineatul (4);

d. în scopuri de arhivare în interes public sau în scopuri *științifice, statistice* și istorice (…) în conformitate cu articolul 83;

e. (...)

f. (...)

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

(4) (...)

(5) (...)

Articolul 17*a*

Dreptul la restricționarea prelucrării

1. Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării datelor cu caracter personal în cazul în care:

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

(b) 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

(c) persoana vizată s-a opus prelucrării în conformitate cu articolul 19 alineatul (1), pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

2. (...)

(3) În cazul în care prelucrarea datelor cu caracter personal a fost restricționată în temeiul alineatului (1), astfel de date 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.

(4) O persoană vizată care a obținut restricționarea prelucrării în temeiul alineatului (1) (…) este informată de către operator înainte de ridicarea restricției de prelucrare.

(5) (...)

(5a) (...)

Articolul 17b

Obligația de notificare privind rectificarea, ștergerea sau restricționarea

Operatorul comunică fiecărui destinatar căruia i-au fost dezvăluite datele **(...)** orice rectificare, ștergere sau restricționare a prelucrării efectuată în conformitate cu articolul 16, articolul 17 alineatul (1) și articolul 17a, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate.

Articolul 18

Dreptul la portabilitatea datelor

(1) (...)

(2) 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 prelucrabil automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele, 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.

(2a) Exercitarea acestui drept nu aduce atingere articolului 17. Dreptul menționat la alineatul (2) nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul.

(2aa) Dreptul menționat la alineatul (2) nu se aplică în cazul în care dezvăluirea datelor cu caracter personal ar încălca drepturile de proprietate intelectuală referitoare la prelucrarea datelor cu caracter personal respective.

(3) (...)

(4) (…).

SECȚIUNEA 4

DREPTUL LA OPOZIȚIE ȘI PROCESUL DECIZIONAL AUTOMATIZAT (…)

Articolul 19

Dreptul la opoziție

(1) În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situația particulară în care se află, prelucrării în temeiul articolului 6 alineatul (1) litera (…) (e) sau (f) sau al articolului 6 alineatul (4) prima teză coroborată cu articolul 6 alineatul (1) litera (e) sau cu articolul 6 alineatul (4) a doua teză, a datelor cu caracter personal care o privesc.

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 primează asupra intereselor, (...) drepturilor și libertăților persoanei vizate sau că scopul este *constatarea, exercitarea sau apărarea unui drept în instanță*.

(1a) (...)

(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. Cel târziu în momentul primei comunicări cu persoana vizată, acest drept este adus în mod explicit în atenția persoanei vizate (…) și este prezentat în mod clar și separat de orice alte informații.

(2a) În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.

(2aa) În cazul în care datele cu caracter personal sunt prelucrate în scopuri istorice, statistice sau științifice, 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.

(3) (…)

(4) (...)

Articolul 20

Procesul decizional automatizat

(1) Persoana vizată are dreptul de a nu face obiectul unei decizii (…) bazate exclusiv pe prelucrarea automată, incluzând crearea de profiluri, care *produce efecte juridice* care privesc persoana vizată sau o afectează în mod semnificativ.

(1a) 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 (...); sau

(b) este (…) autorizată de legislația Uniunii sau a unui stat membru 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 (…).

(1b) În cazurile menționate la alineatul (1a) 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.

(2) (...)

(3) Deciziile menționate la alineatul (1a) nu (…) se bazează pe 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 au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate.

(4) (...)

(5) (...)

SECȚIUNEA 5
RESTRICȚII

Articolul 21

Restricții

(1) Legislația Uniunii sau a unui stat membru care se aplică operatorului de date sau persoanei împuternicite de acesta poate restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la (…) articolele 12-20 și 32, precum și la articolul 5 în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la articolele 12-20, atunci când o astfel de restricție constituie o măsură necesară și proporțională într-o societate democratică pentru a asigura:

(aa) securitatea națională;

(ab) apărarea;

(a) securitatea publică;

(b) prevenirea, investigarea, detectarea sau urmărirea penală a infracțiunilor sau executarea pedepselor penale, sau protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;

(c) 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, în domeniul sănătății publice și al securității sociale, precum și privind protecția stabilității și a integrității pieței;

(ca) protecția independenței judiciare și a procedurilor judiciare;

(d) prevenirea, investigarea, detectarea și punerea sub urmărire a încălcării eticii în cazul profesiilor reglementate;

(e) funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale în cazurile menționate la literele (aa), (ab), (a), (b), (c) și (d);

(f) protecția persoanei vizate sau a drepturilor și libertăților altora;

(g) punerea în aplicare a pretențiilor de drept civil.

(2) Orice măsură legislativă menționată la alineatul (1) conține dispoziții specifice cel puțin, dacă este cazul, în ceea ce privește obiectivele prelucrării sau ale categoriilor de prelucrare, categoriile de date cu caracter personal, domeniul de aplicare al restricțiilor introduse, menționarea operatorului sau a categoriilor de operatori, perioadele de stocare și garanțiile aplicabile având în vedere natura, domeniul de aplicare și scopurile prelucrării sau ale categoriilor de prelucrare, precum și riscurile la adresa drepturilor și libertăților persoanelor vizate.

CAPITOLUL IV

OPERATORUL ȘI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

SECȚIUNEA 1

OBLIGAȚII GENERALE

Articolul 22

Obligațiile operatorului

(1) Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de probabilitatea de a se materializa și de gravitatea riscului la adresa drepturilor și libertăților persoanelor fizice, operatorul (…) pune în aplicare măsuri adecvate și este în măsură să demonstreze că prelucrarea datelor cu caracter personal se efectuează în conformitate cu prezentul regulament.

(2) (...)

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

(2b) Aderarea la coduri de conduită aprobate, în conformitate cu articolul 38, sau la un mecanism de certificare aprobat, în conformitate cu articolul 39, poate fi utilizată ca element care să demonstreze respectarea obligațiilor de către operator.

(3) (...)

(4) (...)

Articolul 23

Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

(1) (...) Având în vedere tehnologia disponibilă și costul punerii în aplicare și *ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de probabilitatea de materializare și de gravitatea riscului la adresa drepturilor și libertăților persoanelor fizice aferent prelucrării*, operatorii pun în aplicare (…) măsuri tehnice și organizatorice adecvate pentru activitatea de prelucrare desfășurată și pentru obiectivele acesteia, precum reducerea sa la minimum și pseudonimizarea, în așa fel încât prelucrarea să îndeplinească cerințele prezentului regulament și să protejeze drepturile (…) persoanelor vizate.

(2) Operatorul pune în aplicare măsuri adecvate prin care să se asigure că, în mod implicit, sunt prelucrate numai (…) date cu caracter personal (…) care sunt necesare pentru fiecare scop specific al prelucrării; acest lucru se aplică volumului de (…) date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În cazul în care scopul prelucrării nu este de a furniza informații publicului, aceste mecanisme asigură faptul că, în mod implicit, datele cu caracter personal nu sunt accesibile, fără intervenție umană, unui număr nedefinit de persoane.

(2a) Un mecanism de certificare aprobat în conformitate cu articolul 39 *poate fi utilizat drept element* care să demonstreze îndeplinirea cerințelor prevăzute la alineatele (1) și (2).

(3) (...)

(4) (...)

Articolul 24

Operatori asociați

(1) În cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare a datelor cu caracter personal, 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 14 și 14a, prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite de legislația Uniunii sau a unui stat membru care se aplică acestora. Acordul desemnează care dintre operatorii asociați acționează ca punct unic de contact pentru exercitarea de către persoanele vizate a drepturilor lor.

(2) Indiferent de termenii 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.

(3) Acordul reflectă în mod adecvat rolurile și relațiile corespunzătoare efective ale operatorilor asociați față de persoanele vizate, iar esența acestui acord este făcută cunoscută persoanei vizate. Alineatul (2) nu se aplică în cazul în care persoana vizată a fost informată în mod transparent și lipsit de echivoc cu privire la operatorul asociat căruia îi revine responsabilitatea, cu excepția cazului în care un astfel de acord, altul decât cel stabilit de legislația Uniunii sau a statului membru, este inechitabil în ceea ce privește drepturile sale (...).

Articolul 25

Reprezentanții operatorilor care nu își au sediul în Uniune

(1) În cazul în carese aplică articolul 3 alineatul (2), operatorul desemnează în scris un reprezentant în Uniune.

(2) Prezenta obligație nu se aplică:

(a) (...); sau

(b) *prelucrării care are* un caracter ocazional şi *care este puțin susceptibilă de a genera un* (...) *risc la adresa drepturilor și libertăților persoanelor fizice, ținând cont de natura, contextul, domeniul de aplicare și scopurile prelucrării* (...); sau

(c) unei autorități sau unui organism public;

(d) (...)

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

(3a) Reprezentantul primește din partea operatorului un mandat prin care autoritățile de supraveghere și persoanele vizate, în special, se pot adresa reprezentantului, în plus față de operator sau în locul acestuia, cu privire la toate chestiunile legate de prelucrarea datelor cu caracter personal, în scopul asigurării respectării prezentului regulament.

(4) Desemnarea unui reprezentant de către operator nu aduce atingere acțiunilor în justiție care ar putea fi introduse împotriva operatorului însuși.

Articolul 26

Persoana împuternicită de operator

(1) (…). Operatorul utilizează numai persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a măsurilor tehnice și organizatorice adecvate (…), astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament (…).

(1a) Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil consimțământul scris, specific sau general, al operatorului. În acest ultim caz, persoana împuternicită de operator ar trebui să informeze întotdeauna 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 .

(1b) (…).

(2) Efectuarea prelucrării de către o persoană împuternicită de un operator este reglementată printr-un contract sau un act juridic în temeiul legislației Uniunii sau a unui stat membru care creează obligații pentru persoana împuternicită de operator în raport cu operatorul, care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate,drepturile operatorului (...) și care prevede în special că respectiva persoană împuternicită:

(a) prelucrează datele cu caracter personal numai la cererea operatorului (…), cu excepția cazului în care această obligație îi revine în temeiul legislației Uniunii sau a unui stat membru care i se aplică; în acest caz, notifică această obligație juridică operatorului înainte de a prelucra datele, cu excepția cazului în care legislația respectivă interzice o astfel de notificare din motive importante legate de interesul public;

(b) (...)

(c) adoptă toate (…) măsurile necesare în conformitate cu articolul 30;

(d) respectă condițiile recrutării unei alte persoane împuternicite de operator (...), cum ar fi condiția autorizării prealabile speciale de către operator;

(e) (…) ținând seama de natura prelucrării, oferă asistență operatorului în ceea ce privește răspunsurile la cererile de exercitare de către persoana vizată a drepturilor prevăzute în capitolul III;

(f) (...) ajută operatorul să asigure respectarea obligațiilor prevăzute la articolele 30-34;

(g) returnează sau șterge, în funcție de opțiunea operatorului, datele cu caracter personal după încetarea furnizării serviciilor de prelucrare a datelor prevăzute în contract sau în alt act juridic, cu excepția cazului în care legislația Uniunii sau a unui stat membru care se aplică persoanei împuternicite impune obligația de a stoca datele respective;

(h) pune la dispoziția operatorului (…) toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute la prezentul articol, permite desfășurarea auditurilor efectuate de operator și contribuie la acestea.

Persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucțiune încalcă prezentul regulament sau dispozițiile Uniunii sau ale unui stat membru referitoare la protecția datelor.

(2a) 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 (2), revin celei de a doua persoane împuternicite, *prin intermediul unui contract sau al unui alt act juridic, în temeiul legislației Uniunii sau a unui stat membru,* în special furnizarea de garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice corespunzătoare, 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.

(2aa) Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, în conformitate cu articolul 38, sau la un mecanism de certificare aprobat, în conformitate cu articolul 39, poate fi utilizată ca element care să demonstreze *existența garanțiilor suficiente menționate la alineatul (1) și la alineatul (2a)*.

(2ab) Fără a aduce atingere unui contract individual încheiat între un operator și o persoană împuternicită de operator, contractul sau un alt act juridic menționat la alineatele (2) și (2a) se poate baza, integral sau parțial, pe clauze contractuale standard menționate la alineatele (2b) și (2c) sau pe clauze contractuale standard care fac parte din certificarea acordată operatorului sau persoanei împuternicite de operator în temeiul articolelor 39 și 39a.

(2b) Comisia poate să prevadă clauze contractuale standard pentru aspectele menționate la alineatele (2) și (2a) și în conformitate cu procedura de examinare menționată la articolul 87 alineatul (2).

(2c) O autoritate de supraveghere poate să adopte clauze contractuale standard pentru aspectele menționate la alineatele (2) și (2a) și în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 57.

(3) Contractul sau un alt act juridic menționat la alineatele (2) și (2a) se formulează în scris, inclusiv în format electronic.

(4) (...)

(5) (...)

Articolul 27

Desfășurarea activității de prelucrare sub autoritatea operatorului și a persoanei împuternicite de operator

(...)

Articolul 28

Evidențe ale categoriilor de activități de prelucrare a datelor cu caracter personal

(1) Fiecare operator (…), precum și reprezentantul său dacă acesta există, păstrează evidențe ale tuturor categoriilor de activități de prelucrare a datelor cu caracter personal desfășurate sub responsabilitatea sa. Aceste evidențe cuprind (…) următoarele informații:

(a) numele și datele de contact ale operatorului și ale oricărui operator asociat (…), reprezentant al operatorului și responsabil cu protecția datelor, dacă aceștia există;

(b) (...)

(c) scopul prelucrării, inclusiv interesele legitime atunci când prelucrarea se bazează pe articolul 6 alineatul (1) litera (f);

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

(e) (…) categoriile de destinatari cărora le-au fost sau le vor fi dezvăluite datele cu caracter personal, în special destinatarii din țări terțe;

(f) acolo unde este cazul, categoriile de transferuri de date cu caracter personal către țări terțe sau organizații internaționale (...);

(g) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;

(h) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 30 alineatul (1).

(2a) Fiecare persoană împuternicită de operator păstrează evidențe ale tuturor categoriilor de activități de prelucrare a datelor cu caracter personal 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 ale reprezentantului operatorului, dacă acesta există;

(b) numele și datele de contact ale responsabilului cu protecția datelor, dacă acesta există;

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

(d) acolo unde este cazul, categoriile de transferuri de date cu caracter personal către țări terțe sau organizații internaționale;

(e) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 30 alineatul (1).

(3a) Evidențele prevăzute la alineatele (1) și (2a) se păstrează în scris, inclusiv în formă electronică sau în altă formă ilizibilă, care să poată fi convertită într-o formă lizibilă.

(3) La cerere, operatorul și persoana împuternicită de acesta, precum și reprezentantul operatorului dacă acesta există, pun evidențele la dispoziția autorității de supraveghere (…).

(4) Obligațiile menționate la alineatele (1) și (2a) nu se aplică:

(a) (…);

(b) unei întreprinderi sau unui organism cu mai puțin de 250 de angajați, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanei vizate, cum ar fi (...) discriminarea, furtul sau frauda de identitate, inversarea neautorizată a pseudonimizării, pierderea financiară, compromiterea reputației, pierderea confidențialității datelor protejate prin secret profesional sau orice alt dezavantaj de natură economică sau socială pentru persoanele vizate, ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării;

(5) (...)

(6) (...)

Articolul 29

Cooperarea cu autoritatea de supraveghere

(...)

SECȚIUNEA 2
SECURITATEA DATELOR

Articolul 30

Securitatea prelucrării

(1) Având în vedere tehnologia disponibilă și costurile punerii în aplicare și ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de probabilitatea de materializare și gravitatea riscului la adresa drepturilor și libertăților persoanelor fizice, operatorul și persoana împuternicită de acesta pun în aplicare măsuri tehnice și organizatorice adecvate, precum pseudonimizarea datelor cu caracter personal, în vederea asigurării unui nivel de securitate corespunzător acestui risc.

(1a) La evaluarea nivelului corespunzător de securitate, se ține seama în special de risc**urile** prezentate de prelucrarea datelor, (...) 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 în alt mod.

(2) (...)

(2a) Aderarea la coduri de conduită aprobate, în conformitate cu articolul 38, sau la un mecanism de certificare aprobat, în conformitate cu articolul 39, poate fi utilizată ca element care să *demonstreze îndeplinirea cerințelor prevăzute la alineatul (1).*

(2b) Operatorul și persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de acesta și care are acces la datele cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul legislației Uniunii sau a statului membru.

(3) (...)

(4) (...)

Articolul 31

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, care este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, cum ar fi discriminarea, furtul sau frauda de identitate, pierderea financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială, operatorul notifică acest lucru autorității de supraveghere competente în temeiul articolului 51, fără întârzieri nejustificate și, în cazul în care este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta. Notificarea autorității de supraveghere este însoțită de o explicație motivată în cazul în care nu are loc în termen de 72 de ore.

(1a) Notificarea menționată la alineatul (1) nu este necesară dacă nici informarea persoanei vizate nu este necesară în temeiul articolului 32 alineatul (3) literele (a) și (b).

(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) trebuie cel puțin:

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

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

(c) (...)

(d) să descrie consecințele probabile, identificate de operator, ale încălcării securității datelor cu caracter personal;

(e) să descrie măsurile luate sau propuse de operator pentru a remedia problema încălcării securității datelor cu caracter personal; și

(f) dacă este cazul, să indice măsuri de atenuare a eventualelor efecte negative ale încălcării respective.

(3a) În cazul în care și în măsura în care furnizarea informațiilor menționate la alineatul (3) literele (d), (e) și (f) în același timp cu informațiile menționate la alineatul (3) literele (a) și (b) nu este posibilă, operatorul furnizează informațiile respective fără întârzieri nejustificate.

(4) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal menționate la alineatele (1) și (2), care cuprind o descriere a situației în care a avut loc încălcarea, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație trebuie să permită autorității de supraveghere să verifice conformitatea cu prezentul articol. (…).

(5) (...)

(6) (...)

Articolul 32

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 la adresa drepturilor și libertăților persoanelor fizice, cum ar fi discriminarea, furtul sau frauda de identitate, pierderea financiară, compromiterea reputației, inversarea neautorizată a pseudonimizării, pierderea confidențialității datelor protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială, operatorul (…) informează persoana vizată, fără întârzieri nejustificate, cu privire la această încălcare.

(2) În informarea transmisă persoanei vizate, prevăzută la alineatul (1), se include o descriere a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile și recomandările prevăzute la articolul 31 alineatul (3) literele (b), (e) și (f).

(3) Informarea (…) persoanei vizate, menționată la alineatul (1), nu este necesară în cazul în care:

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

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

c. ar necesita un efort disproporționat, în special ca urmare a numărului de cazuri implicate. 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; sau

d. ar afecta în mod negativ un interes public major.

(4) (...)

(5) (...)

(6) (...)

SECȚIUNEA 3

EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR ȘI CONSULTAREA PREALABILĂ

Articolul 33

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 la adresa drepturilor și libertăților persoanelor fizice, cum ar fi discriminarea, furtul sau frauda de identitate, pierderea financiară, compromiterea reputației, inversarea neautorizată a pseudonimizării, pierderea confidențialității datelor protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială, operatorul (…) efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. (…).

(1a) La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat.

(2) Evaluarea impactului asupra protecției datelor menționată la alineatul (1) se impune mai ales în următoarele cazuri:

(a) o evaluare sistematică și cuprinzătoare (…) a aspectelor personale referitoare la (…) persoane fizice (…), care se bazează pe crearea de profiluri și care stă la baza deciziilor care produc efecte juridice privind persoanele vizate sau care afectează grav persoanele vizate;

(b) prelucrarea unor categorii speciale de date cu caracter personal în temeiul articolului 9 alineatul (1) (...), a unor date biometrice sau a unor date privind condamnările penale și infracțiunile sau măsuri de securitate conexe, atunci când prelucrarea datelor se efectuează pentru adoptarea (…) unor decizii care vizează anumite persoane pe scară largă;

(c) monitorizarea zonelor accesibile publicului *la scară largă*, mai ales în cazul utilizării dispozitivelor optoelectronice (…);

(d) (…).

(e) (…).

(2a) 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 european pentru protecția datelor.

(2b) 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 european pentru protecția datelor.

(2c) Înainte de adoptarea listelor menționate la alineatele (2a) și (2b), autoritatea de supraveghere competentă aplică mecanismul pentru asigurarea coerenței menționat la articolul 57, 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.

(3) Evaluarea cuprinde cel puțin o descriere generală a operațiunilor de prelucrare preconizate, o evaluare a riscului menționat la alineatul (1), măsurile preconizate în vederea abordării riscului, 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 celorlalte persoane interesate.

(3a) La evaluarea legalității și a impactului operațiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevanți (relevante) se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate menționate la articolul 38, în special în vederea unei evaluări a impactului asupra protecției datelor.

(4) *Operatorul solicită avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută,* fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare (...).

(5) (...) 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, alineatele (1)-(3) nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.

(6) (...)

(7) (...)

Articolul 34

Consultare (…) prealabilă

(1) (...)

(2) Operatorul (…) consultă autoritatea de supraveghere înainte de prelucrarea datelor cu caracter personal în cazul în care evaluarea impactului asupra protecției datelor, prevăzută la articolul 33, indică faptul că prelucrarea ar genera un (...) risc ridicat în absența măsurilor *care trebuie luate de operator* pentru atenuarea riscului.

(3) Atunci când consideră că prelucrarea prevăzută, menționată la alineatul (2), nu ar fi conformă cu prezentul regulament, în special în cazul în care *riscul* nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere, în scris, operatorului de date, într-un interval de cel mult șase săptămâni de la depunerea cererii de consultare, și își poate utiliza oricare dintre competențele menționate la articolul 53 (…). Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute. În cazul în care se aplică prelungirea, operatorul sau persoana împuternicită de operator este informată cu privire la motivele amânării, în termen de o lună de la primirea cererii.

(4) (...)

(5) (...)

(6) Atunci când consultă autoritatea de supraveghere în conformitate cu alineatul (2), operatorul (…) îi furnizează acesteia

(a) dacă este cazul, responsabilitățile 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 persoan**elor** vizate, în conformitate cu prezentul regulament;

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

(e) evaluarea impactului asupra protecției datelor, astfel cum este prevăzută la articolul 33 și

(f) orice (...) altă informație solicitată de autoritatea de supraveghere (...).

(7) Statele membre consultă autoritatea de supraveghere în cadrul procesului de pregătire a unei propuneri de măsură legislativă adoptată de un parlament național sau a unei măsuri de reglementare întemeiate pe o astfel de măsură legislativă care prevede prelucrarea unor date cu caracter personal (...).

(7a) Fără a aduce atingere alineatului (2), legislația statelor membre poate impune operatorilor să se consulte cu autoritatea de supraveghere și să obțină în prealabil autorizare din partea acesteia în legătură cu prelucrarea datelor cu caracter personal de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea unor astfel de date în legătură cu protecția socială și sănătatea publică.

(8) (...)

(9) (...)

SECȚIUNEA 4
RESPONSABILUL CU PROTECȚIA DATELOR

Articolul 35

Desemnarea responsabilului cu protecția datelor

(1) Operatorul sau persoana împuternicită de operator poate să desemneze sau, în cazul în care legislația Uniunii sau a statului membru o impune, trebuie să desemneze un responsabil cu protecția datelor (…).

(2) Un grup de întreprinderi poate numi un responsabil unic cu protecția datelor.

(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) (…).

(5) (…) Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în domeniul legislației și practicilor privind protecția datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la articolul 37, în special în absența oricărui conflict de interese. (…).

(6) (...)

(7) (…). Pe durata mandatului, responsabilul cu protecția datelor poate fi demis doar dacă nu mai întrunește condițiile cerute pentru îndeplinirea sarcinilor sale în temeiul articolului 37, cu excepția cazului în care există motive serioase, în temeiul legislației statului membru în cauză, care să justifice demiterea unui angajat sau a unui funcționar public.

(8) 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.

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

(10) 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.

(11) (...)

Articolul 36

Funcția responsabilului cu protecția datelor

(1) Operatorul sau 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 sau persoana împuternicită de operator sprijină responsabilul cu protecția datelor în îndeplinirea sarcinilor menționate la articolul 37, asigurându-i (...) resursele necesare pentru executarea acestor sarcini, precum și accesul la datele cu caracter personal și la operațiunile de prelucrare.

(3) Operatorul sau persoana împuternicită de operator se asigură că responsabilul cu protecția datelor poate să acționeze în mod independent în ceea ce privește îndeplinirea sarcinilor sale și că nu primește niciun fel de instrucțiuni în această privință. Acesta nu este 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) 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 37

Sarcinile responsabilului cu protecția datelor

(1) (...) Responsabilul cu protecția datelor (…) are următoarele sarcini:

(a) informarea și consilierea operatorului sau a persoanei împuternicite de operator, precum și a angajaților care prelucrează date cu caracter personal, cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții ale Uniunii sau ale statelor membre referitoare la protecția datelor (…);

(b) monitorizarea respectării prezentului regulament, a altor dispoziții ale Uniunii sau ale statelor membre 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) (...)

(d) (...)

(e) (...)

(f) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu articolul 33;

(g) monitorizarea răspunsurilor la cererile adresate de autoritatea de supraveghere și, în limitele competenței responsabilului cu protecția datelor, cooperarea cu autoritatea de supraveghere, la cererea acesteia sau din propria inițiativă a responsabilului cu protecția datelor;

(h) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrarea datelor cu caracter personal, inclusiv consultarea prealabilă menționată la articolul 34, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

(2) (...)

(2a) 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 38

Coduri de conduită

(1) Statele membre, autoritățile de supraveghere, Comitetul european pentru protecția datelor 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 a datelor și de nevoile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii.

(1a) 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 dispozițiilor prezentului regulament, cum ar fi:

(a) prelucrarea datelor în mod echitabil și transparent;

(aa) interesele legitime urmărite de operatori în contexte specifice;

(b) colectarea datelor;

(bb) pseudonimizarea datelor cu caracter personal;

(c) informarea publicului și a persoanelor vizate;

(d) exercitarea drepturilor persoanelor vizate;

(e) informarea și protejarea copiilor și modalitatea de a înregistra consimțământul părintelui sau al tutorelui;

(ee) măsurile și procedurile menționate la articolele 22 și 23 și măsurile de asigurare a securității prelucrării, menționate la articolul 30;

(ef) notificarea autorităților de supraveghere cu privire la încălcările securității datelor cu caracter personal și informarea persoanelor vizate cu privire la aceste încălcări;

(f) (…).

(1ab) La codurile de conduită *aprobate* în temeiul alineatului (2) pot adera nu numai operatorul sau persoana împuternicită de operator care fac obiectul regulamentului, ci și operatorii sau persoanele împuternicite de operatori care nu fac obiectul prezentului regulament în conformitate cu articolul 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 42 alineatul (2) litera (d). Acești operatori sau persoane împuternicite de operatori își asumă angajamente cu caracter obligatoriu și executoriu, prin intermediul unor instrumente contractuale sau al altor tipuri de instrumente, în scopul aplicării garanțiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.

(1b) Codul de conduită cuprinde mecanisme care permit organismului menționat la articolul 38a 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 autorității de supraveghere care este abilitată în temeiul articolului 51 sau 51a.

(2) Asociațiile și alte organisme menționate la alineatul (1a), care intenționează să pregătească un cod de conduită sau să modifice sau să extindă un cod existent, transmit proiectul de cod autorității de supraveghere care este abilitată în temeiul articolului 51. Autoritatea de supraveghere exprimă un aviz cu privire la conformitatea cu prezentul regulament a proiectului de cod sau a codului modificat sau extins și aprobă proiectul de cod sau codul modificat sau extins respectiv în cazul în care constată că acesta oferă garanții adecvate suficiente.

(2a) În cazul în care avizul menționat la alineatul (2) confirmă conformitatea cu prezentul regulament a codului de conduită sau a codului modificat sau extins și codul este aprobat, iar codul de conduită nu are legătură cu activitățile de prelucrare din mai multe state membre, autoritatea de supraveghere înregistrează codul și publică detalii cu privire la acesta.

(2b) În cazul în care proiectul de cod de conduită are legătură cu activitățile de prelucrare din mai multe state membre, autoritatea de supraveghere abilitată în temeiul articolului 51 îl transmite, înainte de aprobare, prin procedura menționată la articolul 57, Comitetului european pentru protecția datelor, care exprimă un aviz cu privire la conformitatea cu prezentul regulament a proiectului de cod sau a codului modificat sau extins sau, în situația menționată la alineatul (1ab), oferă garanții adecvate.

(3) În cazul în care avizul menționat la alineatul (2b) confirmă conformitatea cu prezentul regulament a codului de conduită sau a codului modificat sau extins sau în cazul în care, în situația menționată la alineatul (1ab), codul respectiv oferă garanții adecvate, Comitetul european pentru protecția datelor transmite avizul său Comisiei.

(4) Comisia poate adopta acte de punere în aplicare pentru a decide asupra valabilității generale în Uniune a codurilor de conduită aprobate și a modificărilor sau extinderilor la codurile de conduită aprobate existente care i-au fost prezentate în conformitate cu alineatul (3). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

(5) Comisia asigură publicitatea adecvată pentru codurile aprobate asupra cărora s-a decis că au valabilitate generală în conformitate cu alineatul (4).

(5a) Comitetul european pentru protecția datelor regrupează toate codurile de conduită aprobate și modificările acestora într-un registru și le pune la dispoziția publicului prin orice mijloc corespunzător, cum ar fi portalul european e-justiție.

Articolul 38a

Monitorizarea codurilor de conduită aprobate

(1) Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente în temeiul articolelor 52 și 53, monitorizarea respectării unui cod de conduită în temeiul articolului 38 alineatul (1b) 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 în acest scop 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 soluționarea 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;

(d) demonstrează 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 criterii pentru acreditarea unui organism menționat la alineatul (1) Comitetului european pentru protecția datelor, în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 57.

(4) Fără a aduce atingere dispozițiilor capitolului VIII, un organism menționat la alineatul (1) poate, sub rezerva unor garanții adecvate, să ia măsuri corespunzătoare 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 condițiile pentru acreditare sau măsurile luate de organismul în cauză nu sunt conforme cu prezentul regulament.

(6) Prezentul articol nu se aplică prelucrării datelor cu caracter personal efectuate de autorități și organisme publice.

Articolul 39

Certificare

(1) Statele membre, Comitetul european pentru protecția datelor 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.

(1a) Mecanismele de certificare din domeniul protecției datelor, sigiliile sau mărcile *aprobate* în conformitate cu alineatul (2a) sunt instituite nu numai pentru a fi respectate de operatorii sau de persoanele împuternicite de operatori care fac obiectul prezentului regulament, ele putând fi instituite și pentru a demonstra existența unor garanții adecvate oferite de operatorii sau de persoanele împuternicite de operatori care nu fac obiectul prezentului regulament, în conformitate cu articolul 3, în cadrul transferurilor de date cu caracter personal către țări terțe sau organizații internaționale în condițiile menționate la articolul 42 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 tipuri de instrumente, în scopul aplicării garanțiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.

(2) 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 autorității de supraveghere care este abilitată în temeiul articolului 51 sau 51a.

(2a) *Organismele de certificare menționate la articolul 39a sau, după caz, autoritatea de supraveghere competentă* emite o certificare în conformitate cu prezentul articol, pe baza criteriilor aprobate de către autoritatea de supraveghere competentă sau, *în conformitate cu articolul 57*, de Comitetul european pentru protecția datelor.

(3) Operatorul sau persoana împuternicită de operator care supune activitățile sale de prelucrare mecanismului de certificare oferă organismului de certificare menționat la articolul 39a *sau, după caz, autorității de supraveghere competente*, toate informațiile necesare pentru desfășurarea procedurii de certificare, precum și accesul la activitățile de prelucrare respective.

(4) 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, atât timp cât cerințele relevante sunt îndeplinite în continuare. Aceasta este retrasă de către organismele de certificare menționate la articolul 39a sau, după caz, de către autoritatea de supraveghere competentă în cazul în care nu (mai) sunt îndeplinite cerințele pentru certificare.

(5) Comitetul european pentru protecția datelor regrupează toate mecanismele de certificare și sigiliile de protecție a datelor într-un registru și le pune la dispoziția publicului prin orice mijloc corespunzător, cum ar fi portalul european e-justiție.

Articolul 39a

Organismul de certificare și procedura de certificare

(1) Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente, prevăzute la articolele 52 și 53, certificarea este emisă și reînnoită de un organism de certificare care dispune de un nivel adecvat de competență în domeniul protecției datelor. Fiecare stat membru stabilește dacă aceste organisme de certificare sunt acreditate de către:

(a) autoritatea de supraveghere care este abilitată în temeiul articolului 51 sau 51a; și/sau

(b) organismul național de acreditare numit în conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor în conformitate cu standardul EN-ISO/IEC 17065/2012 și cu cerințele suplimentare stabilite de autoritatea de supraveghere care este abilitată în temeiul articolului 51 sau 51a.

(2) Organismul de certificare menționat la alineatul (1) poate fi acreditat în acest scop numai dacă:

(a) a demonstrat autorității de supraveghere competente, într-un mod satisfăcător, independența și expertiza sa în legătură cu obiectul certificării;

(aa) s-a angajat să respecte criteriile *menționate la articolul 39 alineatul (2a)* și aprobate de autoritatea de supraveghere care este abilitată în temeiul articolului 51 sau 51a sau, în conformitate cu articolul 57, de Comitetul european pentru protecția datelor;

(b) a instituit proceduri pentru emiterea, revizuirea periodică și retragerea sigiliilor și mărcilor de protecție a datelor;

(c) a instituit proceduri și structuri pentru soluționarea 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;

(d) demonstrează 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 alineatul (1) se realizează pe baza criteriilor aprobate de autoritatea de supraveghere care este abilitată în temeiul articolului 51 sau 51a sau, *în conformitate cu articolul 57*, de Comitetul european pentru protecția datelor. *În cazul unei acreditări în conformitate cu alineatul (1) litera (b), aceste cerințe le completează pe cele prevăzute în Regulamentul nr. 765/2008 și normele tehnice care descriu metodele și procedurile organismelor de certificare*.

(4) Organismul de certificare menționat la alineatul (1) este responsabil 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, atât timp cât organismul îndeplinește cerințele.

(5) Organismul de certificare menționat la alineatul (1) transmite autorității de supraveghere competente motivele acordării sau retragerii certificării solicitate.

(6) Cerințe*le* menționate la alineatul (3) și criteriile menționate la articolul 39 alineatul (2a) *se publică de către autoritatea de supraveghere într-o formă ușor de accesat*. Autoritățile de supraveghere transmit, de asemenea, aceste cerințe și criterii Comitetului european pentru protecția datelor. Comitetul european pentru protecția datelor regrupează toate mecanismele de certificare și sigiliile de protecție a datelor într-un registru și le pune la dispoziția publicului prin orice mijloc corespunzător, cum ar fi portalul european e-justiție.

(6a) Fără a aduce atingere dispozițiilor capitolului VIII, autoritatea de supraveghere competentă sau organismul național de acreditare revocă acreditarea acordată unui organism de certificare menționat la alineatul (1) în cazul în care nu (mai) sunt îndeplinite condițiile pentru acreditare sau măsurile luate de organismul în cauză nu sunt conforme cu prezentul regulament.

(7) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 86, în scopul (…) specificării criteriilor și cerințelor care trebuie luate în considerare pentru mecanismele de certificare din domeniul protecției datelor, menționate la alineatul (1) (…).

(7a) Comitetul european pentru protecția datelor emite un aviz către Comisie cu privire la criteriile și cerințele menționate la alineatul (7).

(8) Comisia poate stabili standarde tehnice pentru mecanismele de certificare și pentru sigiliile și mărcile din domeniul protecției datelor, precum și mecanisme de promovare și recunoaștere a mecanismelor de certificare și a sigiliilor și mărcilor din domeniul protecției datelor. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

CAPITOLUL V
TRANSFERUL DATELOR CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Articolul 40

Principiul general al transferurilor

(...)

Articolul 41

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

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

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

(a) statul de drept, respectarea drepturilor omului și a libertăților fundamentale, legislația relevantă (…), atât generală, cât și sectorială, normele de protecție a datelor și măsurile de securitate, inclusiv normele privind transferul ulterior de date cu caracter personal către o altă țară terță sau organizație internațională, care sunt respectate în țara terță respectivă sau în organizația internațională respectivă, precum și existența unor drepturi efective și exercitabile ale persoanelor vizate și a unor căi de atac administrative și judiciare efective pentru persoanele vizate ale căror date cu caracter personal sunt transferate (…);

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

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

(2a) Comitetul european pentru protecția datelor emite un aviz către Comisie pentru evaluarea caracterului adecvat al nivelului de protecție într-o țară terță sau o organizație internațională, inclusiv pentru a determina dacă o țară terță, un teritoriu, o organizație internațională sau un sector specificat nu mai asigură un nivel de protecție adecvat.

(3) Comisia, după ce evaluează caracterul adecvat al nivelului de protecție, poate decide că o țară terță, un teritoriu sau unul sau mai multe sectoare specificate din acea țară terță sau o organizație internațională asigură un nivel de protecție adecvat în sensul alineatului (2). (…). Actul de punere în aplicare menționează aplicarea teritorială și sectorială și, după caz, identifică autoritatea(autoritățile) de supraveghere (independentă/e) menționată/e la alineatul (2) litera (b). Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 87 alineatul (2).

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

(4) (...)

(4a) Comisia monitorizează funcționarea deciziilor adoptate în temeiul alineatului (3) și a deciziilor adoptate în temeiul articolului 25 alineatul (6) sau al articolului 26 alineatul (4) din Directiva 95/46/CE.

(5) Comisia poate decide că o țară terță, un teritoriu sau un sector specificat din acea țară terță sau o organizație internațională nu mai asigură un nivel de protecție adecvat în sensul alineatului (2) și poate, dacă este necesar, să abroge, să modifice sau să suspende decizia respectivă fără efect retroactiv. Actele de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 87 alineatul (2) sau, în cazuri de extremă urgență (…), în conformitate cu procedura menționată la articolul 87 alineatul (3). (...)

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

(6) O decizie luată în temeiul alineatului (5) nu aduce atingere transferurilor de date cu caracter personal către țara terță, teritoriul sau sectorul specificat din acea țară terță sau către organizația internațională în cauză în conformitate cu articolele 42-44.(...)

(7) Comisia publică în *Jurnalul Oficial al Uniunii Europene* o listă a țărilor terțe, a teritoriilor și sectoarelor specificate din țările terțe respective și a organizațiilor internaționale cu privire la care au fost luate decizii în temeiul alineatelor (3), (3a) și (5).

(8) (...)

Articolul 42

Transferuri în baza unor garanții adecvate

(1) În absența unei decizii în temeiul articolului 41 alineatul (3), operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către (…) o țară terță sau o organizație internațională numai dacă operatorul sau persoana împuternicită de operator a oferit garanții adecvate, referitoare și la transferurile ulterioare (…).

(2) Garanțiile adecvate menționate la alineatul 1 *pot* fi furnizate (...), fără să fie nevoie de nicio autorizație specifică din partea unei autorități de supraveghere, prin:

(oa) un instrument cu forță juridică obligatorie și executoriu între autoritățile sau organismele publice; sau

(a) reguli corporatiste obligatorii menționate la articolul 43; sau

(b) clauze standard de protecție a datelor adoptate de Comisie (…) în conformitate cu procedura de examinare menționată la articolul 87 alineatul (2); sau

(c) clauze standard de protecție a datelor adoptate de o autoritate de supraveghere (...) și adoptate de Comisie în conformitate cu procedura de examinare menționată la articolul 87 alineatul (2);

(d) un cod de conduită aprobat în conformitate cu articolul 38, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator (…) din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

(e) un mecanism de certificare aprobat în conformitate cu articolul 39, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator (…) din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

(2a) Sub rezerva autorizării din partea autorității de supraveghere competente, pot fi furnizate și garanțiile adecvate menționate la alineatul (1), în special, prin:

(a) clauze contractuale între operator sau persoana împuternicită de operator și operatorul, persoana împuternicită de operator sau destinatarul datelor (...) din țara terță sau organizația internațională; sau

(b) (...)

(c) (...)

(d) dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice (…).

(3) (...)

(4) (...)

(5) (...)

(5a) Autoritatea de supraveghere aplică mecanismul pentru asigurarea coerenței în cazurile menționate la articolul 57 alineatul (2) literele (ca), (d), (e) și (f).

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

Articolul 43

Regulile corporatiste obligatorii

(1) În conformitate cu mecanismul pentru asigurarea coerenței prevăzut la articolul 57, autoritatea de supraveghere competentă *aprobă reguli corporatiste obligatorii*, cu condiția ca acestea:

(a) să aibă forță juridică obligatorie și să se aplice fiecărui membru vizat al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, precum și să fie puse în aplicare de membrii în cauză;

(b) să confere, în mod expres, drepturi exercitabile persoanelor vizate în ceea ce privește prelucrarea datelor lor cu caracter personal;

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

(2) Regulile corporatiste obligatorii menționate la alineatul (1)precizează cel puțin:

(a) structura și datele de contact ale grupului *în cauză* și ale fiecăruia dintre membrii săi;

(b) transferurile de date sau categoriile de transferuri, inclusiv tipurile de date cu caracter personal, tipul prelucrării și scopurile prelucrării, tipurile de persoane vizate și identificarea țării terțe sau a țărilor terțe în cauză;

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

(d) aplicarea principiilor generale în materie de protecție a datelor, în special limitarea scopului, (...) calitatea datelor, temeiul juridic pentru prelucrare, prelucrarea categoriilor speciale de date cu caracter personal, măsurile de asigurare a securității datelor, precum și cerințele referitoare la transferurile ulterioare către organisme (…) care nu fac obiectul regulilor corporatiste obligatorii;

(e) drepturile persoanelor vizate în ceea ce privește prelucrarea datelor lor cu caracter personal și mijloacele de exercitare a acestor drepturi, inclusiv dreptul de a nu face obiectul unor decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, în conformitate cu articolul 20, dreptul de a depune o plângere în fața autorității de supraveghere competente și în fața instanțelor competente ale statelor membre, în conformitate cu articolul 75, precum și dreptul de a obține despăgubiri și, după caz, compensații pentru încălcarea regulilor corporatiste obligatorii;

(f) acceptarea de către operator sau de persoana împuternicită de operator, care își are sediul pe teritoriul unui stat membru, a răspunderii pentru orice încălcare a regulilor corporatiste obligatorii de către orice membru în cauză care nu își are sediul în Uniune; operatorul sau persoana împuternicită de operator poate fi exonerat(ă) de această răspundere, integral sau parțial, numai atunci când dovedește că membrul respectiv nu a fost răspunzător de evenimentul care a cauzat daune;

(g) modul în care informațiile privind regulile corporatiste obligatorii, în special privind dispozițiile menționate la literele (d), (e) și (f) de la prezentul alineat, sunt furnizate persoanelor vizate în conformitate cu articolele 14 și 14a;

(h) sarcinile oricărui responsabil cu protecția datelor desemnat în conformitate cu articolul 35 sau ale oricărei alte persoane sau entități însărcinate cu monitorizarea (...) respectării regulilor corporatiste obligatorii în cadrul grupului, a activităților de formare și a gestionării plângerilor;

(hh) procedurile de formulare a plângerilor;

(i) mecanismele din cadrul grupului menite să asigure verificarea conformității cu regulile corporatiste obligatorii. Aceste mecanisme includ auditurile privind protecția datelor și metodele de asigurare a acțiunilor corective menite să protejeze drepturile persoanei vizate. Rezultatele acestor verificări ar trebui să fie comunicate persoanei sau entității menționate la litera (h) și consiliului întreprinderii care exercită controlul sau al grupului de întreprinderi și ar trebui să fie puse la dispoziția autorității de supraveghere competente, la cerere;

(j) mecanismele de raportare și înregistrare a modificărilor aduse regulilor și de raportare a acestor modificări autorității de supraveghere;

(k) mecanismul de cooperare cu autoritatea de supraveghere în vederea asigurării respectării regulilor de către orice membru al grupului (…), în special prin punerea la dispoziția autorității de supraveghere a rezultatelor (…) verificărilor cu privire la măsurile menționate la punctul (i) de la prezentul alineat;

(l) mecanismele de raportare către autoritatea de supraveghere competentă a oricăror cerințe legale impuse unui membru al grupului într-o țară terță care pot avea un efect advers considerabil asupra garanțiilor furnizate prin regulile corporatiste obligatorii; și

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

(2a) Comitetul european pentru protecția datelor oferă consultanță Comisiei cu privire la formatul și procedurile pentru schimbul de informații între operatori, persoanele împuternicite de operatori și autoritățile de supraveghere pentru regulile corporative obligatorii.

(3) (...)

(4) Comisia poate preciza formatul și procedurile pentru schimbul de informații (...) între operatori, persoanele împuternicite de operatori și autoritățile de supraveghere pentru regulile corporatiste obligatorii în sensul prezentului articol. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare prevăzută la articolul 87 alineatul (2).

Articolul 44

Derogări pentru situații specifice

(1) În absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 41 alineatul (3) sau a unor garanții adecvate în conformitate cu articolul 42, inclusiv a regulilor corporatiste obligatorii (...), un transfer sau o categorie de transferuri de date cu caracter personal către (...) o țară terță sau o organizație internațională poate avea loc numai în condițiile în care:

(a) persoana vizată și-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a fost informată că astfel de transferuri pot implica *riscuri* pentru persoanele vizate în lipsa unei decizii privind caracterul adecvat al nivelului de protecție și a unor garanții adecvate; sau

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

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

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

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

(f) transferul este necesar pentru protejarea interesului vital al persoanei vizate sau al altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul; sau

(g) transferul se realizează dintr-un registru care, potrivit legislației Uniunii sau a statului membru, are scopul de a furniza informații publicului și care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în măsura în care sunt îndeplinite condițiile cu privire la consultare prevăzute de legislația Uniunii sau a statului membru în acel caz specific; sau

(h) transferul, *care* nu este la scară largă și nici *frecvent*, este necesar în contextul intereselor legitime urmărite de operator asupra cărora nu prevalează interesele sau drepturile și libertățile persoanei vizate și atunci când operatorul (…) a evaluat toate circumstanțele aferente operațiunii de transfer de date sau seriei de operațiuni de transfer de date și (…), în baza acestei evaluări, a oferit garanții adecvate cu privire la protecția datelor cu caracter personal.

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

(3) (...)

(4) Literele(a), (b), (c) și (h) ale alineatului (1) nu se aplică în cazul activităților desfășurate de autoritățile publice în exercitarea competențelor lor publice..

(5) Interesul public prevăzut la alineatul (1) litera (d) trebuie să fie recunoscut în dreptul Uniunii sau în dreptul intern al statului membru sub incidența căruia intră operatorul. **(...)**

(5a) În absența unei decizii privind caracterul adecvat al nivelului de protecție, dreptul Uniunii sau legislația unui stat membru poate, din considerente importante de interes public, stabili în mod expres limite asupra transferului unor categorii specifice de date cu caracter personal către o țară terță sau o organizație internațională. Statele membre notifică aceste dispoziții Comisiei.

(6) Operatorul sau persoana împuternicită de operator consemnează evaluarea, precum și garanțiile adecvate (…) prevăzute la alineatul (1) litera (h), în evidențele menționate la articolul 28 (…).

(6a) (...)

(7) (...)

Articolul 45

Cooperarea internațională în domeniul protecției datelor cu caracter personal

(1) În ceea ce privește țările terțe și organizațiile internaționale, Comisia și autoritățile de supraveghere iau măsurile corespunzătoare pentru:

(a) elaborarea de mecanisme de cooperare internațională pentru a facilita asigurarea aplicării *efective* a legislației privind protecția datelor cu caracter personal;

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

(c) implicarea părților interesate relevante în discuțiile și activitățile care au ca scop promovarea cooperării internaționale în domeniul aplicării legislației privind protecția datelor cu caracter personal;

(d) promovarea schimbului reciproc și a documentației cu privire la legislația și practicile în materie de protecție a datelor cu caracter personal.

(2) (...)

CAPITOLUL VI
AUTORITĂȚI DE SUPRAVEGHERE INDEPENDENTE

SECȚIUNEA 1

STATUTUL INDEPENDENT

Articolul 46

Autoritatea de supraveghere

(1) Fiecare stat membru prevede ca una sau mai multe autorități publice independente să fie responsabile cu monitorizarea aplicării prezentului regulament.

(1a) Fiecare autoritate de supraveghere contribuie la aplicarea consecventă a prezentului regulament în întreaga Uniune (…). În acest scop, autoritățile de supraveghere cooperează atât între ele, cât și cu Comisia, în conformitate cu capitolul VII.

(2) În cazul în care un stat membru instituie mai multe autorități de supraveghere, acesta desemnează autoritatea de supraveghere care reprezintă autoritățile respective în cadrul Comitetului european pentru protecția datelor și instituie un sistem prin care să asigure respectarea de către celelalte autorități a normelor privind mecanismul pentru asigurarea coerenței prevăzut la articolul 57.

(3) Fiecare stat membru notifică Comisiei dispozițiile din legislația sa pe care le adoptă în temeiul prezentului capitol până cel târziu la data menționată la articolul 91 alineatul (2) și, fără întârziere, orice modificare ulterioară pe care o aduce acestor dispoziții.

Articolul 47

Independență

(1) Fiecare autoritate de supraveghere beneficiază de independență deplină în îndeplinirea atribuțiilor și *exercitarea* competențelor care îi sunt încredințate în conformitate cu prezentul regulament.

(2) Membrul sau membrii fiecărei autorități de supraveghere, în cadrul îndeplinirii atribuțiilor și al exercitării competențelor sale (lor) în conformitate cu prezentul regulament, rămâne (rămân) independent (independenți) de orice influență externă directă sau indirectă și nici nu solicită, nici nu acceptă instrucțiuni de la o parte externă.

(3) (...)

(4) (...)

(5) Fiecare stat membru se asigură că fiecare autoritate de supraveghere beneficiază de resurse umane, tehnice și financiare (…), de un sediu și de infrastructura necesară pentru îndeplinirea atribuțiilor și exercitarea competențelor sale în mod eficace, inclusiv a celor care urmează să fie aplicate în contextul asistenței reciproce, al cooperării și al participării în cadrul Comitetului european pentru protecția datelor.

(6) Fiecare stat membru se asigură că fiecare autoritate de supraveghere dispune de personal propriu, (…) care se află sub conducerea membrului sau membrilor autorității de supraveghere.

(7) Statele membre se asigură că fiecare autoritate de supraveghere face obiectul unui control financiar care nu aduce atingere independenței sale. Statele membre se asigură că fiecare autoritate de supraveghere dispune de bugete anuale distincte, publice, care pot face parte din bugetul general de stat sau național.

Articolul 48

Condiții generale aplicabile membrilor autorității de supraveghere

(1) Statele membre stabilesc dispoziții potrivit cărora membrul sau membrii fiecărei autorități de supraveghere trebuie numit (numiți) (...) de parlament și/sau de guvern sau de șeful statului membru în cauză sau de un organism independent împuternicit prin legislația statului membru să facă numirea prin intermediul unei proceduri transparente.

(2) Membrul sau membrii în cauză dispun(e) de calificările, experiența și competențele necesare pentru îndeplinirea atribuțiilor și exercitarea competențelor sale (lor).

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

(4) (...)

(5) (…).

Articolul 49

Norme privind instituirea autorității de supraveghere

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

(a) instituirea (…) fiecărei autorități de supraveghere;
(b) calificările (...) necesare pentru exercitarea funcției de membru al autorității de supraveghere;
(c) normele și procedurile pentru numirea membrului sau membrilor fiecărei autorități de supraveghere (…);
(d) durata mandatului membrului sau membrilor fiecărei autorități de supraveghere, care nu este (…) mai mică de patru ani, cu excepția primului mandat după intrarea în vigoare a prezentului regulament, din care o parte poate fi pe o perioadă mai scurtă în cazul în care acest lucru este necesar pentru a proteja independența autorității de supraveghere printr-o procedură de numiri eșalonate;
(e) dacă și de câte ori este eligibil pentru reînnoire mandatul membrului sau membrilor fiecărei autorități de supraveghere;
(f) (…) condițiile care reglementează obligațiile membrului sau membrilor și ale personalului fiecărei autorități de supraveghere, interdicții privind acțiunile și ocupațiile incompatibile cu acestea în cursul mandatului și după încetarea acestuia, precum și normele care reglementează încetarea contractului de angajare;
(g) (…).

(2) Membrul sau membrii și personalul fiecărei autorități de supraveghere au obligația, în conformitate cu legislația Uniunii sau a statului membru, de a respecta *atât pe parcursul mandatului, cât și după încetarea acestuia,* secretul profesional în ceea ce privește informațiile confidențiale de care au luat cunoștință în cursul îndeplinirii atribuțiilor (…) sau al exercitării competențelor lor.

Articolul 50

Secretul profesional

(...)

SECȚIUNEA 2

ABILITĂRI, SARCINI ȘI COMPETENȚE

Articolul 51

Abilitări

(1) Fiecare autoritate de supraveghere este abilitată să îndeplinească sarcinile și să exercite competențele care îi sunt conferite în conformitate cu prezentul regulament pe teritoriul statului membru de care aparține. (...)

(2) În cazul în care prelucrarea este efectuată de autorități publice sau de organisme private care acționează pe baza literei (c) sau (e) de la articolul 6 alineatul (1), este abilitată autoritatea de supraveghere din statul membru respectiv. În astfel de cazuri, nu se aplică articolul 51a.

(3) Autoritățile de supraveghere nu sunt abilitate să supravegheze operațiunile de prelucrare ale instanțelor care acționează în exercițiul funcției lor judiciare. (…).

Articolul 51a

Abilitările autorității de supraveghere principale

(1) Fără a aduce atingere articolului 51, autoritatea de supraveghere a sediului principal sau a sediului unic al operatorului sau al persoanei împuternicite de operator este abilitată să acționeze în calitate de autoritate de supraveghere principală pentru prelucrarea transnațională efectuată de operatorul sau persoana împuternicită în cauză în conformitate cu procedura prevăzută la articolul 54a.

(2) (...)

(2a) Prin derogare de la alineatul (1), fiecare autoritate de supraveghere este abilitată să trateze o plângere depusă în atenția sa sau o eventuală încălcare a prezentului regulament, în cazul în care obiectul acesteia se referă numai la un sediu aflat în statul său membru sau afectează în mod semnificativ persoane vizate numai în statul său membru.

(2b) În cazurile menționate la alineatul (2a), autoritatea de supraveghere informează fără întârziere autoritatea de supraveghere principală cu privire la această chestiune. În termen de trei săptămâni de la momentul informării, autoritatea de supraveghere principală decide dacă tratează sau nu cazul respectiv în conformitate cu procedura prevăzută la articolul 54a, luând în considerare dacă există sau nu un sediu al operatorului sau al persoanei împuternicite de operator pe teritoriul statului membru a cărui autoritate de supraveghere a informat-o.

(2c) În cazul în care autoritatea de supraveghere principală decide să trateze cazul, se aplică procedura prevăzută la articolul 54a. Autoritatea de supraveghere care a informat autoritatea de supraveghere principală poate înainta un proiect de decizie acesteia din urmă. Autoritatea de supraveghere principală ține seama în cea mai mare măsură posibilă de proiectul respectiv atunci când pregătește proiectul de decizie prevăzut la articolul 54a alineatul (2).

(2d) În cazul în care autoritatea de supraveghere principală decide să nu se ocupe de acesta, autoritatea de supraveghere care a informat autoritatea de supraveghere principală tratează cazul în conformitate cu articolele 55 și 56.

(3) Autoritatea de supraveghere principală este singurul interlocutor al operatorului sau al persoanei împuternicite de operator în ceea ce privește activitatea transnațională a acestuia (acesteia) de prelucrare.

(4) (…).

Articolul 51b

Identificarea autorității de supraveghere competente pentru sediul principal

(...)

Articolul 51c

Registrul ghișeului unic

(...)

Articolul 52

Sarcini

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

(a) monitorizează și asigură aplicarea prezentului regulament;

(aa) promovează acțiuni de sensibilizare și de înțelegere în rândul publicului a riscurilor, normelor, garanțiilor și drepturilor în materie de prelucrare a datelor cu caracter personal. Se acordă atenție specială activităților care se adresează în mod specific copiilor;

(ab) oferă consiliere, în conformitate cu legislația națională, parlamentului național, guvernului și altor instituții și organisme cu privire la măsurile legislative și administrative referitoare la protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal;

(ac) promovează acțiuni de sensibilizare a operatorilor și a persoanelor împuternicite de aceștia cu privire la obligațiile care le revin în temeiul prezentului regulament;

(ad) la cerere, furnizează informații oricărei persoane vizate în legătură cu exercitarea drepturilor sale în conformitate cu prezentul regulament și, dacă este cazul, cooperează cu autoritățile de supraveghere din alte state membre în acest scop;

(b) tratează plângerile depuse de o persoană vizată, un organism, o organizație sau o asociație care reprezintă o persoană vizată, în conformitate cu articolul 73, investighează într-o măsură adecvată obiectul plângerii și informează persoana vizată sau organismul, organizația sau asociația în cauză cu privire la evoluția și rezultatul investigației, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigații mai amănunțite sau coordonarea cu o altă autoritate de supraveghere;

(c) cooperează, inclusiv prin schimb de informații, cu alte autorități de supraveghere și își oferă asistență reciprocă pentru a asigura consecvența aplicării și respectării prezentului regulament;

(d) desfășoară investigații privind aplicarea prezentului regulament, inclusiv pe baza unor informații primite de la o altă autoritate de supraveghere sau autoritate publică;

(e) monitorizează evoluțiile relevante, în măsura în care acestea au impact asupra protecției datelor cu caracter personal, în special evoluția tehnologiilor informației și comunicațiilor și a practicilor comerciale;

(f) adoptă clauze contractuale standard în conformitate cu articolul 26 alineatul (2c);

(fa) decide și întocmește o listă în legătură cu cerința privind evaluarea impactului asupra protecției datelor, în conformitate cu articolul 33 alineatul (2a);

(g) oferă consiliere cu privire la operațiunile de prelucrare menționate la articolul 34 alineatul (3);

(ga) încurajează elaborarea de coduri de conduită în conformitate cu articolul 38, își dă avizul cu privire la acestea și le aprobă pe cele care oferă suficiente garanții, în conformitate cu articolul 38 alineatul (2);

(gb) promovează stabilirea unor mecanisme de certificare, precum și a unor sigilii și mărci în domeniul protecției datelor și aprobă criteriile de certificare în conformitate cu articolul 39 alineatul (2a)**;**

(gc) acolo unde este cazul, efectuează o revizuire periodică a certificărilor acordate, în conformitate cu articolul 39 alineatul (4);

(h) elaborează și publică criteriile de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu articolul 38a și a unui organism de certificare în conformitate cu articolul 39a;

(ha) coordonează procedura de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu articolul 38a și a unui organism de certificare în conformitate cu articolul 39a;

(hb) autorizează clauzele contractuale menționate la articolul 42 alineatul (2a) litera (a);

(i) aprobă regulile corporatiste obligatorii în conformitate cu articolul 43;

(j) contribuie la activitățile Comitetului european pentru protecția datelor;

(k) îndeplinește orice alte sarcini legate de protecția datelor cu caracter personal.

(2) (...)

(3) (…).

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

(5) Îndeplinirea sarcinilor fiecărei autorități de supraveghere este gratuită pentru persoana vizată și pentru responsabilul cu protecția datelor, dacă acesta există.

(6) În cazul în care cererile sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, autoritatea de supraveghere poate refuza să le trateze. Sarcina de a demonstra caracterul evident nefondat sau excesiv al cererii revine autorității de supraveghere.

Articolul 53

Competențe

(1) Fiecare stat membru adoptă dispoziții legislative care conferă autorității sale de supraveghere cel puțin următoarele competențe de investigare:

(a) de a da dispoziții operatorului și persoanei împuternicite de operator și, după caz, reprezentantului operatorului să furnizeze orice informații pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale;

(aa) de a efectua investigații sub formă de audituri privind protecția datelor;

(ab) de a efectua o revizuire a certificărilor acordate în temeiul articolului 39 alineatul (4);

(b) (...)

(c) (...)

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

(da) de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale;

(db) de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor, în conformitate cu dreptul Uniunii sau cu dreptul procedural al statului membru.

(1a) (…).

(1b) Fiecare stat membru adoptă dispoziții legislative care conferă autorității sale de supraveghere următoarele competențe de corectare:

(a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la posibilitatea ca operațiunile de prelucrare prevăzute să încalce dispozițiile prezentului regulament;

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

(c) (…).

(ca) de a da dispoziții operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-și exercita drepturile în temeiul prezentului regulament;

(d) de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile prezentului regulament, acolo unde este cazul, specificând modalitatea și termenul-limită, în special prin impunerea rectificării, restricționării sau ștergerii datelor în conformitate cu articolele 16, 17 și 17a, precum și a notificării acestor acțiuni destinatarilor cărora le-au fost dezvăluite datele, în conformitate cu articolul 17 alineatul (2a) și articolul 17b;

(e) de a impune o limitare temporară sau definitivă asupra prelucrării (…);

(f) de a dispune suspendarea fluxurilor de date către un destinatar dintr-o țară terță sau către o organizație internațională;

(g) de a impune amenzi administrative în conformitate cu articolele 79 și 79a, în completarea sau în locul măsurilor menționate la prezentul alineat, în funcție de circumstanțele fiecărui caz în parte.

(1c) Fiecare stat membru adoptă dispoziții legislative care conferă autorității sale de supraveghere următoarele competențe de autorizare și consiliere:

(a) de a oferi consiliere operatorului în conformitate cu procedura de consultare prealabilă menționată la articolul 34;

(aa) de a emite avize, din proprie inițiativă sau la cerere, parlamentului național, guvernului statului membru sau, în conformitate cu legislația națională, altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal;

(ab) de a autoriza prelucrarea menționată la articolul 34 alineatul (7a), în cazul în care legislația statului membru prevede o astfel de autorizare prealabilă;

(ac) de a emite un aviz și de a aproba proiectele de coduri de conduită, în conformitate cu articolul 38 alineatul (2);

(ad) de a acredita organisme de certificare în conformitate cu articolul 39a;

(ae) de a emite certificări și de a aproba criterii de certificare în conformitate cu articolul 39 alineatul (2a);

(b) de a adopta clauze standard în materie de protecție a datelor, menționate la articolul 42 alineatul (2) litera (c);

(c) de a autoriza clauze contractuale menționate la articolul 42 alineatul (2a) litera (a);

(ca) de a autoriza acorduri administrative menționate la articolul 42 alineatul (2a) litera (d);

(d) de a aproba reguli corporatiste obligatorii în conformitate cu articolul 43.

(2) *Exercitarea competențelor conferite autorității de supraveghere în temeiul prezentului articol face obiectul unor garanții adecvate, inclusiv căi de atac judiciare eficace și procese echitabile, prevăzute în dreptul Uniunii și al statelor membre în conformitate cu Carta drepturilor fundamentale a Uniunii Europene.*

(3) Fiecare stat membru prevede, pe cale legislativă, faptul că autoritatea sa de supraveghere are competența de a aduce în atenția autorităților judiciare cazurile de încălcare a prezentului regulament și (...), după caz, de a iniția sau de a se implica într-un alt mod în proceduri judiciare, în scopul de a asigura aplicarea dispozițiilor prezentului regulament.

(4) (...)

(5) (...)

Articolul 54

Raport de activitate

Fiecare autoritate de supraveghere întocmește un raport anual cu privire la activitățile sale. Raportul se transmite parlamentului național, guvernului și altor autorități desemnate de legislația națională. Acesta se pune la dispoziția publicului, a Comisiei Europene și a Comitetului european pentru protecția datelor.

CAPITOLUL VII

COOPERARE ȘI COERENȚĂ

SECȚIUNEA 1

COOPERARE

Articolul 54a

Cooperarea dintre autoritatea de supraveghere principală și alte autorități de supraveghere vizate

(1) Autoritatea de supraveghere principală (...) cooperează cu celelalte autorități de supraveghere vizate, în conformitate cu prezentul articol, în încercarea de a ajunge la un consens (...). Autoritatea de supraveghere principală și autoritățile de supraveghere vizate își comunică reciproc toate informațiile relevante.

(1a) Autoritatea de supraveghere principală poate solicita în orice moment altor autorități de supraveghere vizate să ofere asistență reciprocă în temeiul articolului 55 și poate desfășura operațiuni comune în temeiul articolului 56, în special în vederea efectuării de investigații sau a monitorizării punerii în aplicare a unei măsuri referitoare la un operator sau o persoană împuternicită de operator, stabilit(ă) în alt stat membru.

(2) Autoritatea de supraveghere principală comunică fără întârziere informațiile relevante referitoare la această chestiune celorlalte autorități de supraveghere vizate. Autoritatea de supraveghere principală transmite fără întârziere un proiect de decizie celorlalte autorități de supraveghere vizate, pentru a obține avizul lor, și ține seama în mod corespunzător de opiniile acestora.

(3) În cazul în care oricare dintre celelalte autorități de supraveghere vizate exprimă, în termen de patru săptămâni după ce a fost consultată în conformitate cu alineatul (2), o obiecție relevantă și motivată *la proiectul de decizie*, autoritatea de supraveghere principală, în cazul în care nu dă curs obiecției sau consideră că aceasta nu este relevantă și motivată, sesizează mecanismul pentru asigurarea coerenței menționat la articolul 57. (...)

(3a) În cazul în care intenționează să dea curs obiecției formulate, autoritatea de supraveghere principală transmite celorlalte autorități de supraveghere vizate un proiect revizuit de decizie pentru a obține avizul acestora. Acest proiect revizuit de decizie face obiectul procedurii menționate la alineatul (3) pe parcursul unei perioade de două săptămâni.

(4) În cazul în care niciuna dintre celelalte autorități de supraveghere vizate nu a formulat obiecții la proiectul de decizie transmis de autoritatea de supraveghere principală în termenul menționat la alineatele (3) și (3a), se consideră că autoritatea de supraveghere principală și autoritățile de supraveghere vizate sunt de acord cu proiectul de decizie respectiv, care devine obligatoriu pentru acestea.

(4a) Autoritatea de supraveghere principală adoptă decizia și o notifică sediului principal sau sediului unic al operatorului sau al persoanei împuternicite de operator, după caz, și informează celelalte autorități de supraveghere vizate și Comitetul european pentru protecția datelor cu privire la decizia în cauză, incluzând un rezumat al elementelor și motivelor relevante. Autoritatea de supraveghere la care a fost depusă plângerea informează reclamantul cu privire la decizie.

(4b) Prin derogare de la alineatul (4a), în cazul în care o plângere este refuzată sau respinsă, autoritatea de supraveghere la care s-a depus plângerea adoptă decizia, o notifică reclamantului și informează operatorul cu privire la acest lucru.

(4bb) În cazul în care autoritatea de supraveghere principală și autoritățile de supraveghere vizate sunt de acord să refuze sau să respingă anumite părți ale unei plângeri și să dea curs altor părți ale plângerii respective, se adoptă o decizie separată pentru fiecare dintre aceste părți. Autoritatea de supraveghere principală adoptă decizia pentru partea care vizează acțiunile referitoare la operator, o notifică sediului principal sau sediului unic al operatorului sau al persoanei împuternicite de operator de pe teritoriul statului membru în cauză și informează reclamantul cu privire la acest lucru, în timp ce autoritatea de supraveghere a reclamantului adoptă decizia pentru partea care vizează refuzarea sau respingerea plângerii respective, o notifică reclamantului și informează operatorul sau persoana împuternicită de operator cu privire la acest lucru.

(4c) În urma notificării deciziei autorității de supraveghere principale în temeiul alineatelor (4a) și (4bb), operatorul sau persoana împuternicită de operator ia măsurile necesare pentru a se asigura că activitățile de prelucrare sunt în conformitate cu decizia în toate sediile sale din Uniune. Operatorul sau persoana împuternicită de operator notifică măsurile luate în vederea respectării deciziei autorității de supraveghere principale, care informează celelalte autorități de supraveghere vizate.

(4d) În cazul în care, în circumstanțe excepționale, o autoritate de supraveghere vizată are motive să considere că există o nevoie urgentă de a acționa în vederea protejării intereselor persoanelor vizate, se aplică procedura de urgență prevăzută la articolul 61.

(5) Autoritatea de supraveghere principală și celelalte autorități de supraveghere vizate își furnizează reciproc informațiile solicitate în temeiul prezentului articol (...), prin mijloace electronice, utilizând un formular standard.

Articolul 54b

Cooperarea dintre autoritatea de supraveghere principală și celelalte autorități de supraveghere vizate în cazuri individuale privind o posibilă nerespectare a regulamentului

(...)

Articolul 55

Asistență reciprocă

(1) Autoritățile de supraveghere își furnizează reciproc informații relevante și asistență pentru a pune în aplicare prezentul regulament în mod coerent și instituie măsuri de cooperare eficace între ele. Asistența reciprocă se referă, în special, la cereri de informații și măsuri de supraveghere, cum ar fi cereri privind autorizări și consultări prealabile, inspecții și investigații. (…)

(2) Fiecare autoritate de supraveghere ia toate măsurile corespunzătoare necesare pentru a răspunde cererii unei alte autorități de supraveghere, fără întârzieri nejustificate și cel târziu în termen de o lună de la data primirii cererii. Aceste măsuri pot include, în special, transmiterea informațiilor relevante privind desfășurarea unei investigații (...).

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

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

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

(b) a da curs cererii ar contraveni dispozițiilor prezentului regulament sau legislației Uniunii sau a unui stat membru sub incidența căreia intră autoritatea de supraveghere care a primit cererea.

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

(6) Ca regulă, autoritățile de supraveghere furnizează informațiile solicitate de alte autorități de supraveghere prin mijloace electronice, utilizând un formular standard.

(7) Pentru acțiunile întreprinse în urma unei cereri de asistență reciprocă nu se percepe nicio taxă. Autoritățile de supraveghere pot conveni împreună cu alte autorități de supraveghere asupra unor norme privind compensațiile din partea acestor alte autorități de supraveghere în cazul unor cheltuieli specifice rezultate în urma acordării de asistență reciprocă în situații excepționale.

(8) În cazul în care o autoritate de supraveghere nu furnizează informațiile menționate la alineatul (5) în termen de o lună de la primirea cererii din partea altei autorități de supraveghere, aceasta din urmă poate adopta o măsură provizorie pe teritoriul propriului stat membru, în conformitate cu articolul 51 alineatul (1), și sesizează Comitetul european pentru protecția datelor (...) în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 57.

(9) Autoritatea de supraveghere precizează perioada de valabilitate a măsurii provizorii respective, care nu depășește trei luni. Autoritatea de supraveghere comunică fără întârziere această măsură, precum și motivele adoptării sale, Comitetului european pentru protecția datelor (…), în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 57.

(10) Comisia poate specifica forma și procedurile pentru asistența reciprocă menționată în prezentul articol, precum și modalitățile de schimb de informații prin mijloace electronice între autoritățile de supraveghere și între autoritățile de supraveghere și Comitetul european pentru protecția datelor, în special formularul standard menționat la alineatul (6). Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 87 alineatul (2).

Articolul 56

Operațiuni comune ale autorităților de supraveghere

(1) Autoritățile de supraveghere pot, după caz, să desfășoare operațiuni comune, inclusiv investigații comune și măsuri comune de aplicare a legii, în care sunt implicați membri sau personal din partea autorităților de supraveghere ale altor state membre.

(2) În cazul în care operatorul sau persoana împuternicită de operator deține sedii în mai multe state membre sau dacă un număr semnificativ de persoane vizate din mai multe state membre sunt susceptibile de a fi afectate în mod semnificativ de operațiuni de prelucrare, o autoritate de supraveghere din fiecare dintre statele membre respective are dreptul de a participa la operațiunile comune, după caz. Autoritatea de supraveghere competentă invită autoritățile de supraveghere din fiecare dintre aceste state membre să ia parte la operațiunile comune respective și răspunde fără întârziere la cererea de participare a unei autorități de supraveghere.

(3) O autoritate de supraveghere poate, în conformitate cu legislația propriului stat membru și cu acordul autorității de supraveghere din statul membru de origine, să acorde competențe, inclusiv competențe de investigare, membrilor sau personalului autorității de supraveghere din statul membru de origine implicați în operațiuni comune sau, în măsura în care legislația statului membru al autorității de supraveghere din statul membru de primire permite acest lucru, poate autoriza membrii sau personalul autorității de supraveghere din statul membru de origine să își exercite competențele de investigare în conformitate cu legislația statului membru al acestei din urmă autorități. Astfel de competențe de investigare pot fi exercitate doar sub coordonarea și în prezența membrilor sau personalului autorității de supraveghere din statul membru de primire. Membrii sau personalul autorității de supraveghere din statul membru de origine sunt supuși legislației naționale a autorității de supraveghere din statul membru de primire. (...)

(3a) În cazul în care, în conformitate cu alineatul (1), personalul unei autorități de supraveghere din statul membru de origine își desfășoară activitatea într-un alt stat membru, statul membru de primire este răspunzător pentru eventualele daune cauzate de membrii personalului respectiv în cursul operațiunilor acestuia, în conformitate cu legislația statului membru pe teritoriul căruia își desfășoară operațiunile.

(3b) Statul membru pe teritoriul căruia s-au produs daunele repară aceste daune în condițiile aplicabile daunelor cauzate de propriul său personal. Statul membru de origine al autorității de supraveghere al cărei personal a cauzat daune unei persoane de pe teritoriul unui alt stat membru rambursează acestuia din urmă totalitatea sumelor pe care le-a plătit persoanelor îndreptățite în numele acestora.

(3c) Fără a aduce atingere exercitării drepturilor sale față de terțe părți și cu excepția alineatului (3b), fiecare stat membru se abține, în cazul prevăzut la alineatul (1), de la a pretinde de la un alt stat membru rambursarea despăgubirilor pentru daunele suferite.

(4) (...)

(5) În cazul în care este planificată o operațiune comună, iar o autoritate de supraveghere nu se conformează, în termen de o lună, obligației prevăzute la alineatul (2) a doua teză, celelalte autorități de supraveghere pot adopta o măsură provizorie pe teritoriul statului membru al respectivei autorități, în conformitate cu articolul 51 alineatul (1).

(6) Autoritatea de supraveghere precizează perioada de valabilitate a măsurii provizorii menționate la alineatul (5), care nu depășește trei luni. Autoritatea de supraveghere comunică fără întârziere această măsură, precum și motivele adoptării sale, Comitetului european pentru protecția datelor (…), în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 57.

SECȚIUNEA 2

ASIGURAREA COERENȚEI

Articolul 57

Mecanismul pentru asigurarea coerenței

(1) Pentru scopul stabilit la articolul 46 alineatul (1a), autoritățile de supraveghere cooperează între ele prin mecanismul pentru asigurarea coerenței, astfel cum se prevede în prezenta secțiune.

(2) Comitetul european pentru protecția datelor emite un aviz de fiecare dată când o *autoritate de supraveghere* competentă intenționează *să adopte* oricare dintre măsurile de mai jos (...). În acest scop, autoritatea de supraveghere competentă comunică proiectul de decizie Comitetului european pentru protecția datelor, atunci când:

(a) (…).

(b) (…).

(c) vizează adoptarea unei liste de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor, în conformitate cu articolul 33 alineatul (2a); sau

(ca) în conformitate cu articolul 38 alineatul (2b), se referă la conformitatea cu prezentul regulament a unui proiect de cod de conduită sau a unei modificări sau extinderi a unui cod de conduită; sau

(cb) vizează aprobarea criteriilor pentru acreditarea unui organism în conformitate cu articolul 38a alineatul (3) sau a unui organism de certificare în conformitate cu (...) articolul 39a alineatul (3);

(d) vizează determinarea clauzelor standard în materie de protecție a datelor menționate la articolul 42 alineatul (2) litera (c);

sau

(e) vizează autorizarea clauzelor contractuale menționate la articolul 42 alineatul (2) litera (d);

sau

(f) vizează aprobarea regulilor corporatiste obligatorii în sensul articolului 43.

(3) Comitetul european pentru protecția datelor adoptă o decizie obligatorie în următoarele cazuri:

a) Atunci când, în unul dintre cazurile menționate la articolul 54a alineatul (3), o autoritate de supraveghere *vizată* a exprimat o obiecție relevantă şi motivată la un proiect de decizie a autorităţii principale sau autoritatea principală a respins obiecția ca nefiind relevantă şi/sau motivată. Decizia obligatorie se referă la toate chestiunile vizate de obiecția relevantă şi motivată, în special la chestiunea privind stabilirea încălcării regulamentului;

b) În cazul în care există opinii divergente cu privire la care dintre autoritățile de supraveghere *vizate* deține competența pentru sediul principal;

c) (...)

d) În cazul în care o autoritate de supraveghere competentă nu solicită avizul Comitetului european pentru protecția datelor în cazurile menționate la alineatul (2) de la prezentul articol sau nu ține seama de avizul Comitetului european pentru protecția datelor emis în conformitate cu articolul 58. În acest caz, orice autoritate de supraveghere vizată sau Comisia poate comunica chestiunea Comitetului european pentru protecția datelor.

(4) Orice autoritate de supraveghere, președintele Comitetului european pentru protecția datelor sau Comisia poate solicita ca orice chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru să fie examinată de Comitetul european pentru protecția datelor în vederea obținerii unui aviz, în special în cazul în care o autoritate de supraveghere competentă nu respectă obligațiile privind asistența reciprocă în conformitate cu articolul 55 sau privind operațiunile comune în conformitate cu articolul 56.

(5) Autoritățile de supraveghere și Comisia comunică electronic Comitetului european pentru protecția datelor, printr-un formular standard, orice informație relevantă, inclusiv, după caz, o sinteză a faptelor, proiectul de decizie, motivele care fac necesară adoptarea unei astfel de măsuri, precum și opiniile altor autorități de supraveghere *vizate*.

(6) Președintele Comitetului european pentru protecția datelor informează pe cale electronică, fără întârzieri nejustificate, membrii Comitetului european pentru protecția datelor și Comisia cu privire la orice informație relevantă care i-a fost comunicată, utilizând un formular standard. Secretariatul Comitetului european pentru protecția datelor furnizează traduceri ale informațiilor relevante, acolo unde este necesar.

Articolul 58

Avizul Comitetului european pentru protecția datelor

(1) (...)

(2) (...)

(3) (...)

(4) (...)

(5) (...)

(6) (...)

(7) În cazurile menționate la articolul 57 alineatele (2) și (4), Comitetul european pentru protecția datelor emite un aviz cu privire la chestiunea care îi este prezentată, cu condiția să nu fi emis deja un aviz cu privire la aceeași chestiune. Avizul respectiv este adoptat în termen de o lună cu majoritate simplă a membrilor Comitetului european pentru protecția datelor. Această perioadă poate fi prelungită cu o lună, ținându-se seama de complexitatea chestiunii. În ceea ce privește proiectul de decizie transmis membrilor comitetului în conformitate cu articolul 57 alineatul (6), un membru care nu a emis obiecții în termenul indicat de președinte se consideră a fi de acord cu proiectul de decizie.

(7a) În cursul perioadei menționate la alineatul (7), autoritatea de supraveghere competentă nu își adoptă proiectul de decizie în conformitate cu articolul 57 alineatul (2).

(7b) Președintele Comitetului european pentru protecția datelor informează, fără întârzieri nejustificate, autoritatea de supraveghere menționată, după caz, la alineatele (2) și (4) de la articolul 57, precum și Comisia, cu privire la aviz și îl publică.

(8) Autoritatea de supraveghere menționată la articolul 57 alineatul (2) ține seama pe deplin de avizul Comitetului european pentru protecția datelor și comunică pe cale electronică președintelui Comitetului european pentru protecția datelor, în termen de două săptămâni de la primirea avizului, dacă își păstrează sau își va modifica proiectul de decizie și, dacă este cazul, transmite proiectul de decizie modificat, utilizând un formular standard.

(9) În cazul în care autoritatea de supraveghere vizată informează președintele Comitetului european pentru protecția datelor, în termenul menționat la alineatul (8), că intenționează să nu se conformeze avizului comitetului, integral sau parțial, oferind motivele relevante, se aplică articolul 57 alineatul **(3)**.

(10) (...)

(11) (...)

Articolul 58a

Deciziile Comitetului european pentru protecția datelor

(1) În cazurile menționate la articolul 57 alineatul (3), Comitetul european pentru protecția datelor adoptă o decizie cu privire la chestiunea care îi este prezentată, pentru a asigura aplicarea corectă și consecventă a prezentului regulament în fiecare caz în parte. Decizia se motivează și se adresează autorității de supraveghere principale și tuturor autorităților de supraveghere vizate, fiind obligatorie pentru acestea.

(2) Decizia menționată la alineatul (1) se adoptă în termen de o lună de la prezentarea chestiunii, cu o majoritate de două treimi a membrilor comitetului. Această perioadă poate fi prelungită cu o lună, ținându-se seama de complexitatea chestiunii.

(3) În cazul în care comitetul nu a fost în măsură să adopte o decizie în termenele menționate la alineatul (2), acesta își adoptă decizia în termen de două săptămâni de la data expirării celei de a doua luni menționate la alineatul (2), cu o majoritate simplă a membrilor săi. În cazul în care membrii comitetului au opinii divergente, decizia se adoptă prin votul președintelui.

(4) Autoritățile de supraveghere vizate nu adoptă o decizie asupra chestiunii prezentate comitetului în conformitate cu alineatul (1) în perioadele menționate la alineatele (2) și (3).

(5) (...)

(6) Președintele Comitetului european pentru protecția datelor notifică, fără întârzieri nejustificate, decizia menționată la alineatul (1) autorităților de supraveghere vizate. Comitetul informează Comisia cu privire la acest lucru. Decizia se publică pe site-ul internet al Comitetului european pentru protecția datelor, fără întârziere după notificarea de către autoritatea de supraveghere a deciziei finale menționate la alineatul (7).

(7) Autoritatea de supraveghere principală sau, dacă este cazul, autoritatea de supraveghere la care s-a depus plângerea își adoptă decizia finală pe baza deciziei menționate la alineatul (1), fără întârziere și în termen de cel mult o lună de la notificarea de către Comitetul european pentru protecția datelor a deciziei sale. Autoritatea de supraveghere principală sau, dacă este cazul, autoritatea de supraveghere la care s-a depus plângerea informează Comitetul european pentru protecția datelor cu privire la data la care decizia sa finală este notificată operatorului sau persoanei împuternicite de operator și, respectiv, persoanei vizate. Decizia finală a autorităților de supraveghere vizate se adoptă în conformitate cu condițiile prevăzute la articolul 54a alineatele (4a), (4b) și (4bb). Decizia finală se referă la decizia menționată la alineatul (1) și precizează faptul că decizia menționată la alineatul (1) va fi publicată pe site-ul internet al Comitetului european pentru protecția datelor, în conformitate cu alineatul (6). La decizia finală se anexează decizia menționată la alineatul (1).

Articolul 59

Avizul Comisiei

(...)

Articolul 60

Suspendarea unui proiect de măsură

(...)

Articolul 61

Procedura de urgență

(1) În circumstanțe excepționale, atunci când o autoritate de supraveghere vizată consideră că există o necesitate urgentă de a acționa în scopul protejării drepturilor și libertăților persoanelor vizate, aceasta poate, prin derogare de la mecanismul pentru asigurarea coerenței menționat la articolul 57 sau de la procedura menționată la articolul 54a, să adopte de îndată măsuri provizorii menite să producă efecte juridice pe teritoriul propriului stat membru, cu o perioadă de valabilitate determinată. Autoritatea de supraveghere comunică fără întârziere aceste măsuri și motivele adoptării lor celorlalte autorități de supraveghere vizate, Comitetului european pentru protecția datelor și Comisiei.

(2) În cazul în care o autoritate de supraveghere a adoptat o măsură în temeiul alineatului (1) și consideră că este necesară adoptarea de urgență a unor măsuri definitive, aceasta poate solicita un aviz de urgență sau o decizie obligatorie urgentă din partea Comitetului european pentru protecția datelor, indicând motivele pentru această solicitare.

(3) Orice autoritate de supraveghere poate solicita un aviz de urgență sau o decizie obligatorie urgentă, după caz, din partea Comitetului european pentru protecția datelor în cazul în care o autoritate de supraveghere competentă nu a luat o măsură adecvată într-o situație în care există o necesitate urgentă de a acționa pentru a proteja drepturile și libertățile persoanelor vizate, indicând motivele pentru solicitarea unui astfel de aviz sau a unei astfel de decizii, inclusiv pentru necesitatea urgentă de a acționa.

(4) Prin derogare de la articolul 58 alineatul (7) și articolul 58a alineatul (2), un aviz de urgență sau o decizie obligatorie urgentă menționat(ă) la alineatele (2) și (3) de la prezentul articol este adoptat(ă) în termen de două săptămâni cu majoritate simplă a membrilor Comitetului european pentru protecția datelor.

Articolul 62

Acte de punere în aplicare

(1) Comisia poate adopta acte de punere în aplicare cu un domeniu de aplicare general pentru:

(a) (…).

(b) (…).

(c) (…).

(d) a defini modalitățile de realizare a schimbului electronic de informații între autoritățile de supraveghere, precum și între autoritățile de supraveghere și Comitetul european pentru protecția datelor, în special formularul standard menționat la articolul 57 alineatele (5) și (6) și la articolul 58 alineatul (8).

Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 87 alineatul (2).

(2) (...)

(3) (...)

Articolul 63

Asigurarea respectării regulamentului

(...)

Secțiunea 3

Comitetul european pentru protecția datelor

Articolul 64

Comitetul european pentru protecția datelor

(1a) Comitetul european pentru protecția datelor se instituie ca organ al Uniunii și are personalitate juridică.

(1b) Comitetul european pentru protecția datelor este reprezentat de președintele său**.**

(2) Comitetul european pentru protecția datelor este alcătuit din șefii câte unei autorități de supraveghere din fiecare stat membru sau din reprezentanții acestor șefi și din Autoritatea Europeană pentru Protecția Datelor.

(3) În cazul în care într-un stat membru mai multe autorități de supraveghere sunt responsabile de monitorizarea punerii în aplicare a dispozițiilor prevăzute de prezentul regulament, (...) se numește un reprezentant comun în conformitate cu legislația națională a statului membru respectiv.

(4) Comisia și Autoritatea Europeană pentru Protecția Datelor sau reprezentatul acesteia din urmă au dreptul de a participa la activitățile și reuniunile Comitetului european pentru protecția datelor *fără drept de vot*. Comisia numește un reprezentant. Președintele Comitetului european pentru protecția datelor comunică Comisiei **(...)** activitățile Comitetului european pentru protecția datelor.

Articolul 65

Independență

(1) Comitetul european pentru protecția datelor acționează independent în îndeplinirea sarcinilor sale sau în exercitarea competențelor sale în conformitate cu articolele 66 (…) și 67.

(2) Fără a aduce atingere solicitărilor din partea Comisiei menționate la articolul 66 alineatul (1) litera (b) și alineatul (2), Comitetul european pentru protecția datelor, în îndeplinirea sarcinilor sale sau în exercitarea competențelor sale, nu solicită și nu acceptă instrucțiuni de la nicio parte externă.

Articolul 66

Sarcinile Comitetului european pentru protecția datelor

(1) Comitetul european pentru protecția datelor promovează aplicarea uniformă a prezentului regulament. În acest sens, din proprie inițiativă sau la solicitarea Comisiei, Comitetul european pentru protecția datelor are, în special, următoarele sarcini:

(aa)să monitorizeze și să asigure aplicarea corectă a prezentului regulament, în cazurile prevăzute la articolul 57 alineatul (3), fără a aduce atingere sarcinilor autorităților naționale de supraveghere;

(a) să ofere Comisiei consiliere cu privire la orice aspect legat de protecția datelor cu caracter personal în cadrul Uniunii, inclusiv cu privire la orice propunere de modificare a prezentului regulament;

(b) să examineze, din proprie inițiativă sau la cererea unuia dintre membrii săi sau la cererea Comisiei, orice chestiune referitoare la punerea în aplicare a prezentului regulament și să emită orientări, recomandări și bune practici pentru a încuraja aplicarea uniformă a prezentului regulament;

(ba) să elaboreze orientări destinate autorităților de supraveghere, referitoare la aplicarea măsurilor menționate la articolul 53 alineatele (1), (1b) și (1c) și să stabilească amenzile administrative în conformitate cu articolele 79 și 79a;

(c) să revizuiască aplicarea practică a orientărilor, recomandărilor și bunelor practici menționate la literele (b) și (ba);

(ca) să încurajeze elaborarea de coduri de conduită și stabilirea unor mecanisme de certificare, precum și a unor sigilii și mărci în domeniul protecției datelor, în conformitate cu articolele 38 și 39;

(cb) să efectueze acreditarea organismelor de certificare și revizuirea periodică a acreditării în conformitate cu articolul 39a și să țină un registru public al organismelor acreditate, în conformitate cu articolul 39a alineatul (6), și al operatorilor acreditați sau al persoanelor împuternicite de operator acreditate, stabiliți (stabilite) în țări terțe, în conformitate cu articolul 39 alineatul (4);

(cd) să precizeze cerințele menționate la articolul 39a alineatul (3), în vederea acreditării organismelor de certificare prevăzute la articolul 39;

(ce) să comunice Comisiei un aviz privind nivelul de protecție a datelor cu caracter personal în țările terțe sau organizațiile internaționale, în special în cazurile menționate la articolul 41;

(d) să emită avize privind proiectele de decizii ale autorităților de supraveghere în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 57 alineatul (2) și privind chestiunile prezentate în conformitate cu articolul 57 alineatul (4);

(e) să promoveze cooperarea și schimbul eficient bilateral și multilateral de informații și practici între autoritățile de supraveghere;

(f) să promoveze programe comune de formare și să faciliteze schimburile de personal între autoritățile de supraveghere, precum și, după caz, cu autoritățile de supraveghere ale țărilor terțe sau organizațiilor internaționale;

(g) să promoveze schimbul de cunoștințe și de documente privind legislația și practicile în materie de protecție a datelor cu autoritățile de supraveghere a protecției datelor la nivel mondial.

(h) (…).

(i) să țină un registru electronic accesibil publicului cu deciziile luate de autoritățile de supraveghere și de instanțe cu privire la chestiuni tratate în cadrul mecanismului pentru asigurarea coerenței.

(2) În cazul în care Comisia consultă Comitetul european pentru protecția datelor, aceasta poate indica un termen limită, ținând seama de caracterul urgent al chestiunii.

(3) Comitetul european pentru protecția datelor își transmite avizele, orientările, recomandările și bunele practici Comisiei și comitetului menționat la articolul 87 și le publică.

Articolul 67

Rapoarte

(1) (...)

(2) Comitetul european pentru protecția datelor *întocmește un raport anual privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal în Uniune și*, dacă este relevant, *în țări terțe* și organizații internaționale. Raportul este pus la dispoziția publicului și transmis Parlamentului European, Consiliului și Comisiei.

(3) Raportul anual include o revizuire a aplicării practice a orientărilor, recomandărilor și bunelor practici menționate la articolul 66 alineatul (1) litera (c), precum și a deciziilor obligatorii menționate la articolul 57 alineatul (3).

Articolul 68

Procedura

(1) Comitetul european pentru protecția datelor adoptă decizii obligatorii, astfel cum se menționează la articolul 57 alineatul (3), în conformitate cu cerințele privind majoritatea prevăzute la articolul 58a alineatele (2) și (3). În ceea ce privește deciziile referitoare la celelalte sarcini menționate la articolul 66, ele se iau cu o majoritate simplă a membrilor săi.

(2) Comitetul european pentru protecția datelor își adoptă propriul regulament de procedură cu o majoritate de două treimi a membrilor săi și își organizează propriile mecanisme de funcționare.

Articolul 69

Președintele

(1) Comitetul european pentru protecția datelor alege un președinte și doi vicepreședinți din rândul membrilor săi, cu majoritate simplă (…).

(2) Mandatul președintelui și al vicepreședinților este de cinci ani și poate fi prelungit o singură dată.

Articolul 70

Sarcinile președintelui

(1) Președintele are următoarele sarcini:

(a) să convoace reuniunile Comitetului european pentru protecția datelor și să stabilească ordinea de zi;

(aa) să notifice deciziile adoptate de Comitetul european pentru protecția datelor, în conformitate cu articolul 58a, autorității de supraveghere principale și autorităților de supraveghere *vizate*;

(b) să asigure îndeplinirea la timp a sarcinilor Comitetului european pentru protecția datelor, în special în ceea ce privește mecanismul pentru asigurarea coerenței menționat la articolul 57.

(2) Comitetul european pentru protecția datelor definește în regulamentul său de procedură repartizarea sarcinilor care revin președintelui și vicepreședinților.

Articolul 71

Secretariatul

(1) Comitetul european pentru protecția datelor dispune de un secretariat, care este asigurat de secretariatul Autorității Europene pentru Protecția Datelor (...).

(1a) Secretariatul își îndeplinește sarcinile exclusiv pe baza instrucțiunilor președintelui Comitetului european pentru protecția datelor.

(1b) Personalul secretariatului Autorității Europene pentru Protecția Datelor implicat în îndeplinirea sarcinilor conferite Comitetului european pentru protecția datelor în temeiul prezentului regulament este separat din punct de vedere organizațional de personalul implicat în îndeplinirea sarcinilor conferite Autorității Europene pentru Protecția Datelor și face obiectul unor linii de raportare separate.

(1c) Dacă este cazul, Comitetul european pentru protecția datelor, în colaborare cu Autoritatea Europeană pentru Protecția Datelor, elaborează și publică un cod de conduită pentru punerea în aplicare a prezentului articol, care să se aplice personalului secretariatului Autorității Europene pentru Protecția Datelor implicat în îndeplinirea sarcinilor conferite Comitetului european pentru protecția datelor în temeiul prezentului regulament.

(2) Secretariatul oferă sprijin analitic, administrativ și logistic Comitetului european pentru protecția datelor.

(3) Secretariatul este responsabil în special de următoarele:

(a) gestionarea cotidiană a Comitetului european pentru protecția datelor;

(b) comunicarea dintre membrii Comitetului european pentru protecția datelor, președintele acestuia și Comisie și comunicarea cu alte instituții și cu publicul larg;

(c) utilizarea mijloacelor electronice pentru comunicarea internă și externă;

(d) traducerea informațiilor relevante;

(e) pregătirea și monitorizarea acțiunilor ulterioare reuniunilor Comitetului european pentru protecția datelor;

(f) pregătirea, redactarea și publicarea avizelor, deciziilor privind soluționarea litigiilor dintre autoritățile de supraveghere și a altor texte adoptate de Comitetul european pentru protecția datelor.

Articolul 72

Confidențialitate

(1) Discuțiile din cadrul Comitetului european pentru protecția datelor sunt confidențiale.

(2) Accesul la documentele prezentate membrilor Comitetului european pentru protecția datelor, experților și reprezentanților părților terțe este reglementat de Regulamentul (CE) nr. 1049/2001.

CAPITOLUL VIII

CĂI DE ATAC, RĂSPUNDERE ȘI SANCȚIUNI

Articolul 73

Dreptul de a depune o plângere la o autoritate de supraveghere

(1) Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o singură autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul său de muncă sau în care a avut loc eventuala încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează nu respectă prezentul regulament.

(2) (...)

(3) (...)

(4) (...)

(5) Autoritatea de supraveghere la care s-a depus plângerea informează reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în conformitate cu articolul 74 (...)**.**

Articolul 74

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

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

(2) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară *eficace* în cazul în care autoritatea de supraveghere competentă în conformitate cu articolele 51 și 51a nu soluționează o plângere sau nu informează persoana vizată în termen de trei luni sau în orice termen mai scurt prevăzut în dreptul Uniunii sau al statului membru cu privire la progresele sau la soluționarea plângerii depuse în conformitate cu articolul 73.

(3) (...) Acțiunile introduse împotriva unei (...) autorități de supraveghere sunt aduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere.

(3a) În cazul în care acțiunile sunt introduse împotriva unei decizii a unei autorități de supraveghere care a fost precedată de un aviz sau o decizie a Comitetului european pentru protecția datelor în cadrul mecanismului pentru asigurarea coerenței, autoritatea de supraveghere transmite curții avizul respectiv sau decizia respectivă.

(4) (...)

(5) (...)

Articolul 75

Dreptul la o cale de atac judiciară eficace împotriva unui operator sau unei persoane împuternicite de operator

(1) Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere în conformitate cu articolul 73, persoanele vizate au dreptul de a exercita o cale de atac judiciară eficace în cazul în care consideră că drepturile de care beneficiază în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării datelor lor cu caracter personal fără a se respecta prezentul regulament.

(2) Acțiunile introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în fața instanțelor din statul membru unde operatorul sau persoana împuternicită de operator are un sediu (...). Alternativ, o astfel de acțiune poate fi prezentată în fața instanțelor din statul membru în care persoana vizată își are reședința obișnuită, cu excepția cazului în care operatorul sau persoana împuternicită de operator este o autoritate publică ce acționează în exercitarea competențelor sale publice.

(3) (...)

(4) (...)

Articolul 76

Reprezentarea persoanelor vizate

1. Persoana vizată are dreptul de a mandata un organism, o organizație sau o asociație*, care au fost constituite în mod corespunzător, în conformitate cu legislația unui stat membru, şi ale căror obiective statutare includ protecția drepturilor şi libertăților persoanelor vizate în ceea ce priveşte protecția datelor lor cu caracter personal, să depună plângerea în numele său* și să exercite în numele său drepturile menționate la articolele 73, 74 și 75.

(1a) (…)

(2) Statele membre pot prevedea că orice organism, organizație sau asociație menționată la alineatul (1), independent de mandatul unei persoanei vizate (...), are în statul membru respectiv dreptul de a depune o plângere la autoritatea de supraveghere competentă în conformitate cu articolul 73 și de a își exercita drepturile menționate la articolele 73, 74 și 75, în cazul în care consideră că drepturile unei persoane vizate au fost încălcate ca urmare a prelucrării datelor cu caracter personal fără respectarea prezentului regulament.

3. (...)

4. (...)

Articolul 76a

Suspendarea procedurilor

(1) În cazul în care o instanță competentă a unui stat membru are informații că pe rolul unei instanțe dintr-un alt stat membru se află proceduri cu privire la același obiect în ceea ce privește activitățile de prelucrare (...) ale aceluiași operator sau ale aceleași persoane împuternicite de operator, instanța respectivă contactează instanța din celălalt stat membru pentru a confirma existența unor astfel de proceduri.

(2) Atunci când pe rolul unei instanțe dintr-un alt stat membru se află proceduri cu privire la același obiect în ceea ce privește activitățile de prelucrare (...) ale aceluiași operator sau ale aceleași persoane împuternicite de operator, orice altă instanță competentă decât instanța sesizată inițial poate suspenda procedurile acesteia.

(2a) În cazul în care aceste proceduri se află pe rolul instanțelor de prim grad de jurisdicție, orice instanță judecătorească sesizată ulterior poate, de asemenea, la cererea uneia dintre părți, să-și decline competența, cu condiția ca respectivele proceduri să fie de competența primei instanțe sesizate și ca legea acesteia să permită conexarea acțiunilor.

(3) (…).

Articolul 77

Dreptul la despăgubiri și răspunderea

(1) Orice persoană care a suferit daune materiale sau nemateriale ca urmare a unei operațiuni de prelucrare care nu este conformă cu dispozițiile prezentului regulament are dreptul să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru daunele suferite.

(2) Orice operator (...) implicat în operațiunile de prelucrare este răspunzător pentru daunele cauzate de operațiunile sale de prelucrare care nu sunt conforme cu prezentul regulament. Persoana împuternicită de operator este răspunzătoare pentru (...) daunele cauzate de prelucrare numai în cazul în care nu a respectat obligațiile din prezentul regulament care revin în mod specific persoanelor împuternicite de operator sau a acționat în afara sau în contradicție cu instrucțiunile legale ale operatorului.

(3) Operatorul sau persoana împuternicită de operator este exonerată de răspundere, în conformitate cu alineatul (2) (...) dacă (....) dovedește că nu este răspunzătoare în niciun fel (....) pentru evenimentul care a cauzat daunele.

(4) *În cazul în care mai mulți operatori sau mai multe persoane împuternicite de operator sau un operator și o persoană împuternicită de operator sunt implicate în aceeași operațiune de prelucrare* și sunt, *în conformitate cu alineatele (2) și (3),* responsabile pentru orice daune cauzate de prelucrare, (…) fiecare operator sau persoană împuternicită de către operator este (...) răspunzătoare *pentru totalitatea daunelor*.

(5) În cazul în care un operator sau o persoană împuternicită de operator a plătit, în conformitate cu alineatul (4), despăgubiri integrale pentru daunele suferite, respectivul operator sau respectiva persoană împuternicită de operator are dreptul să solicite de la ceilalți operatori sau celelalte persoane împuternicite de operator implicate în aceeași operațiune de prelucrare recuperarea acelei părți din despăgubiri care corespunde părții lor de răspundere pentru daune, în conformitate cu condițiile stabilite la alineatul (2).

(6) *Acțiunile în instanță introduse pentru exercitarea dreptului de a primi compensații sunt prezentate instanțelor competente în temeiul dreptului intern din statul membru menționat la articolul 75 alineatul (2).*

Articolul 78

Sancțiuni

(...)

Articolul 79

Condiții generale pentru impunerea amenzilor administrative

(1) Fiecare autoritate de supraveghere **(...)** asigură faptul că impunerea unor amenzi administrative în conformitate cu prezentul articol pentru încălcări ale prezentului regulament menționate la articolul 79a (...) *este, în fiecare caz, eficace, proporțională și disuasivă*.

(2) **(...)**

(2a) *În funcție de circumstanțele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menționate la articolul 53* alineatul (1b) literele (a)-(f). Atunci când se ia decizia dacă să se impună o amendă administrativă (...) și decizia cu privire la valoarea amenzii administrative în fiecare caz în parte, se acordă atenția cuvenită **(...)** următoarelor aspecte:

(a) natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și *de numărul persoanelor vizate afectate și de nivelul daunelor suferite de acestea*;

(b) dacă încălcarea a fost comisă intenționat sau din neglijență;

(c) (…).

(d) acțiunile întreprinse de operator sau de persoana împuternicită de operator pentru a reduce dauna suferită de persoana vizată;

(e) gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator în contextul măsurilor tehnice și organizatorice puse în aplicare de acesta în conformitate cu articolele 23 și 30;

(f) eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;

(g) (…);

(h) modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;

(i) în cazul în care măsurile menționate la (…) articolul 53 alineatul (1b) literele (a), (d), (e) și (f) au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la același obiect, *adică respectarea acestor măsuri*;

(j) aderarea la coduri de conduită aprobate, în conformitate cu articolul 38, sau la mecanisme de certificare aprobate, în conformitate cu articolul 39;

(k) (…);

(l) (…);

(m) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului.

(3) (...)

(3a) (...)

(3b) Fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi impuse amenzi administrative autorităților publice și organismelor publice stabilite în statul membru respectiv.

(4) *Exercitarea de către autoritatea de supraveghere* (...) a competențelor sale în temeiul prezentului articol face obiectul unor garanții procedurale adecvate, în conformitate cu dreptul Uniunii și al statului membru în cauză, printre care se numără căi de atac judiciare eficace și procese echitabile.

(5) Până la [data menționată la articolul 91 alineatul (2)], statele membre se pot abține de la a prevedea norme privind amenzi administrative, astfel cum se menționează la articolul 79a alineatele (1), (2) și (3), în cazul în care sistemele lor juridice nu prevăd amenzi administrative, iar încălcările menționate la articolul respectiv fac deja obiectul sancțiunilor penale în dreptul lor intern, asigurându-se în același timp că aceste sancțiuni penale sunt eficace, proporționate și disuasive, ținând cont de nivelul amenzilor administrative prevăzute în prezentul regulament.

Dacă decid astfel, statele membre notifică Comisiei secțiunile relevante din dreptul lor penal.

Articolul 79a

Amenzi administrative

(1) Autoritatea de supraveghere (...) poate impune o amendă care nu depășește 250 000 EUR sau, în cazul unei întreprinderi, 0,5 % din cifra sa de afaceri anuală totală realizată la nivel mondial din exercițiul financiar anterior, unui operator care, intenționat sau din neglijență:

(a) nu răspunde în termenul menționat la articolul 12 alineatul (2) la cererile persoanei vizate;

(b) percepe o taxă, încălcând articolul 12 alineatul (4) prima teză.

(2) Autoritatea de supraveghere (…) poate impune o amendă care nu depășește 500 000 EUR sau, în cazul unei întreprinderi, 1 % din cifra sa de afaceri anuală totală realizată la nivel mondial (...) din exercițiul financiar anterior, unui operator sau unei persoane împuternicite de operator care, intenționat sau din neglijență:

(a) nu furnizează persoanei vizate informațiile sau (…) furnizează informații incomplete sau nu furnizează informațiile [la timp sau] într-un mod [suficient] de transparent, în temeiul articolului 12 alineatul (3) și al articolelor 14 și 14a;

(b) nu oferă acces persoanei vizate sau nu rectifică datele cu caracter personal în temeiul articolelor 15 și 16 (...);

(c) nu șterge datele cu caracter personal, încălcând dreptul de ștergere și de a fi uitat, în temeiul articolului 17 alineatul (1) litera (a), (b), (d) sau (e);

(d) (...)

(da) prelucrează date cu caracter personal cu încălcarea dreptului la restricționarea prelucrării, în temeiul articolului 17a, sau nu informează persona vizată înainte de ridicarea restricției de prelucrare, în temeiul articolului 17a alineatul (4);

(db) nu comunică nicio rectificare, ștergere sau restricționare a prelucrării fiecărui destinatar căruia operatorul i-a dezvăluit date cu caracter personal, încălcând articolul 17b;

(dc) nu furnizează datele cu caracter personal ale persoanei vizate care îl/o privesc (...), încălcând articolul 18;

(dd) prelucrează date cu caracter personal după declarația de opoziție a persoanei vizate, în temeiul articolului 19 alineatul (1), și nu demonstrează că are motive legitime și imperioase care justifică prelucrarea și care primează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță;

(de) nu furnizează persoanei vizate informații cu privire la dreptul de a se opune prelucrării în scopul marketingului direct, în temeiul articolului 19 alineatul (2), sau continuă să prelucreze date în scopuri de marketing direct după declarația de opoziție a persoanei vizate, încălcând articolului 19 alineatul (2a);

(e) nu definește sau nu definește suficient responsabilitățile respective ale operatorilor asociați, în temeiul articolului 24;

(f) nu păstrează deloc sau nu păstrează suficientă documentație, în temeiul articolului 28 și al articolului 31 alineatul (4).

(g) (...)

(3) Autoritatea de supraveghere (…) poate impune o amendă care nu depășește 1 000 000 EUR sau, în cazul unei întreprinderi, 2 % din cifra sa de afaceri anuală totală realizată la nivel mondial din exercițiul financiar anterior, unui operator sau unei persoane împuternicite de operator care, intenționat sau din neglijență:

(a) prelucrează datele cu caracter personal fără un (...) temei juridic pentru prelucrare sau nu respectă condițiile privind consimțământul, în temeiul articolelor 6, 7, 8 și 9;

(b) (…);

(c) (…);

(d) nu respectă condițiile legate de (…) procesul decizional automatizat, inclusiv crearea de profiluri, în temeiul articolului 20;

(da) nu (…) pune în aplicare măsuri corespunzătoare sau nu poate demonstra conformitatea, în temeiul articolelor 22 (…) și 30;

(db) nu desemnează un reprezentant, încălcând articolul 25;

(dc) prelucrează date cu caracter personal sau dă instrucțiuni de prelucrare a datelor cu caracter personal, încălcând articolul 26 (…);

(dd) nu semnalează sau nu notifică o încălcare a securității datelor cu caracter personal sau nu notifică [la timp ori] complet această încălcare autorității de supraveghere sau persoanei vizate, încălcând articolele 31 și 32;

(de) nu efectuează o evaluare a impactului privind protecția datelor, încălcând articolul 33, sau prelucrează date cu caracter personal fără consultarea prealabilă a autorității de supraveghere, încălcând articolul 34 alineatul (2);

(e) (…);

(f) utilizează abuziv un sigiliu sau o marcă din domeniul protecției datelor, în sensul articolului 39, sau nu respectă condițiile și procedurile prevăzute la articolele 38a și 39a;

(g) efectuează sau dă instrucțiuni pentru efectuarea unui transfer de date către un destinatar dintr-o țară terță sau o organizație internațională, încălcând articolele 41-44;

(h) nu respectă un ordin sau o limitare temporară sau definitivă asupra prelucrării, sau suspendarea fluxurilor de date, emisă de autoritatea de supraveghere, în temeiul articolului 53 alineatul (1b), sau nu acordă accesul, încălcând articolul 53 alineatul (1).

(i) (...)

(j) (…).

(3a) În cazul în care un operator sau o persoană împuternicită de operator încalcă în mod intenționat sau din neglijență mai multe dispoziții din prezentul regulament enumerate la alineatele (1), (2) sau (3), cuantumul total al amenzii nu poate depăși suma prevăzută pentru cele mai grave încălcări.

(4) (...)

Articolul 79b

Sancțiuni

(1) În cazul încălcărilor (...) prezentului regulament, în special al încălcărilor care nu fac obiectul amenzilor administrative în temeiul (...) *articolului 79a, statele membre definesc normele privind sancțiunile aplicabile încălcărilor respective și iau toate măsurile necesare pentru a se asigura că aceste norme sunt puse în aplicare (…). Sancțiunile respective sunt eficace, proporționale și disuasive.*

(2) (…).

(3) Fiecare stat membru informează Comisia cu privire la dispozițiile din propria legislație pe care le adoptă în temeiul alineatului (1), până la data menționată la articolul 91 alineatul (2) cel târziu, precum și, fără întârziere, cu privire la orice modificare ulterioară care le afectează.

CAPITOLUL IX DISPOZIȚII REFERITOARE LA SITUAȚII SPECIFICE DE PRELUCRARE A DATELOR

Articolul 80

Prelucrarea datelor cu caracter personal și libertatea de exprimare <u>și de informare</u>

(1) <u>Dreptul intern al</u> statului membru (…) asigură un echilibru între dreptul la protecția datelor cu caracter personal <u>în temeiul prezentului regulament</u> și <u>dreptul la</u> libertatea de exprimare și <u>de informare, inclusiv prelucrarea acestor date în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare.</u>

(2) <u>În vederea *prelucrării datelor cu caracter personal efectuate în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare*, statele membre prevăd exonerări sau derogări de la dispozițiile capitolului II (principii), ale capitolului III (drepturile persoanei vizate), ale capitolului IV (operatorul și persoana împuternicită de operator), ale capitolului V (transferul datelor cu caracter personal către țări terțe sau organizații internaționale), ale capitolului VI (autorități de supraveghere independente), ale capitolului VII (cooperare și coerență) , în cazul în care acestea sunt necesare pentru a asigura un echilibru între dreptul la protecția datelor cu caracter personal și libertatea de exprimare și de informare</u>.

<u>Articolul 80a</u>

<u>Prelucrarea datelor cu caracter personal și accesul public la documente oficiale</u>

<u>Datele cu caracter personal din documentele oficiale deținute de o autoritate publică sau de un organism public sau privat pentru îndeplinirea unei sarcini care servește interesului public pot fi divulgate de autoritatea sau organismul respectiv în conformitate cu dreptul Uniunii sau al statului membru sub incidența căruia intră autoritatea sau organismul, pentru a stabili un echilibru între accesul public la documente oficiale și dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament.</u>

Articolul 80aa

Prelucrarea datelor cu caracter personal și reutilizarea informațiilor din sectorul public

Datele cu caracter personal din informațiile din sectorul public deținute de o autoritate publică sau de un organism *public* sau privat pentru îndeplinirea unei sarcini care servește interesului public *pot fi divulgate de autoritatea sau organismul respectiv în conformitate cu dreptul Uniunii sau al statului membru sub incidența căruia intră autoritatea sau organismul,* pentru a stabili un echilibru între reutilizarea unor astfel de documente oficiale și informații din sectorul public, pe de o parte, și *dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament, pe de altă parte*.

Articolul 80b

Prelucrarea unui număr de identificare național

Statele membre pot stabili condițiile specifice de prelucrare a unui număr de identificare național sau a oricărui alt identificator cu aplicabilitate generală. În acest caz, numărul de identificare național sau orice alt identificator cu aplicabilitate generală este folosit numai în temeiul unor garanții corespunzătoare pentru drepturile și libertățile persoanei vizate în temeiul prezentului regulament.

Articolul 81

Prelucrarea datelor cu caracter personal în scopuri legate de sănătate

(...)

Articolul 81a

Prelucrarea datelor genetice

(...)

Articolul 82

Prelucrarea în contextul ocupării unui loc de muncă

(1) Prin lege sau prin acorduri colective, statele membre pot asigura norme mai specifice pentru a asigura protecţia drepturilor şi a libertăţilor cu privire la prelucrarea datelor cu caracter personal ale angajaţilor în contextul ocupării unui loc de muncă, în special în scopul recrutării, îndeplinirii prevederilor contractului de muncă, inclusiv descărcarea de obligaţiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării şi organizării muncii, al egalităţii şi diversităţii la locul de muncă, al asigurării sănătăţii şi securităţii la locul de muncă, al protejării proprietăţii angajatorului şi a clientului, precum şi în scopul exercitării şi beneficierii, în mod individual sau colectiv, de drepturile şi beneficiile legate de ocuparea unui loc de muncă, precum şi pentru încetarea raporturilor de muncă. (...)

(2) Fiecare stat membru informează Comisia cu privire la dispoziţiile din propria legislaţie pe care le adoptă în temeiul alineatului (1), până la data menţionată la articolul 91 alineatul (2) cel târziu, precum şi, fără întârziere, cu privire la orice modificare ulterioară care le afectează.

(3) Statele membre pot stabili prin lege condiţiile în care datele cu caracter personal în contextul ocupării unui loc de muncă pot fi prelucrate pe baza consimţământului angajatului.

Articolul 82a

Prelucrarea în scopuri de protecţie socială

(...)

Articolul 83

Derogări aplicabile prelucrării datelor cu caracter personal pentru arhivare în interes public sau în scopuri ştiinţifice, statistice şi istorice

(1) În cazul în care datele cu caracter personal sunt prelucrate în scopuri ştiinţifice, statistice sau istorice, legislaţia Uniunii sau a statului membru, sub rezerva unor garanţii adecvate pentru drepturile şi libertăţile persoanei vizate, poate să prevadă derogări de la articolul 14a alineatele (1) şi (2), articolele 15, 16, 17, 17a, 17b, 18 şi 19, în măsura în care aceste derogări sunt necesare pentru îndeplinirea unor scopuri specifice.

(1a) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare în interes public, legislaţia Uniunii sau a statului membru, sub rezerva unor garanţii adecvate pentru drepturile şi libertăţile persoanei vizate, poate să prevadă derogări de la articolul 14a alineatele (1) şi (2), articolele 15, 16, 17, 17a, 17b, 18, 19, 23, 32, 33 şi 53 alineatul (1b) literele (d) şi (e), în măsura în care aceste derogări sunt necesare pentru îndeplinirea unor scopuri specifice.

(1b) În cazul în care un tip de prelucrare menţionat la alineatele (1) şi (1a) serveşte în acelaşi timp şi altui scop, derogările permise se aplică numai prelucrării în scopurile menţionate la alineatele respective.

(2) Garanţiile adecvate menţionate la alineatele (1) şi (1a) sunt prevăzute de legislaţia Uniunii sau a statelor membre şi sunt în aşa fel concepute încât să asigure că măsurile tehnologice şi/sau organizatorice de protecţie prevăzute de prezentul regulament se aplică datelor cu caracter personal, (…) în aşa fel încât să reducă la minimum prelucrarea datelor cu caracter personal pe baza principiilor proporţionalităţii şi necesităţii, cum ar fi *pseudonimizarea datelor* cu excepţia cazurilor în care aceste măsuri împiedică realizarea scopului prelucrării şi acest scop nu poate fi îndeplinit în alt mod cu mijloace rezonabile.

(3) (…).

Articolul 84

Obligații privind păstrarea confidențialității

(1) (…) Statele membre pot adopta norme specifice pentru a stabili competențele (…) autorităților de supraveghere, prevăzute la articolul 53 alineatul (1) literele (da) și (db), în legătură cu operatori sau cu persoane împuternicite de operatori care, în temeiul dreptului Uniunii sau al unui stat membru sau în temeiul normelor stabilite de organismele naționale competente, au obligația de a păstra secretul profesional, alte obligații echivalente de confidențialitate sau un cod de etică profesională monitorizat și aplicat de organisme profesionale, în cazul în care acest lucru este necesar și proporțional pentru a stabili un echilibru între dreptul la protecția datelor cu caracter personal și obligația păstrării confidențialității. Aceste norme se aplică doar în ceea ce privește datele cu caracter personal pe care operatorul sau persoana împuternicită de operator le-a primit sau le-a obținut în contextul unei activități care intră sub incidența acestei obligații de păstrare a confidențialității.

(2) Fiecare stat membru notifică Comisiei normele adoptate în temeiul alineatului (1), până la data precizată la articolul 91 alineatul (2) cel târziu, precum și, fără întârziere, orice modificare ulterioară care le afectează.

Articolul 85

Normele existente în domeniul protecției datelor pentru biserici și asociații religioase

(1) În cazul în care, într-un stat membru, bisericile și asociațiile sau comunitățile religioase aplică, la data intrării în vigoare a prezentului regulament, un set cuprinzător de norme de protecție a persoanelor fizice cu privire la prelucrarea datelor cu caracter personal, aceste norme pot continua să se aplice, cu condiția să fie aliniate la dispozițiile prezentului regulament.

(2) Bisericile și asociațiile religioase care aplică un set cuprinzător de norme în conformitate cu punctul 1, fac obiectul controlului unei autorități independente de supervizare care poate fi specifică, cu condiția ca aceasta să îndeplinească condițiile stabilite în capitolul VI din prezentul regulament.

CAPITOLUL X
ACTE DELEGATE ȘI ACTE DE PUNERE ÎN APLICARE

Articolul 86

Exercitarea delegării de competențe

(1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute de prezentul articol.

(2) Delegarea competenței prevăzute la (...) articolul 39a alineatul (7) (...) este conferită Comisiei pentru o perioadă nedeterminată, începând cu data intrării în vigoare a prezentului regulament.

(3) Delegarea competenței menționate la (...) articolul 39a alineatul (7) (...) poate fi revocată în orice moment de către Parlamentul European sau de către Consiliu. O decizie de revocare pune capăt delegării de competențe precizată în decizia respectivă. Aceasta intră în vigoare în ziua următoare publicării deciziei în *Jurnalul Oficial al Uniunii Europene* sau la o dată ulterioară menționată în decizie. Aceasta nu aduce atingere validității actelor delegate aflate deja în vigoare.

(4) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(5) Un act delegat adoptat în conformitate cu (...) articolul 39a alineatul (7) (...) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea actului respectiv Parlamentului European și Consiliului sau în cazul în care, înainte de expirarea termenului respectiv, Parlamentul European și Consiliul au informat Comisia cu privire la faptul că nu vor formula obiecții. Perioada se prelungește cu două luni, la inițiativa Parlamentului European sau a Consiliului.

Articolul 87

Procedura comitetului

(1) Comisia este asistată de un comitet. Comitetul respectiv este un comitet în sensul Regulamentului (UE) nr. 182/2011.

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

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

CAPITOLUL XI

DISPOZIȚII FINALE

Articolul 88

Abrogarea Directivei 95/46/CE

(1) Directiva 95/46/CE se abrogă.

(2) Trimiterile la directiva abrogată se interpretează ca trimiteri la prezentul regulament. Trimiterile la Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal instituit prin articolul 29 din Directiva 95/46/CE se interpretează ca trimiteri la Comitetul european pentru protecția datelor instituit prin prezentul regulament.

Articolul 89

Relația cu Directiva 2002/58/CE și modificarea acesteia

(1) Prezentul regulament nu impune obligații suplimentare pentru persoanele fizice sau juridice în ceea ce privește prelucrarea datelor cu caracter personal în legătură cu furnizarea de servicii de comunicații electronice destinate publicului în rețelele de comunicații publice din Uniune, cu privire la aspectele pentru care acestea fac obiectul unor obligații specifice cu același obiectiv precum cel prevăzut în Directiva 2002/58/CE.

2. (...)

Articolul 89a

Relația cu acordurile încheiate anterior

Acordurile internaționale care implică transferul de date cu caracter personal către țări terțe sau organizații internaționale, care au fost încheiate de statele membre înainte de intrarea în vigoare a prezentului regulament și care sunt în conformitate cu Directiva 95/46/CE, rămân în vigoare până când sunt modificate, înlocuite sau revocate.

Articolul 90

Evaluarea

(1) Comisia transmite Parlamentului European și Consiliului, la intervale regulate, rapoarte privind evaluarea și revizuirea prezentului regulament.

(2) În contextul acestor evaluări, Comisia examinează în special aplicarea și funcționarea dispozițiilor de la capitolul VII cu privire la cooperare și consecvență.

(3) Primul raport se transmite în termen de cel mult patru ani de la data intrării în vigoare a prezentului regulament. Următoarele rapoarte se transmit ulterior o dată la patru ani. Rapoartele se publică.

(4) Comisia transmite, dacă este necesar, propuneri corespunzătoare în vederea modificării prezentului regulament, precum și a alinierii altor instrumente juridice, în special ținând seama de evoluțiile din domeniul tehnologiei informației și având în vedere progresele societății informaționale.

Articolul 91

Intrare în vigoare și aplicare

(1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

(2) Prezentul regulament se aplică începând cu [*doi ani de la data menționată la alineatul (1)*].

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles,

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*