Orientările 01/2022 privind drepturile persoanelor vizate – Dreptul de acces

Versiunea 2.0

Adoptate la 28 martie 2023

Adoptate

Istoricul versiunilor

Versiunea 1.0	18 ianuarie 2022	Adoptarea orientărilor pentru consultarea publică
Versiunea 2.0	28 martie 2023	Adoptarea orientărilor în urma consultării publice

REZUMAT

Dreptul de acces al persoanelor vizate este consacrat la articolul 8 din Carta Drepturilor Fundamentale a UE. Acesta a făcut parte din cadrul juridic european privind protecția datelor încă de la început, și, în prezent, este în continuare dezvoltat prin normele mai detaliate și mai precise prevăzute la articolul 15 din RGPD.

Obiectivul și structura generală a dreptului de acces

Obiectivul general al dreptului de acces este de a oferi persoanelor fizice informații suficiente, transparente și ușor accesibile cu privire la prelucrarea datelor lor cu caracter personal, astfel încât să li se permită acestora să fie informate cu privire la prelucrare și să verifice legalitatea acesteia, precum și exactitatea datelor prelucrate. Acest lucru va facilita exercitarea altor drepturi de către persoane, cum ar fi dreptul la ștergere sau rectificare, însă nu constituie o condiție în acest sens.

În conformitate cu legislația privind protecția datelor, trebuie făcută distincția între dreptul de acces și drepturi similare care au alte obiective, de exemplu dreptul de acces la documentele publice, care vizează garantarea transparenței în cadrul procesului decizional al autorităților publice și a bunelor practici administrative.

Cu toate acestea, persoana vizată nu trebuie să prezinte motive pentru cererea de acces și nu este de competența operatorului să analizeze dacă cererea o va ajuta efectiv pe persoana vizată să verifice legalitatea prelucrării relevante sau să își exercite alte drepturi. Operatorul va trebui să dea curs cererii, cu excepția cazului în care este clar că cererea este formulată în temeiul altor norme decât normele privind protecția datelor.

Dreptul de acces include trei componente diferite:

- o confirmare că se prelucrează sau nu date cu caracter personal care privesc persoana în cauză;
- accesul la datele cu caracter personal respective și
- accesul la informații privind prelucrarea, cum ar fi scopul, categoriile de date și destinatarii, durata prelucrării, drepturile persoanelor vizate și garanțiile adecvate în cazul transferurilor către țări terțe.

Considerații generale privind evaluarea cererii persoanei vizate

Atunci când analizează conținutul cererii, operatorul trebuie să evalueze dacă cererea se referă la datele cu caracter personal ale persoanei care înaintează cererea, dacă cererea intră în domeniul de aplicare al articolului 15 și dacă există alte dispoziții mai specifice care reglementează accesul într-un anumit sector. Operatorul trebuie să evalueze, de asemenea, dacă cererea se referă la toate datele sau doar la anumite părți ale datelor prelucrate care privesc persoana vizată.

Nu există cerințe specifice privind formatul unei cereri. Operatorul ar trebui să pună la dispoziție canale de comunicare adecvate și ușor de utilizat, care să poată fi folosite cu ușurință de către persoana vizată. Cu toate acestea, persoana vizată nu este obligată să utilizeze aceste canale specifice și, în schimb, poate trimite cererea către un punct de contact oficial al operatorului. Operatorul nu este obligat să dea curs cererilor trimise la adrese complet aleatorii sau aparent incorecte.

În cazul în care operatorul nu este în măsură să identifice datele care se referă la persoana vizată, acesta informează persoana vizată în acest sens și poate refuza accesul, cu excepția cazului în care persoana vizată furnizează informații suplimentare care să permită identificarea. În plus, dacă are

îndoieli cu privire la faptul că persoana vizată este persoana care pretinde că este, operatorul poate solicita informații suplimentare pentru confirmarea identității persoanei vizate. Cererea de informații suplimentare trebuie să fie proporțională cu tipul de date prelucrate, cu prejudiciile care ar putea apărea etc. pentru a se evita colectarea excesivă a datelor.

Domeniul de aplicare al dreptului de acces

Domeniul de aplicare al dreptului de acces este determinat de domeniul de aplicare al conceptului de „date cu caracter personal", astfel cum este definit la articolul 4 punctul 1 din RGPD. Pe lângă datele cu caracter personal de bază, cum ar fi numele, adresa, numărul de telefon etc., există o gamă variată de date care se pot încadra în această definiție, cum ar fi constatările medicale, istoricul achizițiilor, indicatorii de bonitate, jurnalele de activitate, activitățile de căutare etc. Datele cu caracter personal care au fost pseudonimizate sunt considerate în continuare date cu caracter personal, spre deosebire de datele anonimizate. Dreptul de acces se referă la datele cu caracter personal ale persoanei care înaintează cererea. Acest concept nu ar trebui interpretat într-un mod prea restrictiv și poate include date care ar putea viza și alte persoane, de exemplu istoricul comunicărilor care implică mesaje primite și trimise.

Pe lângă furnizarea accesului la datele cu caracter personal, operatorul trebuie să furnizeze informații suplimentare cu privire la prelucrare și la drepturile persoanelor vizate. Astfel de informații se pot baza pe ceea ce este deja compilat în evidențele activităților de prelucrare ale operatorului (articolul 30 din RGPD) și în declarația de confidențialitate (articolele 13 și 14 din RGPD). Cu toate acestea, este posibil ca aceste informații generale să trebuiască să fie actualizate în funcție de momentul solicitării sau să fie adaptate pentru a reflecta operațiunile de prelucrare efectuate în legătură cu persoana care înaintează cererea.

Modalitatea de acordare a accesului

Modalitățile de acordare a accesului pot varia în funcție de volumul datelor și de complexitatea prelucrării efectuate. Cu excepția cazului în care se prevede altfel în mod explicit, cererea ar trebui înțeleasă ca referindu-se la *toate* datele cu caracter personal care privesc persoana vizată, iar operatorul poate solicita persoanei vizate să furnizeze precizări cu privire la cerere în cazul în care prelucrează un volum mare de date.

Operatorul va trebui să caute date cu caracter personal în toate sistemele informatice și neinformatice de evidență a datelor pe baza unor criterii de căutare care reflectă modul în care sunt structurate informațiile, de exemplu numele și numărul clientului. Comunicarea datelor și a altor informații cu privire la prelucrare trebuie să fie concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Cerințele mai precise în această privință depind de circumstanțele prelucrării datelor, precum și de capacitatea persoanei vizate de a pricepe și a înțelege comunicarea (de exemplu, ținând seama de faptul că persoana vizată este un copil sau o persoană cu nevoi speciale). În cazul în care datele constau în coduri sau alte „date primare", este posibil ca acestea să trebuiască să fie explicate pentru a avea sens pentru persoana vizată.

Principala modalitate de acordare a accesului este de a furniza persoanei vizate o copie a datelor sale, dar pot fi prevăzute și alte modalități (cum ar fi informațiile transmise verbal și accesul la fața locului) în cazul în care persoana vizată solicită acest lucru. Datele pot fi trimise prin e-mail, cu condiția să fie aplicate toate garanțiile necesare luând în considerare, de exemplu, natura datelor, sau în alte moduri, de exemplu printr-un instrument de *self-service*.

Uneori, atunci când există un volum mare de date și ar fi dificil pentru persoana vizată să înțeleagă informațiile dacă acestea sunt furnizate într-un singur calup – în special în contextul online – cea mai adecvată măsură ar putea fi o abordare pe mai multe niveluri. Furnizarea de informații pe mai multe niveluri poate facilita înțelegerea datelor de către persoana vizată. Operatorul trebuie să fie în măsură să demonstreze că abordarea pe mai multe niveluri are o valoare adăugată pentru persoana vizată, iar toate nivelurile ar trebui furnizate în același timp, dacă persoana vizată alege această variantă.

Copia datelor și informațiile suplimentare ar trebui furnizate în format permanent, cum ar fi text scris, care poate avea un format electronic utilizat în mod curent, astfel încât persoana vizată să îl poată descărca cu ușurință. Datele pot fi furnizate într-o transcriere sau într-o formă compilată, cu condiția să fie incluse toate informațiile, iar acest lucru să nu modifice sau să schimbe conținutul informațiilor.

Cererii trebuie să i se dea curs cât mai curând posibil și, în orice caz, în termen de o lună de la primire. Acest termen poate fi prelungit cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererii. Persoana vizată trebuie apoi să fie informată cu privire la motivul întârzierii. Operatorul trebuie să pună în aplicare măsurile necesare pentru a trata cererile cât mai curând posibil și să adapteze aceste măsuri la circumstanțele prelucrării. În cazul în care datele sunt stocate doar pentru o perioadă foarte scurtă, trebuie să existe măsuri care să garanteze că unei cereri de acces i se poate da curs fără ca datele să fie șterse în timpul soluționării cererii. În cazul în care se prelucrează un volum mare de date, operatorul va trebui să instituie proceduri și mecanisme adaptate complexității prelucrării.

Evaluarea cererii ar trebui să reflecte situația din momentul în care cererea a fost primită de operator. Vor trebui furnizate chiar și datele care ar putea fi incorecte sau prelucrate în mod ilegal. Datele care au fost deja șterse, de exemplu în conformitate cu o politică de păstrare și, prin urmare, nu mai sunt disponibile pentru operator nu pot fi furnizate.

Limitări și restricții

RGPD permite anumite limitări ale dreptului de acces. Nu există alte exceptări sau derogări. Dreptul de acces nu are nicio rezervă generală în ceea ce privește proporționalitatea legată de eforturile pe care operatorul trebuie să le depună pentru a da curs cererii persoanei vizate.

În conformitate cu articolul 15 alineatul (4), dreptul de a obține o copie nu aduce atingere drepturilor și libertăților altora. CEPD este de părere că aceste drepturi trebuie luate în considerare nu numai atunci când se acordă accesul prin furnizarea unei copii, ci și în cazul în care accesul la date este acordat prin alte mijloace (de exemplu, accesul la fața locului). Cu toate acestea, articolul 15 alineatul (4) nu se aplică informațiilor suplimentare privind prelucrarea, astfel cum se prevede la articolul 15 alineatul (1) literele (a)-(h). Operatorul trebuie să fie în măsură să demonstreze că, în situația concretă, nu se aduce atingere drepturilor sau libertăților altora. Aplicarea articolului 15 alineatul (4) nu ar trebui să conducă la refuzarea totală a cererii persoanei vizate; aceasta ar avea ca rezultat numai excluderea sau asigurarea ilizibilității acelor părți care pot aduce atingere drepturilor și libertăților altora.

Articolul 12 alineatul (5) din RGPD permite operatorilor să respingă cererile care sunt în mod vădit nefondate sau excesive sau să perceapă o taxă rezonabilă pentru astfel de cereri. Aceste concepte trebuie interpretate în sens restrâns. Întrucât există foarte puține condiții prealabile în ceea ce privește cererile de acces, domeniul de aplicare al interpretării unei cereri ca fiind în mod vădit nefondată este destul de limitat. Cererile excesive depind de particularitățile sectorului în care își desfășoară activitatea operatorul. Cu cât apar mai multe modificări în baza de date a operatorului, cu atât mai des persoana vizată poate fi autorizată să solicite accesul fără ca cererea să fie una excesivă. În loc să refuze accesul, operatorul poate decide să perceapă o taxă de la persoana vizată. Această taxă ar fi relevantă

numai în cazul cererilor excesive pentru a acoperi costurile administrative pe care le pot ocaziona astfel de cereri. Operatorul trebuie să fie în măsură să demonstreze caracterul vădit nefondat sau excesiv al unei cereri.

Restricții privind dreptul de acces pot fi prevăzute, de asemenea, în dreptul intern al statelor membre, în conformitate cu articolul 23 din RGPD și cu derogările prevăzute în acesta. Operatorii care intenționează să se bazeze pe astfel de restricții trebuie să verifice cu atenție cerințele dispozițiilor naționale și să ia act de oricare condiții specifice care s-ar putea aplica. Astfel de condiții pot consta într-o amânare doar temporară a dreptului de acces sau în aplicarea restricției exclusiv anumitor categorii de date.

Cuprins

Comitetul European pentru Protecția Datelor

având în vedere articolul 70 alineatul (1) litera (e) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „RGPD”),

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

având în vedere articolele 12 și 22 din Regulamentul său de procedură,

întrucât activitățile pregătitoare ale prezentelor orientări au implicat colectarea de contribuții de la părțile interesate, atât în scris, cât și în cadrul unui eveniment dedicat al părților interesate privind drepturile persoanelor vizate, pentru a identifica provocările și problemele de interpretare cu care se confruntă în aplicarea dispozițiilor relevante ale RGPD;

A ADOPTAT URMĂTOARELE ORIENTĂRI

1 INTRODUCERE – OBSERVAȚII GENERALE

1. În societatea de astăzi, datele cu caracter personal sunt prelucrate de entități publice și private, în cursul multor activități, cu o gamă largă de scopuri și în numeroase moduri diferite. Persoanele fizice se pot afla adesea într-o poziție dezavantajată în ceea ce privește înțelegerea modului în care sunt prelucrate datele lor cu caracter personal, inclusiv în ceea ce privește tehnologia utilizată în cazul respectiv, fie de către o entitate privată, fie de către o entitate publică. Pentru protejarea datelor cu caracter personal ale persoanelor fizice în aceste situații, RGPD a creat un cadru juridic coerent și solid, general aplicabil în ceea ce privește diferitele tipuri de prelucrare, inclusiv dispoziții specifice referitoare la drepturile persoanelor vizate.

2. Dreptul de acces la datele cu caracter personal este unul dintre drepturile persoanelor vizate prevăzute în capitolul III din RGPD, printre alte drepturi, cum ar fi, de exemplu, dreptul la rectificare și ștergere, dreptul la restricționarea prelucrării, dreptul la portabilitate, dreptul la opoziție sau dreptul de a nu face obiectul unui proces decizional individual automatizat, inclusiv crearea de profiluri[2]. Dreptul de acces al persoanei vizate este consacrat atât în Carta Drepturilor Fundamentale a UE (Carta)[3], cât și la articolul 15 din RGPD, unde este formulat cu precizie ca drept de acces la datele cu caracter personal și la alte informații conexe.

3. În temeiul RGPD, dreptul de acces constă în trei componente, și anume confirmarea că se prelucrează sau nu date cu caracter personal, accesul la acestea și informații cu privire la prelucrarea propriu-zisă.

[1] Trimiterile la „statele membre” din prezentul document trebuie înțelese ca trimiteri la „statele membre ale SEE”.
[2] Articolele 15-22 din RGPD.
[3] În temeiul articolului 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene, orice persoană are dreptul la protecția datelor cu caracter personal care o privesc. În temeiul articolului 8 alineatul (2) a doua teză, orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora.

De asemenea, persoana vizată poate obține o copie a datelor cu caracter personal prelucrate, această posibilitate nefiind un drept suplimentar al persoanei vizate, ci modalitatea de acordare a accesului la date. Astfel, dreptul de acces poate fi înțeles atât ca posibilitatea persoanei vizate de a întreba operatorul dacă sunt prelucrate date cu caracter personal care o privesc, cât și ca posibilitatea de a accesa și de a verifica aceste date. Operatorul furnizează persoanei vizate, pe baza cererii acesteia, informațiile care intră sub incidența articolului 15 alineatele (1) și (2) din RGPD.

4. Exercitarea dreptului de acces se realizează atât în cadrul legislației privind protecția datelor, în conformitate cu obiectivele legislației privind protecția datelor, cât și, mai precis, în cadrul „*drepturilor și libertăților fundamentale ale persoanelor fizice și în special a dreptului acestora la protecția datelor cu caracter personal*", astfel cum se prevede la articolul 1 alineatul (2) din RGPD. Dreptul de acces este un element important al întregului sistem de protecție a datelor.

5. Scopul practic al dreptului de acces este de a permite persoanelor fizice să dețină controlul asupra propriilor date cu caracter personal[4]. Pentru îndeplinirea acestui obiectiv în mod eficace în practică, RGPD urmărește să faciliteze această exercitare printr-o serie de garanții care permit persoanei vizate să își exercite acest drept cu ușurință, fără constrângeri inutile, la intervale rezonabile și fără întârzieri sau cheltuieli excesive. Toate acestea ar trebui să conducă la o aplicare mai eficace a dreptului de acces de către persoana vizată în era digitală, din care o parte, într-un sens mai larg, este, de asemenea, dreptul persoanei vizate de a depune o plângere la autoritatea de supraveghere și dreptul la protecție judiciară efectivă[5].

6. În ceea ce privește dezvoltarea dreptului de acces, ca parte a cadrului juridic privind protecția datelor, ar trebui subliniat faptul că acesta a fost un element al sistemului european de protecție a datelor încă de la început. În comparație cu Directiva 95/46/CE, standardul drepturilor persoanelor vizate prevăzut în RGPD a fost atât îmbunătățit, cât și consolidat; acest lucru este valabil și pentru dreptul de acces. Întrucât modalitățile de exercitare a dreptului de acces sunt în prezent specificate mai precis în RGPD, acest drept este, de asemenea, mai instructiv din punctul de vedere al securității juridice atât pentru persoana vizată, cât și pentru operator. În plus, formularea specifică a articolului 15 și termenul precis pentru furnizarea de date în temeiul articolului 12 alineatul (3) din RGPD îl obligă pe operator să fie pregătit pentru solicitările persoanelor vizate prin elaborarea de proceduri pentru tratarea cererilor.

7. Dreptul de acces nu ar trebui privit în mod izolat, deoarece este strâns legat de alte dispoziții ale RGPD, în special de principiile de protecție a datelor, inclusiv de echitatea și legalitatea prelucrării, de obligația de asigurare a transparenței de către operator și de alte drepturi ale persoanelor vizate prevăzute în capitolul III din RGPD.

8. În cadrul drepturilor persoanelor vizate, este, de asemenea, important să se sublinieze atât importanța articolului 12 din RGPD, care stabilește cerințe privind măsurile adecvate adoptate de operator pentru furnizarea informațiilor menționate la articolele 13 și 14 din RGPD, cât și comunicările menționate la articolele 15-22 și 34 din RGPD; aceste cerințe specifică, în general, forma, modalitatea și termenul pentru răspunsurile adresate persoanei vizate și, în special, pentru orice informație adresată copilului.

9. CEPD consideră că este necesar să se ofere orientări mai precise cu privire la modul în care trebuie pus în aplicare dreptul de acces în diferite situații. Prezentele orientări au ca scop analizarea diferitelor aspecte ale dreptului de acces. Mai precis, secțiunea de mai jos este menită să ofere o imagine de ansamblu și o explicație a conținutului articolului 15 în sine, în timp ce secțiunile următoare oferă o

[4] A se vedea considerentele 7, 68, 75 și 85 din RGPD.

[5] A se vedea capitolul VIII articolele 77, 78 și 79 din RGPD.

analiză mai aprofundată a celor mai frecvente întrebări și aspecte practice legate de punerea în aplicare a dreptului de acces.

2 SCOPUL DREPTULUI DE ACCES, STRUCTURA ARTICOLULUI 15 DIN RGPD ȘI PRINCIPII GENERALE

2.1 Scopul dreptului de acces

10. Dreptul de acces este conceput astfel încât să permită oricărei persoane fizice să aibă control asupra datelor cu caracter personal care o privesc *„pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia”*[6]. Mai precis, scopul dreptului de acces este de a permite persoanelor vizate să înțeleagă modul în care sunt prelucrate datele lor cu caracter personal, precum și consecințele unei astfel de prelucrări, și să verifice exactitatea datelor prelucrate fără a trebui să își justifice intenția. Cu alte cuvinte, scopul dreptului de acces este de a oferi persoanelor fizice informații suficiente, transparente și ușor accesibile cu privire la prelucrarea datelor, indiferent de tehnologiile utilizate, și de a le permite să verifice diferite aspecte ale unei anumite activități de prelucrare în temeiul RGPD (de exemplu, legalitatea, exactitatea).

11. Interpretarea RGPD furnizată în prezentele orientări se bazează pe jurisprudența CJUE care a fost pronunțată până în prezent. Având în vedere importanța dreptului de acces, este de așteptat ca jurisprudența aferentă să evolueze semnificativ în viitor.

12. În conformitate cu hotărârile CJUE[7], dreptul de acces servește scopului de a asigura protecția dreptului persoanelor vizate la viață privată și la protecția datelor în ceea ce privește prelucrarea datelor care le privesc[8] și poate facilita exercitarea drepturilor lor care decurg, de exemplu, din articolele 16-19, 21-22 și 82 din RGPD. Cu toate acestea, exercitarea dreptului de acces este un drept al unei persoane fizice și nu este condiționată de exercitarea acestor alte drepturi, iar exercitarea altor drepturi nu depinde de exercitarea dreptului de acces.

13. Având în vedere scopul amplu al dreptului de acces, acesta nu este adecvat pentru a fi analizat ca o condiție prealabilă a exercitării dreptului de acces de către operator în cadrul evaluării cererilor de acces. Astfel, operatorii nu ar trebui să evalueze „de ce” persoana vizată solicită acces, ci doar „ce” solicită persoana vizată (a se vedea secțiunea 3 privind analiza cererii) și dacă dețin date cu caracter personal referitoare la persoana respectivă (a se vedea secțiunea 4). Prin urmare, de exemplu, operatorul nu ar trebui să refuze accesul pe baza motivelor sau a suspiciunii că datele solicitate ar putea fi utilizate de persoana vizată pentru a se apăra în instanță în cazul unei concedieri sau al unui litigiu comercial cu operatorul[9]. În ceea ce privește limitările și restricțiile dreptului de acces, a se vedea secțiunea 6.

Exemplul 1: un angajator a concediat o persoană. O săptămână mai târziu, persoana decide să colecteze probe pentru a introduce o acțiune în justiție împotriva acestui fost angajator pentru concediere abuzivă. Din această perspectivă, persoana respectivă îi scrie fostului angajator solicitând accesul la toate datele cu caracter personal care o privesc, în calitate de persoană vizată, pe care fostul angajator, în calitate de operator, le prelucrează.

Operatorul nu analizează intenția persoanei vizate, iar persoana vizată nu trebuie să furnizeze operatorului motivul cererii. Prin urmare, dacă cererea îndeplinește toate celelalte cerințe (a se vedea

[6] Considerentul 63 din RGPD.
[7] CJUE, C-434/16, Nowak, și cauzele conexate C-141/12 și C-372/12, YS și alții.
[8] CJUE, C-434/16, Nowak, punctul 56.
[9] Întrebări referitoare la acest subiect sunt în discuție într-o cauză aflată în prezent pe rolul CJUE (C-307/22).

secțiunea 3), operatorul trebuie să dea curs cererii, cu excepția cazului în care cererea se dovedește a fi în mod vădit nefondată sau excesivă în conformitate cu articolul 12 alineatul (5) din RGPD (a se vedea secțiunea 6.3), aspect care trebuie demonstrat de operator.

Variantă: persoana vizată își exercită dreptul de acces la datele cu caracter personal care o privesc pe parcursul procesului. Cu toate acestea, dreptul intern al statului membru, care reglementează raportul de muncă dintre operator și persoana vizată, conține anumite dispoziții care limitează domeniul de aplicare al informațiilor care trebuie furnizate părților la procedurile judiciare în curs sau viitoare sau schimbate între acestea, care sunt aplicabile în cazul procesului de concediere abuzivă introdus de persoana vizată. În acest context și cu condiția ca aceste dispoziții naționale să respecte cerințele prevăzute la articolul 23 din RGPD[10], persoana vizată nu are dreptul de a primi de la operator mai multe informații decât cele prevăzute de dispozițiile dreptului intern al statului membru care reglementează schimbul de informații între părțile la litigiile juridice.

14. Deși scopul dreptului de acces este larg, CJUE a ilustrat, de asemenea, limitele domeniului de aplicare al legislației privind protecția datelor și al dreptului de acces. De exemplu, CJUE a constatat că trebuie să se facă o distincție între obiectivul dreptului de acces garantat de dreptul UE în materie de protecție a datelor și obiectivul dreptului de acces la documente publice instituit de legislația UE și de cea națională, care vizează să asigure „transparența procesului decizional al autorităților publice și să promoveze bunele practici administrative”[11], obiectiv care nu este urmărit de dreptul în materie de protecție a datelor. CJUE a concluzionat că dreptul de acces la datele cu caracter personal se aplică indiferent dacă se aplică sau nu un alt tip de drept de acces cu un scop diferit, cum ar fi în contextul unei proceduri de examinare.

2.2 Structura articolului 15 din RGPD

15. Pentru a răspunde unei cereri de acces și pentru a se asigura că niciunul dintre aspectele sale nu poate fi ignorat, este necesar să se înțeleagă mai întâi structura articolului 15 și componentele dreptului de acces prevăzute la acest articol.

16. Articolul 15 poate fi defalcat în opt elemente diferite, astfel cum sunt enumerate în tabelul de mai jos:

1.	O confirmare că operatorul prelucrează sau nu date cu caracter personal care privesc persoana solicitantă	Articolul 15 alineatul (1) prima jumătate a tezei
2.	Accesul la datele cu caracter personal ale persoanei solicitante	Articolul 15 alineatul (1) a doua jumătate a tezei (prima parte)
3.	Accesul la următoarele informații privind prelucrarea: (a) scopurile prelucrării; (b) categoriile de date cu caracter personal; (c) destinatarii sau categoriile de destinatari ai datelor; (d) durata preconizată a prelucrării sau criteriile de stabilire a duratei; (e) existența dreptului de rectificare, de ștergere, de restricționare a prelucrării și de a se opune prelucrării;	Articolul 15 alineatul (1) a doua jumătate a tezei (a doua parte)

[10] Orientările CEPD 10/2020 privind restricțiile în temeiul articolului 23 din RGPD, versiunea pentru consultare publică, 18 decembrie 2020.
[11] CJUE, cauzele conexate C-141/12 și C-372/12, YS și alții, punctul 47.

	(f) dreptul de a depune o plângere în fața unei autorități de supraveghere; (g) în cazul în care datele nu sunt colectate de la persoana vizată, orice informație disponibilă privind sursa acestora; (h) existența unui proces decizional automatizat, incluzând crearea de profiluri și alte informații legate de acesta.	
4.	Informații privind garanțiile în temeiul articolului 46 în cazul în care datele cu caracter personal sunt transferate către o țară terță sau către o organizație internațională	Articolul 15 alineatul (2)
5.	Obligația operatorului de a furniza o copie a datelor cu caracter personal care fac obiectul prelucrării	Articolul 15 alineatul (3) prima teză
6.	Perceperea de către operator a unei taxe rezonabile, bazată pe costurile administrative, pentru oricare alte copii solicitate de persoana vizată	Articolul 15 alineatul (3) a doua teză
7.	Furnizarea de informații în format electronic	Articolul 15 alineatul (3) a treia teză
8.	Luarea în considerare a drepturilor și libertăților altora	Articolul 15 alineatul (4)

În timp ce toate elementele de la articolul 15 alineatele (1) și (2) definesc împreună conținutul dreptului de acces, articolul 15 alineatul (3) se referă la modalitățile de acces, în plus față de cerințele generale prevăzute la articolul 12 din RGPD. Articolul 15 alineatul (4) completează limitările și restricțiile pe care articolul 12 alineatul (5) din RGPD le prevede pentru toate drepturile persoanelor vizate, cu un accent specific pe drepturile și libertățile altora în contextul accesului.

2.2.1 Definirea conținutului dreptului de acces

17. Articolul 15 alineatele (1) și (2) conține următoarele trei aspecte: în primul rând, o confirmare că se prelucrează sau nu date cu caracter personal ale persoanei solicitante și, în caz afirmativ, în al doilea rând, accesul la aceste date și, în al treilea rând, informații privind prelucrarea. Acestea pot fi considerate trei componente diferite care, împreună, alcătuiesc dreptul de acces.

2.2.1.1 Confirmarea că „se prelucrează sau nu” date cu caracter personal

18. Atunci când formulează o cerere de acces la datele cu caracter personal, primul lucru pe care persoanele vizate trebuie să îl cunoască este dacă operatorul prelucrează sau nu date care le privesc. În consecință, aceste informații constituie prima componentă a dreptului de acces în temeiul articolului 15 alineatul (1). În cazul în care operatorul nu prelucrează date cu caracter personal referitoare la persoana vizată care solicită accesul, informațiile care trebuie furnizate ar fi limitate la o confirmare că nu se prelucrează date cu caracter personal referitoare la persoana vizată. În cazul în care operatorul prelucrează date referitoare la persoana solicitantă, acesta trebuie să confirme acest fapt persoanei respective. Această confirmare poate fi comunicată separat sau poate fi inclusă ca parte a informațiilor privind datele cu caracter personal prelucrate (a se vedea mai jos).

2.2.1.2 Accesul la datele cu caracter personal prelucrate

19. Accesul la datele cu caracter personal este a doua componentă a dreptului de acces în temeiul articolului 15 alineatul (1) și constituie esența acestui drept. Acesta se referă la noțiunea de „date cu caracter personal”, astfel cum este definită la articolul 4 punctul 1 din RGPD. Pe lângă datele cu caracter personal de bază, cum ar fi numele și adresa, există o variate nelimitată de date care s-ar

putea încadra în această definiție, cu condiția să intre sub incidența domeniului de aplicare material al RGPD, în special în ceea ce privește modul în care sunt prelucrate (articolul 2 din RGPD). În cazul de față, accesul la date cu caracter personal înseamnă accesul la datele cu caracter personal propriu-zise, nu numai o descriere generală a datelor, nici o simplă trimitere la categoriile de date cu caracter personal prelucrate de operator. În cazul în care nu se aplică limitări sau restricții[12], persoanele vizate au dreptul de a avea acces la toate datele sau la părți ale datelor prelucrate care le privesc, în funcție de domeniul de aplicare al cererii (a se vedea subsecțiunea 2.3.1). Obligația de a acorda acces la date nu depinde de tipul sau sursa acestor date. Această obligație se aplică pe deplin chiar și în cazurile în care persoana solicitantă a furnizat inițial operatorului datele, deoarece scopul său este de a permite informarea persoanei vizate cu privire la prelucrarea efectivă a respectivelor date de către operator. Domeniul de aplicare al datelor cu caracter personal în temeiul articolului 15 este explicat în detaliu în secțiunile 4.1 și 4.2.

2.2.1.3 Informații privind prelucrarea și drepturile persoanelor vizate

20. Cea de a treia componentă a dreptului de acces este reprezentată de informațiile privind prelucrarea și drepturile persoanelor vizate pe care operatorul trebuie să le furnizeze în temeiul articolului 15 alineatul (1) literele (a)-(h) și al articolului 15 alineatul (2). Astfel de informații s-ar putea baza pe textul preluat, de exemplu, din declarația de confidențialitate a operatorului[13] sau din evidențele operatorului privind activitățile de prelucrare menționate la articolul 30 din RGPD, dar ar putea fi necesar ca acestea să fie actualizate și adaptate la cererea persoanei vizate. Conținutul și gradul de detaliere al informațiilor sunt prezentate în secțiunea 4.3.

2.2.2 Dispoziții privind modalitățile

21. Articolul 15 alineatul (3) completează cerințele privind modalitățile de răspuns la cererile de acces prevăzute la articolul 12 din RGPD cu anumite specificații în contextul cererilor de acces.

2.2.2.1 Furnizarea unei copii

22. În temeiul articolului 15 alineatul (3) prima teză din RGPD, operatorul furnizează o copie gratuită a datelor cu caracter personal care fac obiectul prelucrării. Prin urmare, copia se referă numai la a doua componentă a dreptului de acces („accesul la datele cu caracter personal prelucrate”; a se vedea mai sus). Operatorul trebuie să se asigure că prima copie este gratuită, chiar și în cazul în care consideră că reproducerea are un cost ridicat (de exemplu: costul furnizării unei copii a înregistrării unei conversații telefonice).

23. Obligația de a furniza o copie nu trebuie înțeleasă ca un drept suplimentar al persoanei vizate, ci ca o modalitate de a oferi acces la date. Aceasta consolidează dreptul de acces la date[14] și contribuie la interpretarea acestui drept întrucât clarifică faptul că accesul la date în temeiul articolului 15 alineatul (1) cuprinde informații complete cu privire la toate datele și nu poate fi înțeles ca furnizare doar a unui rezumat al datelor. În același timp, obligația de a furniza o copie nu este concepută pentru a extinde domeniul de aplicare al dreptului de acces: aceasta se referă (numai) la o copie a datelor cu caracter personal care fac obiectul prelucrării, nu neapărat la o reproducere a documentelor originale

[12] A se vedea secțiunea 6 din prezentele orientări.
[13] Pentru informații cu privire la Grupul de lucru „Articolul 29”, GL260 rev.01, 11 aprilie 2018, Orientări privind transparența în temeiul Regulamentului 2016/679 – aprobate de CEPD (denumite în continuare „Orientările GL29 privind transparența – aprobate de CEPD”).
[14] Obligația de a furniza o copie nu a fost menționată în Directiva 95/46/CE privind protecția datelor.

(a se vedea secțiunea 5 punctul 152). La un nivel mai general, nu există informații suplimentare care să fie furnizate persoanei vizate în momentul furnizării unei copii: domeniul de aplicare al informațiilor care urmează să fie incluse în copie coincide cu domeniul de aplicare al accesului la date conform articolului 15 alineatul (1) (a doua componentă a dreptului de acces menționat mai sus, a se vedea punctul 19), care include toate informațiile necesare pentru a permite persoanei vizate să înțeleagă și să verifice legalitatea prelucrării[15].

24. Având în vedere cele de mai sus, în cazul în care accesul la date în sensul articolului 15 alineatul (1) este acordat prin furnizarea unei copii, se respectă obligația de a furniza o copie menționată la articolul 15 alineatul (3). Obligația de a furniza o copie servește obiectivelor dreptului de acces de a permite persoanei vizate să fie informată cu privire la prelucrare și să verifice legalitatea acesteia (considerentul 63). Pentru atingerea acestor obiective, persoana vizată va trebui, în majoritatea cazurilor, să vadă informațiile nu numai temporar. Prin urmare, persoana vizată va trebui să obțină acces la informații prin primirea unei copii a datelor cu caracter personal.

25. Având în vedere cele de mai sus, noțiunea de copie trebuie interpretată în sens larg și include diferitele tipuri de acces la datele cu caracter personal atât timp cât sunt complete (adică includ toate datele cu caracter personal solicitate) și pot fi păstrate de persoana vizată. Astfel, cerința de a furniza o copie implică faptul că informațiile privind datele cu caracter personal referitoare la persoana care înaintează cererea sunt furnizate persoanei vizate într-un mod care permite acesteia să păstreze toate informațiile și să le consulte în orice moment.

26. În pofida acestei înțelegeri largi a ceea ce înseamnă o copie și având în vedere că aceasta este principala modalitate prin care ar trebui acordat accesul, în anumite circumstanțe ar putea fi adecvate alte modalități. Explicații suplimentare privind copiile și alte modalități de acordare a accesului sunt furnizate în secțiunea 5, în special în subsecțiunile 5.2.2-5.2.5.

2.2.2.2 Furnizarea altor copii

27. Articolul 15 alineatul (3) a doua teză se referă la situațiile în care persoana vizată solicită operatorului mai multe copii, de exemplu în cazul în care prima copie a fost pierdută sau deteriorată ori în cazul în care persoana vizată dorește să transmită o copie unei alte persoane sau unei autorități de supraveghere. Pe baza obligației operatorului de a furniza alte copii la cererea persoanei vizate, articolul 15 alineatul (3) prevede că, pentru orice altă copie solicitată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative [articolul 15 alineatul (3) a doua teză].

28. În cazul în care persoana vizată solicită o copie suplimentară după înaintarea primei cereri, se poate pune întrebarea dacă aceasta ar trebui considerată o cerere nouă sau dacă persoana vizată dorește o copie suplimentară a datelor în sensul articolului 15 alineatul (3) a doua teză, caz în care se poate percepe o taxă pentru o copie suplimentară. Răspunsul la aceste întrebări depinde exclusiv de conținutul cererii: cererea ar trebui interpretată ca solicitând o copie suplimentară, în măsura în care, în ceea ce privește momentul și domeniul de aplicare, se referă la aceeași prelucrare a datelor cu caracter personal ca și cererea anterioară. Cu toate acestea, în cazul în care persoana vizată urmărește să obțină informații cu privire la datele prelucrate la un alt moment sau referitoare la un set diferit de date decât cele solicitate inițial, dreptul de a obține o copie gratuită în conformitate cu articolul 15 alineatul (3) se aplică din nou. Acest lucru este valabil și în cazurile în care persoana vizată a formulat o primă cerere cu puțin timp înainte. O persoană vizată își poate exercita dreptul de acces printr-o

[15] Întrebări referitoare la subiectul acestui alineat sunt în discuție într-o cauză aflată în prezent pe rolul CJUE (C-487/21).

cerere ulterioară și poate obține o copie gratuită, cu excepția cazului în care cererea este considerată excesivă în temeiul articolului 12 alineatul (5), cu posibilitatea de a se percepe o taxă rezonabilă în conformitate cu articolul 12 alineatul (5) litera (a) (privind caracterul excesiv al cererilor repetitive, a se vedea secțiunea 6).

Exemplul 2: un client transmite o cerere de acces unei societăți comerciale. La un an de la răspunsul societății, același client adresează aceleiași societăți o cerere de acces în temeiul articolului 15. Indiferent dacă au existat tranzacții comerciale noi sau alte contacte între părți de la cererea anterioară, această a doua cerere trebuie considerată o cerere nouă. Chiar dacă nu există nicio modificare în prelucrarea datelor de către societate – ceea ce nu este neapărat evident pentru persoana vizată – persoana vizată are dreptul de a obține o copie gratuită a datelor.

Varianta 1: chiar dacă, în cazurile de mai sus, clientul depune cererea nouă, de exemplu, la doar o săptămână de la prima cerere, aceasta poate fi considerată o cerere nouă în temeiul articolului 15 alineatul (1) și al articolului 15 alineatul (3) prima teză, dacă nu trebuie interpretată ca simplu mesaj de reamintire cu privire la prima cerere. În ceea ce privește intervalul scurt și în funcție de circumstanțele specifice ale noii cereri, intră în discuție caracterul său excesiv în conformitate cu articolul 12 alineatul (5) (a se vedea secțiunea 6).

Varianta 2: solicitarea unei „copii noi” a informațiilor care au fost deja furnizate sub forma unei copii ca răspuns la o cerere anterioară, de exemplu în cazul în care clientul a pierdut copia primită anterior, ar trebui să fie considerată, în mod normal, o cerere pentru o copie suplimentară, deoarece se referă la cererea anterioară în ceea ce privește domeniul de aplicare și momentul prelucrării.

29. În cazul în care persoana vizată repetă o primă cerere de acces pe motiv că răspunsul primit nu a fost complet sau că refuzul nu a fost motivat, această cerere nu trebuie considerată ca fiind o cerere nouă, deoarece reprezintă doar un mesaj de reamintire cu privire la prima cerere căreia nu i s-a dat curs.

30. În ceea ce privește alocarea costurilor în cazul cererilor pentru o copie suplimentară, articolul 15 alineatul (3) prevede că operatorul poate percepe o taxă rezonabilă bazată pe costurile administrative generate de cerere. Aceasta înseamnă că costurile administrative reprezintă un criteriu relevant pentru stabilirea nivelului taxei. În același timp, taxa ar trebui să fie adecvată, ținând seama de importanța dreptului de acces ca drept fundamental al persoanei vizate. Operatorul nu ar trebui să transfere persoanei vizate costurile generale sau alte cheltuieli generale, ci ar trebui să se concentreze asupra costurilor specifice generate de furnizarea copiei suplimentare. Atunci când organizează acest proces, operatorul ar trebui să își utilizeze resursele umane și materiale în mod eficient pentru a menține costurile copiei la un nivel scăzut, inclusiv în cazul în care operatorul implică sprijin extern.

31. În cazul în care decide să perceapă o taxă, operatorul ar trebui să indice în avans că se va percepe o taxă și – cât mai exact posibil – cuantumul costurilor pe care intenționează să le perceapă de la persoana vizată pentru a oferi acesteia posibilitatea de a stabili dacă să mențină sau să retragă cererea.

2.2.2.3 Punerea la dispoziție a informațiilor într-un format electronic utilizat în mod curent

32. În cazul unei cereri transmise în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil și cu excepția cazului în care persoana vizată solicită un alt format [a se vedea articolul 12 alineatul (3) din RGPD]. Articolul 15 alineatul (3) a treia teză completează această cerință în contextul cererilor de acces, precizând că, în plus, operatorul este obligat să furnizeze răspunsul într-un format electronic utilizat în mod curent, cu excepția cazului în care persoana vizată solicită un alt format. Articolul 15 alineatul (3) presupune că, în cazul operatorilor care sunt în măsură să primească cereri în format electronic, va fi posibilă furnizarea răspunsului la cerere într-un format electronic

utilizat în mod curent (pentru detalii, a se vedea subsecțiunea 5.2.5). Această dispoziție se referă la toate informațiile care trebuie furnizate în conformitate cu articolul 15 alineatele (1) și (2). Prin urmare, în cazul în care persoana vizată transmite cererea de acces în format electronic, toate informațiile trebuie furnizate într-un format electronic utilizat în mod curent. Întrebările privind formatul sunt prezentate în detaliu în secțiunea 5. Operatorul ar trebui, ca întotdeauna, să pună în aplicare măsuri de securitate adecvate, în special atunci când tratează categorii speciale de date cu caracter personal (a se vedea mai jos, subsecțiunea 2.3.4).

2.2.3 Posibila limitare a dreptului de acces

33. În cele din urmă, în contextul dreptului de acces, la articolul 15 alineatul (4) este prevăzută o limitare specifică. Aceasta prevede că trebuie să se țină seama de posibilitatea de a aduce atingere drepturilor și libertăților altora. Întrebările privind domeniul de aplicare și consecințele acestei limitări, precum și limitările și restricțiile suplimentare prevăzute la articolul 12 alineatul (5) sau la articolul 23 din RGPD sunt explicate în secțiunea 6.

2.3 Principii generale ale dreptului de acces

34. Atunci când persoanele vizate depun o cerere de acces la datele lor, în principiu, informațiile menționate la articolul 15 din RGPD trebuie să fie întotdeauna furnizate integral. În consecință, în cazul în care prelucrează date referitoare la persoana vizată, operatorul furnizează toate informațiile menționate la articolul 15 alineatul (1) și, după caz, informațiile menționate la articolul 15 alineatul (2). Operatorul trebuie să ia măsurile adecvate pentru a se asigura că informațiile sunt complete, corecte și actualizate și corespund cât mai bine posibil cu stadiul prelucrării datelor la momentul primirii cererii[16]. În cazul în care doi sau mai mulți operatori prelucrează date în comun, acordul operatorilor asociați cu privire la responsabilitățile care le revin în ceea ce privește exercitarea drepturilor persoanei vizate, în special în ceea ce privește răspunsul la cererile de acces, nu aduce atingere drepturilor persoanelor vizate în raport cu operatorul căruia îi adresează cererea[17].

2.3.1 Caracterul complet al informațiilor

35. Persoanele vizate au dreptul de a obține, cu excepțiile menționate mai jos, comunicarea integrală a tuturor datelor care le privesc (pentru detalii privind domeniul de aplicare, a se vedea secțiunea 4.2). Cu excepția cazului în care persoana vizată solicită în mod explicit altceva, o cerere de exercitare a dreptului de acces se interpretează în termeni generali, și anume cuprinzând toate datele cu caracter personal referitoare la persoana vizată[18]. Limitarea accesului la o parte din informații poate fi luată în considerare în următoarele cazuri:

a) Persoana vizată a limitat în mod explicit cererea la un subset de date. Pentru a se evita furnizarea de informații incomplete, operatorul poate lua în considerare această limitare a cererii persoanei vizate numai dacă poate fi sigur că această interpretare corespunde dorinței persoanei vizate (pentru detalii suplimentare, a se vedea subsecțiunea 3.1.1 punctul 51). În principiu, persoana vizată nu trebuie să repete cererea de transmitere a tuturor datelor pe care are dreptul să le obțină.

[16] Pentru orientări privind măsurile adecvate, a se vedea secțiunea 5 punctele 123-129.
[17] Orientările CEPD 07/2020 privind conceptele de operator și persoană împuternicită de operator în cadrul RGPD, punctul 162f. Persoanele împuternicite de operator trebuie să acorde asistență operatorului, ibidem, punctul 129.
[18] Pentru detalii, a se vedea subsecțiunea 5.2.3 de mai jos cu privire la abordarea pe mai multe niveluri.

b) În situațiile în care prelucrează un volum mare de date referitoare la persoana vizată, operatorul poate avea îndoieli cu privire la faptul că o cerere de acces, care este formulată în termeni foarte generali, vizează într-adevăr obținerea de informații cu privire la toate tipurile de date prelucrate sau la toate ramurile de activitate ale operatorului în detaliu. Aceste îndoieli pot apărea în special atunci când nu a existat nicio posibilitate de a pune la dispoziția persoanei vizate instrumente pentru a furniza precizări cu privire la cererea sa de la început sau în care persoana vizată nu le-a utilizat. Operatorul se confruntă apoi cu probleme legate de modalitatea de a oferi un răspuns complet, evitând în același timp apariția unui exces de informații pentru persoana vizată, de care persoana vizată nu este interesată și pe care nu le poate trata în mod eficace. Pot exista modalități de soluționare a acestei probleme, în funcție de circumstanțe și de posibilitățile tehnice, de exemplu prin furnizarea de instrumente de *self-service* în contexte online (a se vedea secțiunea 5 privind abordarea pe mai multe niveluri). Dacă astfel de soluții nu sunt aplicabile, un operator care prelucrează un volum mare de informații privind persoana vizată poate solicita ca, înainte de a îi fi furnizate informațiile, persoana vizată să precizeze informațiile sau activitățile de prelucrare la care se referă cererea sa (a se vedea considerentul 63 din RGPD). Exemple în acest sens pot include o societate cu mai multe domenii de activitate sau o autoritate publică cu unități administrative diferite, în cazul în care operatorul constată că numeroase date referitoare la persoana vizată sunt prelucrate în sucursalele respective. În plus, un volum mare de date poate fi prelucrat de operatori care colectează date privind activitățile frecvente ale persoanei vizate pe o perioadă îndelungată.

Exemplul 3: o autoritate publică prelucrează date privind persoana vizată în cadrul mai multor departamente diferite, în contexte diferite. Gestionarea și păstrarea dosarelor se realizează parțial prin mijloace neautomatizate, iar majoritatea datelor sunt stocate numai în dosare pe suport de hârtie. În ceea ce privește formularea generală a cererii, autoritatea publică se îndoiește că persoana vizată cunoaște amploarea cererii, în special varietatea operațiunilor de prelucrare pe care le-ar include, volumul de informații și numărul de pagini pe care persoana vizată le-ar primi.

Exemplul 4: o societate de asigurări de mari dimensiuni primește o cerere de acces general printr-o scrisoare din partea unei persoane care este client de mulți ani. Chiar dacă termenele de ștergere sunt pe deplin respectate, societatea prelucrează efectiv un volum mare de date referitoare la client, deoarece prelucrarea este în continuare necesară pentru îndeplinirea obligațiilor contractuale care decurg din relația contractuală cu clientul (inclusiv, de exemplu, obligațiile continue, comunicarea privind aspectele controversate cu clientul și cu terții etc.) sau pentru respectarea obligațiilor legale (date arhivate care trebuie stocate în scopuri fiscale etc.). Societatea de asigurări poate avea îndoieli în a ști dacă cererea, formulată în termeni foarte generali, este într-adevăr destinată includerii tuturor tipurilor de date respective. Acest aspect poate fi problematic în special în cazul în care societatea de asigurări are doar o adresă poștală a persoanei vizate și, prin urmare, trebuie să trimită orice informație pe suport de hârtie. Totuși, aceleași îndoieli pot fi relevante și atunci când se furnizează informațiile prin alte mijloace.

Dacă, în astfel de cazuri, operatorul decide să solicite persoanei vizate să furnizeze precizări cu privire la cerere, pentru a-și îndeplini obligația de a facilita exercitarea dreptului de acces [articolul 12 alineatul (2) din RGPD], operatorul furnizează în același timp informații semnificative cu privire la operațiunile sale de prelucrare a datelor care ar putea să privească persoana vizată, informând-o cu privire la sectoarele relevante ale activităților sale, bazele sale de date etc.

Exemplul 5: în cadrul unui raport de muncă, în cazul unei cereri de acces formulate în termeni generali, nu este clar *per se* că angajatul dorește să primească toate datele de autentificare a utilizatorului, datele privind accesul la un loc de muncă, datele privind aranjamentele legate de cantină, datele

privind salariul etc. O cerere de furnizare de precizări formulată de angajator ar putea, de exemplu, să clarifice faptul că interesul angajatului este de a înțelege sau de a verifica cui i-a fost transmisă evaluarea performanței. Fără o cerere de precizări, angajatul ar primi un volum mare de informații, fără a avea un interes pentru majoritatea datelor. În același timp, angajatorul ar trebui să furnizeze informații cu privire la diferitele contexte de prelucrare care l-ar putea viza pe angajat, pentru a permite acestuia să furnizeze precizări cu privire la cerere în mod rezonabil.

Este important de subliniat faptul că cererea de furnizare de precizări nu vizează o limitare a răspunsului la cererea de acces și nu poate fi utilizată pentru a ascunde nicio informație privind datele sau prelucrarea referitoare la persoana vizată. În cazul în care persoana vizată, căreia i s-a solicitat să precizeze domeniul de aplicare al cererii sale, confirmă că dorește toate datele cu caracter personal care o privesc, operatorul trebuie, desigur, să i le furnizeze integral.

În orice caz, operatorul ar trebui să fie întotdeauna în măsură să demonstreze că modul în care tratează cererea urmărește să confere cel mai larg efect dreptului de acces și că este în conformitate cu obligația sa de a facilita exercitarea drepturilor persoanelor vizate [articolul 12 alineatul (2) din RGPD]. Sub rezerva acestor principii, operatorul poate aștepta răspunsul persoanei vizate înainte de a furniza date suplimentare în funcție de dorința acesteia, dacă operatorul a furnizat persoanei vizate o imagine de ansamblu clară a tuturor operațiunilor de prelucrare a datelor care ar putea să o vizeze, în special a celor la care persoana vizată ar fi putut să nu se aștepte, dacă operatorul a acordat, de asemenea, acces la toate datele pe care persoana vizată le-a vizat în mod clar și dacă, în plus, aceste informații au fost combinate cu indicații clare privind modul în care se poate obține accesul la celelalte părți ale datelor prelucrate.

c) Se aplică excepții sau restricții de la dreptul de acces (a se vedea secțiunea 6 de mai jos). În astfel de cazuri, operatorul ar trebui să verifice cu atenție la ce părți din informații se referă excepția și să furnizeze toate informațiile care nu sunt excluse de excepție. De exemplu, confirmarea prelucrării datelor cu caracter personal în sine (componenta 1) nu poate fi afectată de excepție. Prin urmare, trebuie furnizate informații cu privire la toate datele cu caracter personal și toate informațiile menționate la articolul 15 alineatele (1) și (2) care nu sunt vizate de excepție sau de restricție.

2.3.2 Corectitudinea informațiilor

36. Informațiile incluse în copia datelor cu caracter personal furnizate persoanei vizate trebuie să cuprindă informațiile sau datele cu caracter personal deținute efectiv cu privire la persoana vizată. Acestea includ obligația de a furniza informații cu privire la datele care sunt inexacte sau cu privire la prelucrarea de date care nu este sau nu mai este legală. De exemplu, persoana vizată poate utiliza dreptul de acces pentru a afla sursa datelor inexacte care circulă între diferiți operatori. În cazul în care operatorul corectează date inexacte înainte de a informa în acest sens persoana vizată, aceasta din urmă ar fi privată de o astfel de posibilitate. Același lucru este valabil și în cazul prelucrării ilegale. Posibilitatea persoanei vizate de a afla informații despre prelucrarea ilegală a unor date care o privesc este unul dintre scopurile principale ale dreptului de acces. Obligația de a informa cu privire la nemodificarea stadiului prelucrării nu aduce atingere obligației operatorului de a pune capăt prelucrării ilegale sau de a corecta datele inexacte. În continuare sunt prezentate răspunsuri la întrebările referitoare la ordinea în care ar trebui îndeplinite aceste obligații.

2.3.3 Momentul de referință al evaluării

37. Evaluarea datelor prelucrate trebuie să reflecte cât mai bine posibil situația în care operatorul primește cererea, iar răspunsul ar trebui să acopere toate datele disponibile la momentul respectiv. Aceasta

înseamnă că operatorul trebuie să încerce să afle, fără întârzieri nejustificate, informații cu privire la toate activitățile de prelucrare a datelor referitoare la persoana vizată. Prin urmare, operatorii nu sunt obligați să furnizeze date cu caracter personal pe care le-au prelucrat în trecut, dar pe care nu le mai au la dispoziție[19]. De exemplu, este posibil ca operatorul să fi șters date cu caracter personal în conformitate cu politica sa de păstrare a datelor și/sau cu dispozițiile sale statutare și, prin urmare, să nu mai fie în măsură să furnizeze datele cu caracter personal solicitate. În acest context, ar trebui reamintit faptul că perioada de stocare a datelor ar trebui să fie stabilită în conformitate cu articolul 5 alineatul (1) litera (e) din RGPD, întrucât orice păstrare a datelor trebuie să fie justificată în mod obiectiv.

38. În același timp, operatorul pune în aplicare în prealabil măsurile necesare pentru a facilita exercitarea dreptului de acces și pentru a da curs acestor cereri cât mai curând posibil [a se vedea articolul 12 alineatul (3)] și înainte ca datele să fie șterse. Prin urmare, în cazul unor perioade scurte de păstrare, măsurile luate pentru a răspunde cererii ar trebui adaptate la perioada de păstrare adecvată pentru a facilita exercitarea dreptului de acces și pentru a evita imposibilitatea permanentă de a oferi acces la datele prelucrate în momentul formulării cererii[20]. Cu toate acestea, în unele cazuri s-ar putea să nu fie posibil să se răspundă la o cerere înainte de data la care este programată ștergerea datelor. De exemplu, în cazul în care, în cursul oferirii unui răspuns la o cerere cât mai rapid posibil, un operator extrage date cu caracter personal care au fost programate să fie șterse în ziua următoare, operatorul poate avea nevoie de un timp suplimentar pentru a analiza dacă este necesar să cenzureze anumite date pentru a proteja libertățile altora înainte de a elibera solicitantului o copie a datelor cu caracter personal. În cazul în care datele au fost extrase în cursul perioadei de păstrare programate, operatorul poate continua să prelucreze datele respective în scopul îndeplinirii obligației sale de a răspunde cererii. Prelucrarea în astfel de cazuri se poate întemeia pe articolul 6 alineatul (1) litera (c) coroborat cu articolul 15 din RGPD, iar durata sa trebuie să respecte cerințele de la articolul 12 alineatul (3) din RGPD[21]. Aplicarea acestui temei juridic se limitează la prelucrarea datelor identificate ca fiind necesare pentru a răspunde la cererea concretă și nu trebuie utilizată ca justificare pentru prelungirile generale ale perioadelor de păstrare.

39. În plus, operatorul nu se sustrage în mod deliberat obligației de a furniza datele cu caracter personal solicitate prin ștergerea sau modificarea datelor cu caracter personal ca răspuns la o cerere de acces (a se vedea subsecțiunea 2.3.2). În cazul în care, în cursul prelucrării cererii de acces, operatorul descoperă date inexacte sau o prelucrare ilegală, acesta trebuie să evalueze stadiul prelucrării și să informeze persoana vizată în consecință înainte de a-și respecta celelalte obligații. În interesul propriu, pentru a evita necesitatea unor comunicări suplimentare în acest sens, precum și pentru a respecta principiul transparenței, operatorul ar trebui să adauge informații cu privire la rectificările sau eliminările ulterioare.

---

[19] A se vedea, în acest sens, clarificările suplimentare din secțiunea 4 din prezentele orientări, precum și hotărârea Curții de Justiție a Uniunii Europene în cauza C-553/07, 7 mai 2009, College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer, cu privire la acordarea pentru trecut a dreptului de acces la informațiile referitoare la destinatarii sau categoriile de destinatari ai datelor.

[20] De exemplu, ar putea fi luată în considerare punerea în aplicare a unui instrument de *self-service* care să permită persoanei vizate să acceseze cu ușurință datele cu caracter personal solicitate și a unui sistem de notificare prin care operatorul să fie avertizat cu privire la o cerere care se referă la date cu caracter personal cu perioade scurte de păstrare, pentru a facilita luarea de măsuri prompte.

[21] Acest lucru nu aduce atingere prelucrării ulterioare a datelor în scopuri probatorii în legătură cu tratarea cererii de acces pentru o perioadă adecvată.

Exemplul 6: cu ocazia răspunsului la o cerere de acces, un operator își dă seama că o cerere de angajare a persoanei vizate pe un post vacant în cadrul societății operatorului a fost stocată după expirarea perioadei de păstrare. În acest caz, operatorul nu poate șterge mai întâi și, ulterior, să răspundă persoanei vizate că nu sunt prelucrate date (referitoare la cerere). Operatorul trebuie mai întâi să ofere acces la date și apoi să le șteargă. Pentru a preveni o cerere ulterioară de ștergere, se recomandă adăugarea de informații cu privire la faptul și momentul ștergerii.

Pentru a respecta principiul transparenței, operatorii ar trebui să informeze persoana vizată cu privire la momentul specific al prelucrării la care se referă răspunsul operatorilor. În unele cazuri, de exemplu în contextul activităților frecvente de comunicare, pot avea loc prelucrări suplimentare sau modificări ale datelor între acest moment de referință, în care prelucrarea a fost evaluată, și răspunsul operatorului. În cazul în care operatorul are cunoștință de astfel de modificări, se recomandă să se includă informații cu privire la modificările respective, precum și informații privind prelucrarea suplimentară necesară pentru a răspunde cererii.

2.3.4 Respectarea cerințelor de securitate a datelor

40. Întrucât comunicarea și punerea la dispoziția persoanei vizate a datelor cu caracter personal reprezintă o operațiune de prelucrare, operatorul este întotdeauna obligat să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate corespunzător riscului prelucrării [a se vedea articolul 5 alineatul (1) litera (f) și articolele 24 și 32 din RGPD]. Acest lucru este valabil indiferent de modalitatea în care se acordă accesul. În cazul transmiterii electronice a datelor către persoana vizată prin alte mijloace decât cele electronice, în funcție de riscurile prezentate de prelucrare, operatorul poate lua în considerare transmiterea prin scrisoare recomandată sau, alternativ, poate oferi persoanei vizate, fără a-i impune nicio obligație, posibilitatea de a primi dosarul pe bază de semnătură direct de la unul dintre sediile operatorului. În cazul în care, în conformitate cu articolul 12 alineatele (1) și (3), informațiile sunt furnizate în format electronic, operatorul alege mijloacele electronice care respectă cerințele de securitate a datelor. De asemenea, în cazul furnizării unei copii a datelor într-un format electronic utilizat în mod curent [a se vedea articolul 15 alineatul (3)], operatorul ține seama de cerințele de asigurare a securității datelor atunci când alege mijloacele de transmitere a fișierului în format electronic către persoana vizată. Aceasta ar putea include aplicarea criptării, protecția parolelor etc. Pentru a facilita accesul la datele criptate, operatorul ar trebui, de asemenea, să se asigure că sunt puse la dispoziție informații adecvate, astfel încât persoana vizată să poată accesa informațiile decriptate. În cazurile în care cerințele de asigurare a securității datelor ar necesita criptarea de la un capăt la altul a e-mailurilor, însă operatorul este în măsură să trimită doar un e-mail normal, acesta va trebui să utilizeze alte mijloace, cum ar fi trimiterea prin poștă (recomandată) către persoana vizată a unei unități flash pentru USB.

3 CONSIDERAȚII GENERALE PRIVIND EVALUAREA CERERILOR DE ACCES

3.1 Introducere

41. Atunci când primește cereri de acces la date cu caracter personal, operatorul trebuie să evalueze fiecare cerere în parte. Operatorul ia în considerare, printre altele, următoarele aspecte, prezentate în detaliu în următoarele paragrafe: dacă cererea se referă la date cu caracter personal legate de persoana solicitantă și identitatea acesteia. Scopul acestei secțiuni este de a clarifica elementele cererii de acces pe care operatorul ar trebui să le ia în considerare atunci când efectuează evaluarea și de a

analiza scenarii posibile pentru o astfel de evaluare, precum și consecințele acesteia. Atunci când evaluează o cerere de acces la date cu caracter personal, operatorul ia în considerare, de asemenea, în temeiul articolului 12 alineatul (2) din RGPD, obligația de a facilita exercitarea drepturilor persoanelor vizate, asigurând totodată securitatea adecvată a datelor cu caracter personal[22].

42. Prin urmare, operatorii ar trebui să se pregătească în mod proactiv să trateze cererile de acces la datele cu caracter personal. Aceasta înseamnă că operatorul ar trebui să fie pregătit să primească cererea, să o evalueze în mod corespunzător (această evaluare face obiectul prezentei secțiuni a orientărilor) și să furnizeze persoanei solicitante un răspuns adecvat, fără întârzieri nejustificate. Modul în care operatorii se vor pregăti pentru exercitarea cererilor de acces ar trebui să fie adecvat și proporțional și să depindă de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile pentru drepturile și libertățile persoanelor fizice, în conformitate cu articolul 24 din RGPD. În funcție de circumstanțele specifice, operatorilor li se poate solicita, de exemplu, să pună în aplicare o procedură adecvată, care ar trebui să garanteze securitatea datelor fără a împiedica exercitarea drepturilor persoanei vizate.

3.1.1 Analiza conținutului cererii

43. Acest aspect poate fi evaluat mai precis prin adresarea următoarelor întrebări.

a) <u>Cererea se referă la date cu caracter personal?</u>

44. În temeiul RGPD, domeniul de aplicare al cererii acoperă numai datele cu caracter personal[23]. Prin urmare, orice cerere de informații cu privire la alte aspecte, inclusiv informații generale despre operator, modelele sale de afaceri sau activitățile sale de prelucrare care nu au legătură cu datele cu caracter personal, nu trebuie considerată o cerere formulată în temeiul articolului 15 din RGPD. În plus, o cerere de informații privind date anonime sau date care nu privesc persoana solicitantă sau persoana în numele căreia persoana autorizată a înaintat cererea nu va intra în domeniul de aplicare al dreptului de acces. Această întrebare va fi analizată mai detaliat în secțiunea 4.

45. Spre deosebire de datele anonime (care nu sunt date cu caracter personal), datele pseudonimizate, care ar putea fi atribuite unei persoane fizice prin utilizarea de informații suplimentare, sunt date cu caracter personal[24]. Astfel, datele pseudonimizate care ar putea avea legătură cu o persoană vizată – de exemplu, atunci când persoana vizată furnizează un element de identificare corespunzător care permite identificarea sa sau atunci când operatorul este în măsură să coreleze datele cu persoana

[22] Operatorul asigură securitatea adecvată a datelor cu caracter personal, în conformitate cu principiul integrității și confidențialității [articolul 5 alineatul (1) litera (f) din RGPD], prin punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel cum se menționează la articolul 32 din RGPD și se specifică în detaliu la articolul 24 din RGPD. Operatorul trebuie să fie în măsură să demonstreze că asigură un nivel adecvat de protecție a datelor, în conformitate cu principiul responsabilității (a se vedea, de asemenea: Avizul 3/2010 al Grupului de lucru „Articolul 29” privind principiul responsabilității, adoptat la 13 iulie 2010, 00062/10/RO, GL 173 și Orientările CEPD 07/2020 privind conceptele de operator și persoană împuternicită de operator în cadrul RGPD).

[23] Cu excepția cazului în care cererea se referă și la date fără caracter personal legate în mod indisolubil de datele cu caracter personal ale persoanei vizate. Pentru explicații suplimentare, a se vedea punctul 100.

[24] A se vedea considerentul 26 din RGPD. Explicații suplimentare privind conceptele de date anonime și date pseudonimizate sunt disponibile în Avizul 4/2007 al Grupului de lucru „Articolul 29” privind conceptul de date cu caracter personal, p. 18-21.

solicitantă prin mijloace proprii – trebuie să fie considerate a se încadra în domeniul de aplicare al cererii[25].

b) <u>Cererea se referă la persoana solicitantă (sau la persoana în numele căreia persoana autorizată înaintează cererea)?</u>

46. Ca regulă generală, o cerere poate viza numai datele persoanei solicitante. Accesul la datele altor persoane poate fi solicitat numai sub rezerva autorizării corespunzătoare[26].

Exemplul 7: persoana vizată X este director de departament în cadrul unei societăți care pune la dispoziția directorilor săi locuri de parcare într-o parcare de serviciu. Deși persoana vizată X dispune de un loc de parcare permanent, atunci când lucrează în tura a doua, acest loc este adesea deja ocupat de un alt autovehicul atunci când sosește la birou. Întrucât această situație se repetă, pentru a-l identifica pe conducătorul auto care ocupă neautorizat locul său, persoana vizată solicită operatorului sistemului de supraveghere video care acoperă zona de parcare a biroului accesul la datele cu caracter personal ale acestui conducător auto. Într-un astfel de caz, cererea persoanei vizate X nu va fi o cerere de acces la datele sale cu caracter personal, deoarece cererea nu se referă la datele persoanei solicitante, ci la datele unei alte persoane – și, prin urmare, nu ar trebui să fie considerată o cerere înaintată în temeiul articolului 15 din RGPD.

c) <u>Se aplică alte dispoziții decât cele ale RGPD care reglementează accesul la o anumită categorie de date?</u>

47. Persoanele vizate nu sunt obligate să specifice temeiul juridic în cererea lor. Cu toate acestea, în cazul în care persoanele vizate clarifică faptul că cererea lor se bazează pe legislația sectorială sau pe legislația națională care reglementează chestiunea specifică a accesului la anumite categorii de date, și nu pe RGPD, o astfel de cerere este examinată de operator în conformitate cu respectivele norme sectoriale sau naționale, după caz. Adesea, în funcție de legislația națională relevantă, operatorilor li se poate solicita să furnizeze răspunsuri separate, fiecare vizând cerințele specifice prevăzute de diferitele acte legislative. Acestea nu trebuie confundate cu legislația națională sau cu legislația UE care stabilește restricții privind dreptul de acces care trebuie respectate atunci când se răspunde la cererile de acces.

48. În cazul în care operatorul are îndoieli cu privire la dreptul pe care persoana vizată dorește să îl exercite, se recomandă să se solicite persoanei vizate care înaintează cererea să explice obiectul cererii. Această corespondență cu persoana vizată nu aduce atingere obligației operatorului de a acționa fără întârzieri nejustificate[27]. Cu toate acestea, în cazul în care există îndoieli, dacă operatorul solicită explicații suplimentare persoanei vizate și nu primește niciun răspuns, având în vedere obligația de a facilita exercitarea dreptului de acces al persoanei, operatorul ar trebui să interpreteze informațiile cuprinse în prima cerere și să acționeze pe această bază. În conformitate cu principiul responsabilității, operatorul poate stabili un termen adecvat în care persoana vizată poate oferi explicații suplimentare. Atunci când stabilește un astfel de termen, operatorul ar trebui să acorde timp suficient pentru a da curs cererii după expirarea acestuia și, prin urmare, să analizeze cât timp este necesar în mod obiectiv

[25] Grupul de lucru „Articolul 29”, GL242 rev.01, 5 aprilie 2017, Ghid privind dreptul la portabilitatea datelor – aprobat de CEPD (denumit în continuare „Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD”), p. 9.

[26] A se vedea secțiunea 3.4 („Cereri efectuate prin intermediul unor terți/reprezentanți”).

[27] A se vedea orientări suplimentare privind calendarul în secțiunea 5.3.

pentru compilarea și furnizarea datelor solicitate odată ce precizările au fost (sau nu) furnizate de către persoana vizată.

49. În cazul în care cererea intră în domeniul de aplicare al RGPD, existența unei astfel de legislații specifice nu prevalează asupra aplicării generale a dreptului de acces, astfel cum este prevăzut în RGPD. Ar putea exista restricții prevăzute de dreptul Uniunii sau de dreptul intern, atunci când acestea sunt permise în temeiul articolului 23 din RGPD (a se vedea secțiunea 6.4).

d) Cererea intră în domeniul de aplicare al *articolului 15?*

50. Ar trebui remarcat faptul că RGPD nu introduce nicio cerință formală pentru persoanele care solicită acces la date. Pentru a formula cererea de acces, este suficient ca persoanele solicitante să precizeze că doresc să știe care sunt datele cu caracter personal pe care le prelucrează operatorul. Prin urmare, operatorul nu poate refuza să furnizeze datele făcând referire la lipsa indicării temeiului juridic al cererii, în special la lipsa unei trimiteri specifice la dreptul de acces sau la RGPD.

De exemplu, pentru a formula o cerere, ar fi suficient ca persoana solicitantă să indice:

- că dorește să obțină acces la datele cu caracter personal care o privesc;
- că își exercită dreptul de acces sau
- că dorește să cunoască informațiile care o privesc pe care le prelucrează operatorul.

Trebuie să se țină seama de faptul că este posibil ca solicitanții să nu cunoască complexitatea RGPD și că este recomandabil să se acționeze cu indulgență față de persoanele care își exercită dreptul de acces, în special atunci când acesta este exercitat de minori. Astfel cum s-a indicat mai sus, în cazul în care există îndoieli, se recomandă operatorului să solicite persoanei vizate care înaintează cererea să specifice obiectul cererii.

e) Persoanele vizate doresc să acceseze toate informațiile prelucrate cu privire la ele sau doar părți din acestea?

51. În plus, operatorul trebuie să evalueze dacă cererile înaintate de persoanele solicitante se referă la toate informațiile sau la o parte a informațiilor prelucrate în legătură cu acestea. Orice limitare a domeniului de aplicare al unei cereri la o dispoziție specifică de la articolul 15 din RGPD, înaintată de persoanele vizate, trebuie să fie clară și lipsită de ambiguitate. De exemplu, în cazul în care persoanele vizate solicită textual „informații cu privire la datele prelucrate în legătură cu acestea”, operatorul ar trebui să presupună că persoanele vizate intenționează să își exercite pe deplin dreptul în temeiul articolului 15 alineatele (1)-(2) din RGPD. O astfel de cerere nu ar trebui interpretată în sensul că persoanele vizate doresc să primească numai categoriile de date cu caracter personal care sunt prelucrate și să renunțe la dreptul lor de a primi informațiile enumerate la articolul 15 alineatul (1) literele (a)-(h). Situația ar fi diferită, de exemplu, în cazul în care persoanele vizate doresc, în ceea ce privește datele pe care le specifică, să aibă acces la sursa sau originea datelor cu caracter personal sau la perioada specificată de stocare. Într-un astfel de caz, operatorul își poate limita răspunsul la informațiile specifice solicitate.

3.1.2 Formatul cererii

52. Astfel cum s-a menționat anterior, RGPD nu impune persoanelor vizate nicio cerință în ceea ce privește formatul cererii de acces la datele cu caracter personal. Prin urmare, nu există, în principiu, nicio cerință în temeiul RGPD pe care persoanele vizate trebuie să o respecte atunci când aleg un canal de comunicare prin care intră în contact cu operatorul.

53. CEPD încurajează operatorii să furnizeze cele mai adecvate și mai ușor de utilizat canale de comunicare, în conformitate cu articolul 12 alineatul (2) și cu articolul 25 din RGPD, pentru a permite persoanei vizate să înainteze o cerere eficace. Cu toate acestea, în cazul în care o persoană vizată înaintează o cerere utilizând un canal de comunicare pus la dispoziție de operator[28], care este diferit de cel indicat ca fiind preferabil, o astfel de cerere este, în general, considerată eficace, iar operatorul ar trebui să trateze o astfel de cerere în consecință (a se vedea exemplele de mai jos). Operatorii ar trebui să depună toate eforturile rezonabile pentru a se asigura că exercitarea drepturilor persoanelor vizate este facilitată (de exemplu, atunci când o persoană vizată trimite o cerere de acces unui angajat aflat în concediu, un mesaj automat prin care persoana vizată este informată cu privire la un canal de comunicare alternativ pentru această cerere ar putea fi un efort rezonabil).

54. Ar trebui remarcat faptul că operatorul nu este obligat să dea curs unei cereri trimise la o adresă de e-mail (sau poștală) aleatorie sau incorectă, care nu este furnizată direct de operator, sau printr-un canal de comunicare care, în mod evident, nu este destinat primirii de cereri privind drepturile persoanei vizate în cazul în care operatorul a pus la dispoziție un canal de comunicare adecvat, care poate fi utilizat de persoana vizată.

55. De asemenea, operatorul nu este obligat să dea curs unei cereri trimise la adresa de e-mail a unui angajat al operatorului care ar putea să nu fie implicat în prelucrarea cererilor privind drepturile persoanelor vizate (de exemplu, conducători auto, personal de curățenie etc.). Astfel de cereri nu sunt considerate eficace dacă operatorul a pus în mod clar la dispoziția persoanei vizate un canal de comunicare adecvat. Cu toate acestea, în cazul în care persoana vizată trimite o cerere angajatului operatorului care a fost desemnat ca persoană de contact (cum ar fi, de exemplu, un administrator de conturi personale la o bancă sau un consultant al unui operator de telefonie mobilă), un astfel de contact nu ar trebui să fie considerat aleatoriu, iar operatorul ar trebui să depună toate eforturile rezonabile pentru a trata respectiva cerere, astfel încât aceasta să poată fi redirecționată către punctul de contact și să poată primi un răspuns în termenele prevăzute de RGPD.

56. Cu toate acestea, CEPD recomandă, ca bună practică, ca operatorii să introducă mecanisme adecvate pentru a facilita exercitarea drepturilor persoanelor vizate, inclusiv sisteme de răspuns automat pentru a informa cu privire la absențele personalului și contacte alternative adecvate și, acolo unde este posibil, mecanisme de îmbunătățire a comunicării interne între angajați cu privire la cererile primite de cei care ar putea să nu aibă competența de a da curs unor astfel de cereri.

Exemplul 8: operatorul X indică, atât pe site-ul său, cât și în declarația de confidențialitate, două adrese de e-mail – adresa de e-mail generală a operatorului: CONTACT@X.COM și adresa de e-mail a punctului de contact pentru protecția datelor al operatorului: QUERIES@X.COM. În plus, operatorul X indică pe site-ul său că, pentru a adresa întrebări sau pentru a înainta o cerere cu privire la prelucrarea datelor cu caracter personal, persoanele fizice ar trebui să contacteze punctul de contact pentru protecția datelor prin intermediul adresei de e-mail furnizate. Cu toate acestea, persoana vizată trimite o cerere la adresa de e-mail generală a operatorului: CONTACT@X.COM.

Într-un astfel de caz, operatorul ar trebui să depună toate eforturile rezonabile pentru a-și informa serviciile cu privire la cerere, care a fost transmisă prin adresa de e-mail generală, astfel încât aceasta să poată fi redirecționată către punctul de contact pentru protecția datelor și să poată primi un răspuns

[28] Acesta ar putea include, de exemplu, datele de comunicare ale operatorului furnizate în comunicările sale adresate direct persoanelor vizate sau datele de contact furnizate public de operator, cum ar fi în declarația de confidențialitate a operatorului sau în alte avize juridice obligatorii ale operatorului (de exemplu, datele de contact ale proprietarului sau ale întreprinderii pe un site internet).

în termenele prevăzute de RGPD. În plus, operatorul nu are dreptul de a prelungi termenul de răspuns la o cerere pentru simplul motiv că persoana vizată a trimis o cerere la adresa de e-mail generală a operatorului, nu la adresa de e-mail a punctului de contact pentru protecția datelor al operatorului.

Exemplul 9: operatorul Y administrează o rețea de cluburi de fitness. Operatorul Y indică pe site-ul său și în declarația de confidențialitate pentru clienții clubului de fitness că, pentru a transmite orice întrebare sau pentru a depune o cerere cu privire la prelucrarea datelor cu caracter personal, persoanele fizice ar trebui să contacteze operatorul la adresa de e-mail: QUERIES@Y.COM. Cu toate acestea, persoana vizată trimite o cerere la o adresă de e-mail afișată la vestiar, unde a găsit un anunț cu următorul text: „Dacă nu sunteți mulțumit de curățenia sălii, vă rugăm să ne contactați la adresa: CLEANERS@Y.COM", aceasta fiind adresa de e-mail a personalului de curățenie angajat de Y. În mod evident, personalul de curățenie nu este implicat în gestionarea aspectelor legate de exercitarea drepturilor persoanelor vizate – clienții clubului de fitness. Deși adresa de e-mail era disponibilă la sediul clubului de fitness, persoana vizată nu se putea aștepta în mod rezonabil ca aceasta să fie o adresă de contact adecvată pentru astfel de cereri, întrucât pe site și în declarația de confidențialitate se oferă în mod clar informații cu privire la canalul de comunicare care trebuie să fie utilizat pentru exercitarea drepturilor persoanelor vizate.

57. Data primirii cererii de către operator declanșează, ca regulă generală, termenul de o lună în care operatorul trebuie să furnizeze informații cu privire la măsurile luate ca urmare a unei cereri, în conformitate cu articolul 12 alineatul (3) din RGPD (orientări suplimentare privind calendarul sunt furnizate în secțiunea 5.3). CEPD consideră drept bună practică pentru operatori confirmarea în scris a primirii cererilor, de exemplu prin trimiterea de e-mailuri (sau informări prin poștă, dacă este cazul) persoanelor solicitante care confirmă că cererile lor au fost primite și că termenul de o lună începe din data de X și se încheie în data de Y.

3.2 Identificarea și autentificarea

58. Pentru a asigura securitatea prelucrării și pentru a reduce la minimum riscul divulgării neautorizate a datelor cu caracter personal, operatorul trebuie să fie în măsură să afle ce date se referă la persoana vizată (identificare) și să confirme identitatea persoanei respective (autentificare).

59. Se poate reaminti că, în situațiile în care scopul prelucrării datelor cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate, operatorul nu are obligația de a păstra identificarea în scopul unic al respectării drepturilor persoanelor vizate, inclusiv din perspectiva principiului reducerii la minimum a datelor. Aceste situații sunt abordate la articolul 11 alineatul (1) din RGPD.

60. Articolul 12 alineatul (2) din RGPD prevede că operatorul nu refuză să dea curs cererii persoanei vizate de a-și exercita drepturile, cu excepția cazului în care operatorul prelucrează date cu caracter personal într-un scop care nu necesită identificarea persoanei vizate și demonstrează că nu este în măsură să identifice persoana vizată. Cu toate acestea, în astfel de circumstanțe, persoana vizată poate decide să ofere informații suplimentare care să permită această identificare [articolul 11 alineatul (2) din RGPD][29].

61. Operatorul nu este obligat să obțină astfel de informații suplimentare pentru a identifica persoana vizată cu scopul unic de a da curs cererii persoanei vizate, având în vedere, de asemenea, principiul reducerii la minimum a datelor. Cu toate acestea, nu ar trebui să refuze să preia astfel de informații

[29] Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD, p. 13.

suplimentare furnizate de persoana vizată cu scopul de a sprijini exercitarea drepturilor acesteia (considerentul 57 din RGPD).

Exemplul 10: X este operatorul datelor prelucrate în legătură cu supravegherea video a unei clădiri. În conformitate cu articolul 11 alineatul (1) din RGPD, operatorul nu este obligat să identifice toate persoanele care au fost înregistrate de o cameră de securitate ca parte a monitorizării (scop care nu necesită identificare). Operatorul primește o cerere de acces la datele cu caracter personal din partea persoanei care susține că a fost înregistrată de sistemul de supraveghere video al operatorului. Acțiunile operatorului vor depinde de informațiile suplimentare furnizate. În cazul în care persoana solicitantă indică o anumită zi și oră în care este posibil ca evenimentul în cauză să fi fost înregistrat de camere, este probabil ca operatorul să fie în măsură să furnizeze astfel de date [articolul 11 alineatul (2) din RGPD]. Cu toate acestea, în cazul în care operatorul nu este în măsură să identifice persoana vizată (de exemplu, dacă este imposibil pentru operator să se asigure că o persoană solicitantă este de fapt persoana vizată sau dacă cererea se referă, de exemplu, la o perioadă lungă de înregistrări, iar un operator nu este în măsură să prelucreze un volum atât de mare de date), operatorul poate refuza să ia măsuri dacă demonstrează că nu este în măsură să identifice persoana vizată [articolul 12 alineatul (2) din RGPD].

Exemplul 11: un operator C prelucrează date cu caracter personal în scopul direcționării publicității comportamentale către utilizatorii site-ului său. Datele cu caracter personal colectate în scopuri legate de publicitatea comportamentală sunt, de obicei, colectate prin intermediul cookie-urilor și sunt asociate cu identificatori aleatorii pseudonimizați. O persoană vizată, dl X, își exercită dreptul de acces prin intermediul site-ului operatorului C. Operatorul C este în măsură să îl identifice cu precizie pe dl X pentru a afișa publicitatea comportamentală destinată persoanei vizate, asociind echipamentul terminal al dlui X cu profilul său publicitar prin intermediul cookie-urilor stocate în terminal. Operatorul C ar trebui, de asemenea, să fie în măsură să îl identifice cu precizie pe dl X pentru a-i acorda acces la datele sale cu caracter personal, întrucât se poate stabili o legătură între datele prelucrate și persoana vizată. Prin urmare, și ținând seama de principiile RGPD, exemplul de mai sus nu ar intra în domeniul de aplicare al articolului 11 din RGPD. Mai precis, în exemplul de mai sus, scopurile operatorului C necesită identificarea persoanelor vizate, în timp ce articolul 11 din RGPD abordează situația prelucrării care nu necesită identificarea, caz în care un operator nu este obligat să prelucreze date suplimentare în sensul articolului 11 alineatul (1) din RGPD cu unicul scop de a fi în măsură să respecte RGPD. Prin urmare, în unele cazuri, nu ar trebui solicitate date suplimentare pentru exercitarea drepturilor persoanei vizate.

Cu toate acestea, în cazul în care dl X încearcă să își exercite dreptul de acces prin e-mail sau prin poștă obișnuită, atunci, în acest context, operatorul C nu va avea altă opțiune decât să solicite dlui X să furnizeze „informații suplimentare” [articolul 12 alineatul (6) din RGPD] pentru a putea identifica profilul publicitar asociat dlui X. În acest caz, informațiile suplimentare vor fi identificatorul cookie stocat în echipamentul terminal al dlui X.

62. În cazul unei imposibilități demonstrate de a identifica persoana vizată (articolul 11 din RGPD), operatorul trebuie să informeze persoana vizată în consecință, dacă este posibil, întrucât operatorul răspunde cererilor persoanei vizate fără întârzieri nejustificate și prezintă motivele pentru care nu intenționează să dea curs unor astfel de cereri. Aceste informații trebuie furnizate numai „dacă este posibil”, deoarece este posibil ca operatorul să nu fie în măsură să informeze persoanele vizate dacă identificarea acestora este imposibilă.

63. Atât atunci când prelucrarea nu impune o identificare, cât și atunci când impune acest lucru, în cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea, operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate [articolul 12 alineatul (6) din RGPD].

64. RGPD nu prevede nicio cerință cu privire la modul de autentificare a persoanei vizate. Cu toate acestea, articolele 11 și 12 din RGPD prevăd condițiile de exercitare a tuturor drepturilor persoanelor vizate, inclusiv dreptul de acces la datele cu caracter personal.

65. Ar trebui reamintit faptul că, de regulă, operatorul nu poate solicita mai multe date cu caracter personal decât este necesar pentru a permite această autentificare și că utilizarea unor astfel de informații ar trebui să se limiteze strict la soluționarea cererii persoanelor vizate.

66. Adesea, există deja proceduri de autentificare între persoanele vizate și operatori. Operatorii pot utiliza aceste proceduri de autentificare pentru a stabili identitatea persoanelor vizate care solicită datele lor cu caracter personal sau care își exercită drepturile acordate de RGPD[30]. În caz contrar, operatorii ar trebui să pună în aplicare o procedură de autentificare în acest scop[31].

67. În cazurile în care operatorul solicită informațiile suplimentare necesare pentru a confirma identitatea persoanei vizate sau îi sunt furnizate astfel de informații de către persoana vizată, operatorul trebuie să evalueze, de fiecare dată, informațiile care îi vor permite să confirme identitatea persoanei vizate și, eventual, va adresa întrebări suplimentare persoanei solicitante sau va solicita persoanei vizate să prezinte anumite elemente de identificare suplimentare, dacă acest lucru este proporțional (a se vedea secțiunea 3.3).

68. Pentru a permite persoanei vizate să furnizeze informațiile suplimentare necesare pentru identificarea datelor sale, operatorul ar trebui să informeze persoana vizată cu privire la natura informațiilor suplimentare necesare pentru a permite identificarea. Aceste informații suplimentare nu ar trebui să depășească informațiile necesare inițial pentru autentificarea persoanei vizate. În general, faptul că operatorul poate solicita informații suplimentare pentru a evalua identitatea persoanei vizate nu poate conduce la cerințe excesive și la colectarea de date cu caracter personal care nu sunt relevante sau necesare pentru a consolida legătura dintre persoana vizată și datele cu caracter personal solicitate[32].

69. În consecință, în cazul în care informațiile colectate online sunt asociate unor pseudonime sau altor identificatori unici, operatorul poate pune în aplicare proceduri adecvate care să permită persoanei solicitante să înainteze o cerere de acces la date și să primească datele care o privesc[33].

Exemplul 12: persoana vizată, dna X, solicită acces la datele sale în cadrul unei conversații cu consultantul unui serviciu de asistență al unei societăți de furnizare de energie electrică cu care a încheiat un contract. Consultantul, având îndoieli cu privire la identitatea persoanei care înaintează cererea, generează în sistemul societății un cod de unică utilizare trimis pe numărul de telefon mobil al utilizatorului, furnizat la momentul creării contului, ca parte a sistemului de dublă verificare, acțiune care ar trebui considerată proporțională în acest caz.

[30] Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD, p. 14.
[31] A se vedea orientările suplimentare privind autentificarea în secțiunea 3.3.
[32] Ibidem, p. 14.
[33] Ibidem, p. 13-14.

3.3 Evaluarea proporționalității în ceea ce privește autentificarea persoanei solicitante

70. Astfel cum s-a indicat mai sus, în cazul în care operatorul are motive întemeiate să pună la îndoială identitatea persoanei solicitante, acesta poate solicita informații suplimentare pentru a confirma identitatea persoanei vizate. Cu toate acestea, operatorul trebuie, în același timp, să se asigure că nu colectează mai multe date cu caracter personal decât este necesar pentru a permite autentificarea persoanei solicitante. Prin urmare, operatorul efectuează o evaluare a proporționalității, care trebuie să țină seama de tipul de date cu caracter personal prelucrate (de exemplu, categorii speciale de date sau nu), de natura cererii, de contextul în care este înaintată cererea, precum și de orice prejudiciu care ar putea rezulta din divulgarea necorespunzătoare. Atunci când se evaluează proporționalitatea, ar trebui să se țină seama de faptul că trebuie să se evite colectarea excesivă a datelor, asigurând, în același timp, un nivel adecvat de securitate a prelucrării.

71. Operatorul ar trebui să pună în aplicare o procedură de autentificare pentru a fi sigur de identitatea persoanelor care solicită acces la datele lor[34] și să asigure securitatea prelucrării pe tot parcursul procesului tratării cererilor de acces în conformitate cu articolul 32 din RGPD, inclusiv, de exemplu, un canal securizat prin care persoanele vizate să furnizeze informații suplimentare. Metoda utilizată pentru autentificare ar trebui să fie relevantă, adecvată, proporțională și să respecte principiul reducerii la minimum a datelor. În cazul în care operatorul impune măsuri care vizează autentificarea persoanei vizate care sunt împovărătoare, acesta trebuie să justifice în mod adecvat acest lucru și să asigure respectarea tuturor principiilor fundamentale, inclusiv reducerea la minimum a datelor și obligația de a facilita exercitarea drepturilor persoanelor vizate [articolul 12 alineatul (2) din RGPD].

72. Într-un context online, mecanismul de autentificare poate include aceleași acreditări, utilizate de persoana vizată pentru conectarea la serviciul online oferit de operator (considerentul 57 din RGPD)[35].

73. În practică, există adesea proceduri de autentificare, iar operatorii nu trebuie să introducă garanții suplimentare pentru a preveni accesul neautorizat la servicii. Pentru a permite persoanelor fizice să acceseze datele conținute în conturile lor (cum ar fi un cont de e-mail, un cont pe rețelele sociale sau pe site-urile magazinelor online), este foarte probabil ca operatorii să solicite înregistrarea prin intermediul numelui de utilizator și al parolei utilizatorului, ceea ce, în astfel de cazuri, ar trebui să fie suficient pentru a autentifica o persoană vizată[36]. În plus, persoanele vizate sunt adesea deja autentificate de operator înainte de încheierea unui contract sau de obținerea consimțământului lor pentru prelucrare și, prin urmare, datele cu caracter personal utilizate pentru înregistrarea persoanei vizate de prelucrare pot fi, de asemenea, utilizate ca dovezi pentru autentificarea persoanei vizate în scopul accesului[37]. În consecință, este disproporționat să se solicite o copie a unui document de identitate în cazul în care persoana vizată care înaintează o cerere este deja autentificată de operator.

74. Ar trebui subliniat faptul că utilizarea unei copii a unui document de identitate ca parte a procesului de autentificare creează un risc pentru securitatea datelor cu caracter personal și poate conduce la o prelucrare neautorizată sau ilegală și, ca atare, ar trebui considerată inadecvată, cu excepția cazului în

[34] Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD, p. 14.

[35] A se vedea orientări suplimentare privind metodele de autentificare în Orientările CEPD 01/2021 referitoare la exemple de notificare privind încălcarea securității datelor cu caracter personal, adoptate la 14 ianuarie 2021, p. 30-31, și în Orientările CEPD 02/2021 privind asistenții vocali virtuali, versiunea 2.0, adoptate la 7 iulie 2021, secțiunea 3.7.

[36] Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD, p. 14.

[37] Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD, p. 14.

care este necesară, adecvată și conformă cu dreptul intern. În astfel de cazuri, operatorii ar trebui să dispună de sisteme care să asigure un nivel de securitate adecvat pentru a atenua riscurile mai mari la adresa drepturilor și libertăților persoanei vizate de a primi astfel de date. De asemenea, este important de remarcat faptul că autentificarea prin intermediul unei cărți de identitate nu ajută neapărat în context online (de exemplu, prin utilizarea pseudonimelor) dacă persoana în cauză nu poate prezenta alte dovezi, de exemplu caracteristici suplimentare care corespund contului de utilizator.

75. Având în vedere faptul că numeroase organizații (de exemplu, hoteluri, bănci, societăți de închirieri auto) solicită copii ale cărților de identitate ale clienților lor, aceasta nu ar trebui, în general, să fie considerată o modalitate adecvată de autentificare. În mod alternativ, operatorul poate pune în aplicare o măsură de securitate rapidă și eficace pentru a identifica o persoană vizată pe baza autentificării pe care a efectuat-o anterior, de exemplu prin e-mail sau mesaj text care conține linkuri de confirmare, întrebări de securitate sau coduri de confirmare[38].

76. Informațiile privind documentul de identitate care nu sunt necesare pentru confirmarea identității persoanei vizate, cum ar fi numărul și seria, cetățenia, înălțimea, culoarea ochilor, fotografia și zona citibilă automat, în funcție de o evaluare de la caz la caz, pot fi cenzurate sau ascunse de persoana vizată înainte de a le transmite operatorului, cu excepția cazului în care legislația națională prevede furnizarea unei copii integrale necenzurate a cărții de identitate (a se vedea punctul 78 de mai jos). În general, data eliberării sau data expirării, autoritatea emitentă și numele complet care corespunde contului online sunt suficiente pentru ca operatorul să verifice identitatea, cu condiția să se asigure întotdeauna autenticitatea copiei și relația cu solicitantul. Informații suplimentare, cum ar fi data nașterii persoanei vizate, pot fi solicitate numai în cazul în care persistă riscul de eroare de identitate, dacă operatorul este în măsură să le compare cu informațiile pe care le prelucrează deja.

77. Pentru a respecta principiul reducerii la minimum a datelor, operatorul ar trebui să informeze persoana vizată cu privire la informațiile care nu sunt necesare și la posibilitatea de a cenzura sau de a ascunde acele părți ale documentului de identitate. Într-un astfel de caz, dacă persoana vizată nu știe cum să cenzureze astfel de informații sau nu este în măsură să facă acest lucru, o bună practică este ca operatorul să le cenzureze la primirea documentului, dacă are această posibilitate, ținând seama de mijloacele de care dispune acesta în circumstanțele date.

Exemplul 13: utilizatorul, dna Y, a creat un cont protejat cu parolă pe site-ul magazinului online, furnizând e-mailul său și/sau numele său de utilizator. Ulterior, proprietarul contului solicită operatorului informații pentru a afla dacă îi prelucrează datele cu caracter personal și, în caz afirmativ, solicită acces la acestea în domeniul de aplicare indicat la articolul 15. Operatorul solicită documentul de identitate al persoanei solicitante pentru a confirma identitatea acesteia. Acțiunea operatorului în acest caz este disproporționată și conduce la colectarea inutilă a datelor.

Cu toate acestea, pentru a confirma identitatea persoanei solicitante, prevenind în același timp colectarea datelor inutile, operatorul i-ar putea solicita acesteia să se autentifice prin conectare la cont sau să îi adreseze întrebările de securitate (adecvate), al căror răspuns ar trebui să fie cunoscut numai de persoana vizată, sau să utilizeze autentificarea multifactorială configurată atunci când persoana vizată și-a înregistrat contul sau să utilizeze alte mijloace de comunicare existente, cunoscute ca

[38] A se vedea, de asemenea, Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, care a propus diferite servicii care permit identificarea securizată la distanță.

aparținând persoanei vizate, cum ar fi adresa de e-mail sau un număr de telefon, pentru a trimite o parolă de acces.

Exemplul 14: un client al băncii, dl Y, intenționează să obțină un credit de consum. În acest scop, dl Y merge la o sucursală a băncii pentru a obține informațiile, inclusiv datele sale cu caracter personal, necesare pentru evaluarea bonității sale. Pentru a verifica identitatea persoanei vizate, consultantul solicită o certificare legalizată a identității sale, pentru a putea să îi furnizeze informațiile necesare.

Operatorul nu ar trebui să solicite confirmarea legalizată a identității, cu excepția cazului în care acest lucru este necesar, adecvat și în conformitate cu dreptul intern (de exemplu, în cazul în care o persoană nu se află temporar în posesia niciunui document de identitate, iar dovada identității persoanei vizate este impusă de dreptul intern pentru executarea unui act juridic). O astfel de practică expune persoanele solicitante la costuri suplimentare și impune o sarcină excesivă asupra persoanelor vizate, împiedicând exercitarea dreptului lor de acces.

78. Fără a aduce atingere principiilor generale de mai sus, în anumite circumstanțe, autentificarea pe baza unui document de identitate poate fi o măsură justificată și proporțională, în special pentru entitățile care prelucrează categorii speciale de date cu caracter personal sau care efectuează prelucrarea datelor care pot prezenta un risc pentru persoana vizată (de exemplu, informații medicale sau privind sănătatea). Totuși, în același timp, ar trebui să se țină seama de faptul că anumite dispoziții naționale prevăd restricții privind prelucrarea datelor conținute în documentele oficiale, inclusiv documente care confirmă identitatea unei persoane (inclusiv în temeiul articolului 87 din RGPD). Restricțiile privind prelucrarea datelor din aceste documente se pot referi în special la scanarea sau fotocopierea cărților de identitate sau la prelucrarea codurilor numerice personale oficiale[39].

79. Având în vedere cele de mai sus, în cazul în care se solicită un document de identitate (iar acest lucru este în conformitate cu dreptul intern și este justificat și proporțional în temeiul RGPD), operatorul trebuie să pună în aplicare garanții pentru a preveni prelucrarea ilegală a documentului de identitate. Fără a aduce atingere niciunei dispoziții naționale aplicabile privind autentificarea pe baza documentului de identitate, aceasta poate include abținerea de la efectuarea unei copii sau ștergerea unei copii a unui document de identitate imediat după autentificarea cu succes a identității persoanei vizate. Motivul în acest caz este faptul că stocarea ulterioară a unei copii a unui document de identitate ar putea constitui o încălcare a principiilor limitării scopului și limitării legate de stocare [articolul 5 alineatul (1) literele (b) și (e) din RGPD] și, în plus, a legislației naționale privind prelucrarea numărului de identificare național (articolul 87 din RGPD). Ca bună practică, CEPD recomandă ca, după verificarea cărții de identitate, operatorul să formuleze o notă, de exemplu, „cartea de identitate a fost verificată” pentru a evita copierea sau stocarea inutilă a copiilor cărților de identitate.

3.4 Cereri înaintate prin intermediul terților/reprezentanților

80. Deși dreptul de acces este, în general, exercitat de persoanele vizate întrucât se referă la acestea, există posibilitatea ca cererea să fie înaintată de un terț în numele persoanei vizate. Această situație poate apărea, printre altele, în cazul acționării prin intermediul unui reprezentant sau al unor tutori legali în

[39] Mai multe state membre au introdus o astfel de restricție în dispozițiile lor naționale în această privință, afirmând, de exemplu, că realizarea de copii ale cărților de identitate este legală numai dacă rezultă direct din dispozițiile unui act juridic.

numele minorilor, precum și în cazul acționării prin intermediul altor entități folosind portaluri online. În anumite circumstanțe, identitatea persoanei autorizate să exercite dreptul de acces, precum și autorizația de a acționa în numele persoanei vizate pot necesita o verificare, în cazul în care aceasta este adecvată și proporțională (a se vedea secțiunea 3.3 de mai sus)[40]. Ar trebui reamintit faptul că punerea datelor cu caracter personal la dispoziția unei persoane care nu are drept de acces poate constitui o încălcare a securității datelor cu caracter personal[41].

81. În acest sens, ar trebui luate în considerare actele legislative naționale care reglementează reprezentarea juridică (de exemplu, împuternicirile), care pot impune cerințe specifice pentru demonstrarea autorizării de a depune o cerere în numele persoanei vizate, întrucât RGPD nu reglementează acest aspect. În conformitate cu principiul responsabilității, precum și cu celelalte principii de protecție a datelor, operatorii trebuie să fie în măsură să demonstreze existența autorizației relevante de a depune o cerere în numele persoanei vizate și de a primi informațiile solicitate, cu excepția cazului în care dreptul intern diferă (de exemplu, dreptul intern conține norme specifice privind credibilitatea avocaților), lăsându-i operatorului responsabilitatea de a verifica identitatea reprezentantului (de exemplu, în cazul avocaților verificarea înscrierii la barou). Prin urmare, se recomandă colectarea documentației corespunzătoare în acest sens, în legătură cu normele generale indicate anterior privind confirmarea identității unei persoane fizice care înaintează o cerere și, în cazul în care operatorul are îndoieli întemeiate cu privire la identitatea unei persoane care acționează în numele persoanei vizate, acesta trebuie să solicite informații suplimentare pentru confirmarea identității persoanei respective.

82. Deși exercitarea dreptului de acces la datele cu caracter personal ale persoanelor decedate constituie un alt exemplu de acces al unui terț, altul decât persoana vizată, considerentul 27 precizează că RGPD nu se aplică datelor cu caracter personal ale persoanelor decedate. Prin urmare, acest aspect este reglementat de dreptul intern, iar statele membre pot prevedea norme privind prelucrarea datelor cu caracter personal ale persoanelor decedate. Cu toate acestea, trebuie să se țină seama de faptul că datele pot, în plus, să se refere la persoane terțe în viață, de exemplu în contextul cererii de acces la corespondența unei persoane decedate. Confidențialitatea acestor date trebuie protejată în continuare.

3.4.1 Exercitarea dreptului de acces în numele copiilor

83. Copiii au nevoie de o protecție specifică a datelor lor cu caracter personal, întrucât pot fi mai puțin conștienți de riscurile, consecințele, garanțiile privind drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal[42]. Toate informațiile și comunicările către un copil, în cazul în care sunt prelucrate date cu caracter personal ale unui copil, ar trebui să fie redactate într-un limbaj clar și simplu, astfel încât copilul să îl poată înțelege cu ușurință[43].

[40] În ceea ce privește termenele pentru exercitarea dreptului de acces atunci când operatorul trebuie să obțină informații suplimentare, a se vedea punctul 157.
[41] Articolul 4 punctul 12 din RGPD.
[42] Considerentul 38 din RGPD. Astfel cum se prevede în programul de lucru al CEPD, intenția sa este de a oferi orientări cu privire la datele copiilor. Se preconizează că un astfel de document va oferi mai multe orientări cu privire la condițiile în care un copil își poate exercita propriul drept de acces, iar titularul răspunderii părintești își poate exercita dreptul de acces în numele copilului.
[43] Considerentul 58 din RGPD. Orientările 05/2020 ale CEPD privind consimțământul în temeiul Regulamentului 2016/679, secțiunea 7.

84. Copiii sunt persoane vizate de sine stătătoare și, ca atare, dreptul de acces aparține copilului. În funcție de maturitatea și capacitatea copilului, acesta poate avea nevoie de o parte terță pentru a acționa în numele său, de exemplu, titularul răspunderii părintești.

85. Interesul superior al copilului ar trebui să fie un considerent principal în toate deciziile luate cu privire la exercitarea dreptului de acces în contextul copiilor, în special în cazul în care dreptul de acces este exercitat în numele copilului, de exemplu de către titularul autorității părintești.

86. Având în vedere protecția specială a datelor cu caracter personal ale copiilor prevăzută în RGPD, operatorul ia măsurile adecvate pentru a evita orice divulgare a datelor cu caracter personal ale unui minor către o persoană neautorizată (a se vedea în acest sens și secțiunea 3.4 de mai sus).

87. În cele din urmă, dreptul titularului răspunderii părintești de a acționa în numele copilului nu ar trebui confundat cu cazurile, în afara legislației privind protecția datelor, în care legislația națională poate prevedea dreptul titularului răspunderii părintești de a solicita și de a primi informații cu privire la copil (de exemplu, rezultatele școlare ale copilului).

3.4.2 Exercitarea dreptului de acces prin intermediul portalurilor/canalelor puse la dispoziție de un terț

88. Există întreprinderi care oferă servicii ce permit persoanelor vizate să înainteze cereri de acces prin intermediul unui portal. Persoana vizată se conectează și obține acces la un portal prin intermediul căruia poate depune, de exemplu, o cerere de acces, poate solicita rectificarea datelor sau ștergerea datelor de la diferiți operatori. Utilizarea portalurilor puse la dispoziție de un terț generează diferite întrebări.

89. Primul aspect pe care operatorii trebuie să îl abordeze atunci când se confruntă cu aceste circumstanțe este acela de a se asigura că partea terță acționează în mod legitim în numele persoanei vizate, deoarece este necesar să se asigure că niciun fel de date nu sunt divulgate unor părți neautorizate.

90. În plus, un operator care primește o cerere depusă prin intermediul unui astfel de portal trebuie, în mod invariabil, să trateze cererea respectivă în timp util[44]. Cu toate acestea, nu există nicio obligație pentru operator de a furniza datele în temeiul articolului 15 din RGPD direct portalului, în cazul în care operatorul, de exemplu, stabilește că măsurile de securitate sunt insuficiente sau că ar fi oportun să se utilizeze o altă modalitate pentru divulgarea datelor către persoana vizată. În astfel de circumstanțe, atunci când operatorul dispune de alte proceduri pentru a trata cererile de acces într-un mod eficient și sigur, operatorul poate furniza informațiile solicitate prin intermediul acestor proceduri.

4 DOMENIUL DE APLICARE AL DREPTULUI DE ACCES ȘI DATELE CU CARACTER PERSONAL ȘI INFORMAȚIILE LA CARE SE REFERĂ

91. Prezenta secțiune are ca scop clarificarea definiției noțiunii de „date cu caracter personal” (secțiunea 4.1) și clarificarea domeniului de aplicare al informațiilor care fac obiectul dreptului de acces în general (secțiunile 4.2 și 4.3). Trebuie remarcat faptul că domeniul de aplicare al noțiunii de „date cu caracter personal” și, prin urmare, diferențierea dintre datele cu caracter personal și alte date face

[44] În ceea ce privește termenele pentru exercitarea dreptului de acces atunci când operatorul trebuie să obțină informații suplimentare, a se vedea punctul 157.

parte integrantă din evaluarea efectuată de operator pentru a identifica domeniul de aplicare al datelor la care persoana vizată are dreptul să obțină acces[45].

92. Cu titlu preliminar, trebuie amintit că dreptul de acces poate fi exercitat numai în ceea ce privește prelucrarea datelor cu caracter personal care intră în domeniul de aplicare material și teritorial al RGPD. Prin urmare, datele cu caracter personal care nu sunt prelucrate prin mijloace automatizate sau care nu fac parte sau care nu sunt destinate să devină parte dintr-un sistem de evidență a datelor în conformitate cu articolul 2 alineatul (1) din RGPD sau care sunt prelucrate de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice în conformitate cu articolul 2 alineatul (2) din RGPD nu sunt vizate de dreptul de acces.

4.1 Definiția datelor cu caracter personal

93. Articolul 15 alineatele (1) și (3) din RGPD se referă la „*date cu caracter personal*" și, respectiv, la „*date cu caracter personal care fac obiectul prelucrării*". Prin urmare, domeniul de aplicare al dreptului de acces este determinat în primul rând de domeniul de aplicare al conceptului de „date cu caracter personal", definit la articolul 4 punctul 1 din RGPD[46]. Conceptul de „date cu caracter personal" a făcut deja obiectul mai multor documente[47] ale Grupului de lucru „Articolul 29"[48] și a fost interpretat de CJUE, inclusiv în contextul dreptului de acces în temeiul articolului 12 din Directiva 95/46/CE.

94. GL29 a considerat că definiția datelor cu caracter personal din Directiva 95/46/CE „*reflectă intenția legiuitorului european de a adopta o definiție în sens larg a noțiunii de «date cu caracter personal»*"[49]. În temeiul RGPD, definiția se referă în continuare la „*orice informații privind o persoană fizică identificată sau identificabilă*". Pe lângă datele cu caracter personal de bază, cum ar fi numele și adresa, numărul de telefon etc., o gamă variată și nelimitată de date s-ar putea încadra în această definiție, inclusiv constatările medicale, istoricul achizițiilor, indicatorii de bonitate, conținutul comunicațiilor etc. Având în vedere domeniul larg de aplicare al definiției datelor cu caracter personal, o evaluare restrictivă a acestei definiții de către operator ar conduce la o clasificare eronată a datelor cu caracter personal[50] și, în cele din urmă, la o încălcare a dreptului de acces.

---

[45] În conformitate cu principiul protecției datelor începând cu momentul conceperii, o astfel de analiză face parte din evaluarea măsurilor și a garanțiilor adecvate pentru protejarea principiilor de protecție a datelor și a drepturilor persoanelor vizate, care se efectuează „*în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine*", de exemplu reducerea timpului de răspuns în care persoanele vizate își exercită drepturile poate fi unul dintre indicatori. Pentru explicații suplimentare, a se vedea Orientările nr. 4/2019 privind articolul 25 - Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit.

[46] În conformitate cu articolul 4 punctul 1 din RGPD, „«date cu caracter personal» înseamnă orice informații privind o persoană fizică identificată sau identificabilă («persoana vizată»); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;".

[47] Grupul de lucru „Articolul 29" (GL „Articolul 29") este grupul de lucru european independent care a abordat aspecte legate de protecția vieții private și a datelor cu caracter personal până la 25 mai 2018 (intrarea în vigoare a RGPD), predecesorul CEPD.

[48] de exemplu, Orientările GL251 rev01 privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului (UE) 2016/679, și anume p. 19; Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD, p. 9.

[49] Avizul 4/2007 al Grupului de lucru „Articolul 29" privind conceptul de date cu caracter personal, p. 4.

[50] ca informații care nu se referă la o persoană fizică identificată sau identificabilă.

95. În cauzele conexate C-141/12 și C-372/12[51], CJUE a statuat că dreptul de acces vizează datele cu caracter personal conținute în minute, și anume „*numele, data nașterii, cetățenia, sexul, etnia, religia și limba [solicitantului]*” *și, „după caz, cele care figurează în analiza juridică cuprinsă în [minută]*”, dar nu și analiza juridică în sine[52]. În acest context, analiza juridică nu era susceptibilă, în sine, să facă obiectul unui control al exactității sale de către persoana vizată și nici al unei rectificări. În plus, asigurarea accesului la analiza juridică nu îndeplinește scopul de a garanta viața privată, ci accesul la documentele administrative.

96. În cauza Nowak[53], CJUE a efectuat o analiză mai amplă și a constatat că răspunsurile scrise prezentate de un candidat la un examen profesional și observațiile unui examinator cu privire la răspunsurile respective constituie date cu caracter personal referitoare la candidatul la examen. Mai precis, astfel de informații subiective sunt date cu caracter personal „*sub formă de opinii sau de aprecieri, cu condiția ca acestea să fie «referitoare» la persoana în cauză*”[54], spre deosebire de întrebările de examinare, care nu sunt considerate date cu caracter personal[55]. Astfel, o evaluare contextuală ar trebui să clarifice efectul sau rezultatul pe care o informație îl poate avea asupra unei persoane și, prin urmare, domeniul de aplicare al dreptului de acces.

Exemplul 15: o persoană are un interviu de angajare la o întreprindere. În acest context, solicitantul postului înmânează un CV și o scrisoare de candidatură. În timpul interviului, ofițerul de resurse umane ia notițe pe calculator pentru a documenta interviul. Ulterior, solicitantul, în calitate de persoană vizată, solicită accesul la datele cu caracter personal care o privesc pe care întreprinderea, în calitate de operator, le-a colectat în cursul procedurii de recrutare.

Operatorul are obligația de a furniza persoanei vizate datele cu caracter personal comunicate în mod activ de către aceasta în CV-ul său și în scrisoarea de candidatură. În plus, operatorul trebuie să furnizeze persoanei vizate rezumatul interviului, inclusiv observațiile subiective privind comportamentul persoanei vizate, pe care responsabilul cu resursele umane le-a notat în timpul interviului de angajare, sub rezerva oricăror excepții prevăzute de dreptul intern și în conformitate cu articolul 23 din RGPD.

97. Astfel, sub rezerva elementelor specifice ale cazului, atunci când se evaluează o cerere specifică de acces, următoarele tipuri de date, printre altele, trebuie să fie furnizate de operatori fără a aduce atingere articolului 15 alineatul (4) din RGPD:

- categoriile speciale de date cu caracter personal prevăzute de articolul 9 din RGPD;
- datele cu caracter personal referitoare la condamnări penale și infracțiuni, în conformitate cu articolul 10 din RGPD;
- datele furnizate în cunoștință de cauză și în mod activ de persoana vizată (de exemplu, datele privind conturile transmise prin intermediul formularelor, răspunsurile la un chestionar)[56];
- datele observate sau datele primare furnizate de persoana vizată în virtutea utilizării serviciului sau a dispozitivului (de exemplu, datele prelucrate de obiecte conectate, istoricul tranzacțiilor,

[51] CJUE, cauzele conexate C-141/12 și C-372/12, YS/Minister voor Immigratie, Integratie en Asiel și Minister voor Immigratie, Integratie en Asiel împotriva M și S, 17 iulie 2014.
[52] CJUE, cauzele conexate C-141/12 și C-372/12, YS și alții, punctele 38 și 48.
[53] CJUE, C-434/16, Peter Nowak/Data Protection Commissioner, 20 decembrie 2017.
[54] CJUE, C 434/16, Nowak, punctele 34-35.
[55] CJUE, C-434/16, Nowak, punctul 58.
[56] Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD, p. 9.

jurnalele de activitate, cum ar fi jurnalele de acces, istoricul utilizării site-ului, activitățile de căutare, datele de localizare, activitatea de accesare, aspectele unice ale comportamentului unei persoane, cum ar fi scrisul de mână, apăsarea de taste, particularități legate de mers sau de vorbire)[57];

- date derivate din alte date, mai degrabă decât furnizate direct de persoana vizată (de exemplu, rata de credit, clasificarea bazată pe atributele comune ale persoanelor vizate, țara de reședință derivată din codul poștal)[58];
- date deduse din alte date, mai degrabă decât furnizate direct de persoana vizată (de exemplu, pentru atribuirea unui punctaj de credit sau pentru respectarea normelor de combatere a spălării banilor, rezultatele algoritmice, rezultatele unei evaluări a stării de sănătate sau ale unui proces de personalizare sau de recomandare)[59];
- date pseudonimizate, spre deosebire de datele anonimizate (a se vedea, de asemenea, secțiunea 3 din prezentele orientări).

Exemplul 16: elementele care au fost utilizate pentru a se ajunge la o decizie privind, de exemplu, promovarea angajatului, mărirea salariului sau noul loc de muncă (de exemplu, evaluări anuale ale performanței, cerințe de formare, evidențe disciplinare, ierarhie, potențialul profesional) sunt date cu caracter personal referitoare la angajatul respectiv. Astfel, aceste de elemente pot fi accesate de persoana vizată la cerere și cu respectarea articolului 15 alineatul (4) din RGPD în cazul în care, de exemplu, datele cu caracter personal se referă și la o altă persoană [de exemplu, identitatea sau elementele care dezvăluie identitatea unui alt angajat a cărui mărturie cu privire la performanța profesională este inclusă într-o evaluare anuală a performanței ar putea face obiectul unor limitări în temeiul articolului 15 alineatul (4) din RGPD și, prin urmare, este posibil ca acestea să nu poată fi comunicate persoanei vizate pentru a proteja drepturile și libertățile angajatului respectiv]. Cu toate acestea, dispozițiile dreptului național al muncii se pot aplica, de exemplu, în ceea ce privește accesul angajaților la dosarele personalului sau alte dispoziții naționale, cum ar fi cele privind secretul profesional. În toate circumstanțele, astfel de restricții privind exercitarea dreptului de acces al persoanei vizate (sau a altor drepturi) prevăzute în legislația națională trebuie să respecte condițiile prevăzute la articolul 23 din RGPD (a se vedea secțiunea 6.4).

98. Din lista neexhaustivă de mai sus a datelor cu caracter personal care pot fi furnizate persoanei vizate în contextul unei cereri de acces se pot trage mai multe concluzii. Din cele de mai sus reiese că operatorul nu poate face o distincție, atunci când acordă acces la datele cu caracter personal, între datele conținute în dosarele pe suport de hârtie și cele stocate în format electronic, atât timp cât acestea intră în domeniul de aplicare al RGPD. Cu alte cuvinte, datele cu caracter personal care sunt conținute în dosare pe suport de hârtie în cadrul unui sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor intră sub incidența dreptului de acces în același mod ca și datele cu caracter personal stocate în memoria unui calculator, de exemplu prin intermediul unui cod binar sau al unei înregistrări video.

[57] Avizul 4/2007 al Grupului de lucru „Articolul 29” privind conceptul de date cu caracter personal, p. 8.
[58] Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD, p. 10-11.
[59] Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD, p. 10-11; Grupul de lucru „Articolul 29”, GL251 rev.01, 6 februarie 2018, Orientări privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului 2016/679 – aprobate de CEPD (denumite în continuare „Orientările GL29 privind procesul decizional individual automatizat și crearea de profiluri – aprobate de CEPD”), p. 9-10.

99. În plus, la fel ca majoritatea drepturilor persoanelor vizate, dreptul de acces include atât date deduse, cât și date derivate, inclusiv date cu caracter personal create de un furnizor de servicii, în timp ce dreptul la portabilitatea datelor include numai datele furnizate de persoana vizată[60]. Prin urmare, în cazul unei cereri de acces și spre deosebire de o cerere de portabilitate a datelor, persoanei vizate ar trebui să i se furnizeze nu numai datele cu caracter personal furnizate operatorului pentru a efectua o analiză sau o evaluare ulterioară cu privire la aceste date, ci și rezultatul oricărei astfel de analize sau evaluări ulterioare.

100. De asemenea, este important să se reamintească faptul că există informații, cum ar fi datele anonime[61], care sunt date ce nu se referă direct sau indirect la o persoană identificabilă și care, prin urmare, sunt excluse din domeniul de aplicare al RGPD. De exemplu, locul unde se află serverul pe care sunt prelucrate datele cu caracter personal ale persoanei vizate nu reprezintă date cu caracter personal. Distincția poate fi dificilă, iar operatorii se pot întreba cum se poate stabili o linie de demarcație clară între datele cu caracter personal și datele fără caracter personal, în special în cazul seturilor de date mixte. În acest caz, ar putea fi util să se facă o distincție între seturile de date mixte în care datele cu caracter personal și cele fără caracter personal sunt legate în mod indisolubil și cele în care nu este cazul. Datele cu caracter personal și datele fără caracter personal pot fi legate în mod indisolubil în seturi de date mixte și intră în totalitate în domeniul de aplicare al dreptului de acces al persoanei vizate la care se referă datele cu caracter personal[62]. În alte cazuri, datele cu caracter personal și datele fără caracter personal din seturile de date mixte nu pot fi legate în mod indisolubil, făcând accesibile persoanei vizate numai datele cu caracter personal din set. De exemplu, o întreprindere ar putea fi nevoită să furnizeze unei persoane vizate rapoartele individuale privind incidentele informatice pe care le-a declanșat, dar nu și baza de cunoștințe a societății cu privire la problemele informatice. Cu toate acestea, măsurile de securitate pe care le-a instituit operatorul nu trebuie, în general, să fie înțelese ca fiind date cu caracter personal, cu condiția ca acestea să nu fie legate în mod indisolubil de datele cu caracter personal și, prin urmare, să nu fie acoperite de dreptul de acces.

101. Înainte de a încheia secțiunea, CEPD reamintește, în acest context, că protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal cuprinde toate tipurile de date cu caracter personal enumerate mai sus și că o interpretare restrictivă a definiției contravine dispozițiilor RGPD și, în cele din urmă, încalcă articolul 8 din Carta drepturilor fundamentale. Aplicarea unui regim diferit pentru exercitarea unui drept în legătură cu anumite tipuri de date cu caracter personal, care nu a fost prevăzută de RGPD, poate fi introdusă exclusiv prin lege, în conformitate cu articolul 23 din RGPD (astfel cum se explică în secțiunea 6.4). Astfel, operatorii nu pot limita exercitarea dreptului de acces limitând în mod nejustificat domeniul de aplicare al datelor cu caracter personal.

4.2 Datele cu caracter personal la care se referă dreptul de acces

[60] Astfel cum s-a menționat anterior în Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD, p. 10 și cum s-a reiterat în Orientările GL29 privind procesul decizional individual automatizat și crearea de profiluri – aprobate de CEPD, p. 17.

[61] Explicații suplimentare privind conceptul de anonimizare pot fi găsite în Avizul 05/2014 al Grupului de lucru „Articolul 29" privind tehnicile de anonimizare, GL216, 10 aprilie 2014, p. 5-19.

[62] Comunicare a Comisiei către Parlamentul European și Consiliu - Orientări referitoare la Regulamentul privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană, 29.5.2019, COM/2019/250 final.

102. În conformitate cu articolul 15 alineatul (1) din RGPD, „*[p]ersoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații*" (sublinierea noastră).

103. Din articolul 15 alineatul (1) din RGPD reies mai multe elemente. Alineatul se referă *expressis verbis* la „*date cu caracter personal care o privesc*" (subsecțiunea 4.2.1), care „*se prelucrează*" (subsecțiunea 4.2.2) de către operator:

4.2.1 „date cu caracter personal care o privesc"

104. Dreptul de acces poate fi exercitat exclusiv în ceea ce privește datele cu caracter personal referitoare la persoana vizată care solicită accesul sau, după caz, de către o persoană autorizată sau un reprezentant (a se vedea secțiunea 3.4). Există, de asemenea, situații în care datele nu au o legătură cu persoana care își exercită dreptul de acces, ci cu o altă persoană. Cu toate acestea, persoana vizată are dreptul numai la datele cu caracter personal care se referă la ea însăși, excluzând datele care privesc exclusiv pe altcineva[63].

105. Cu toate acestea, clasificarea datelor ca date cu caracter personal referitoare la persoana vizată nu depinde de faptul că aceste date cu caracter personal se referă și la altcineva[64]. Prin urmare, este posibil ca datele cu caracter personal să se refere la mai multe persoane în același timp. Acest lucru nu înseamnă în mod automat că ar trebui acordat accesul la datele cu caracter personal care se referă și la altcineva, întrucât operatorul trebuie să respecte articolul 15 alineatul (4) din RGPD.

106. Expresiile „*date cu caracter personal care o privesc*" nu ar trebui interpretate într-un mod „*prea restrictiv*" de către operatori, astfel cum a afirmat deja Grupul de lucru „Articolul 29" cu privire la dreptul la portabilitatea datelor[65]. Aplicat dreptului de acces, CEPD consideră, de exemplu, că înregistrările convorbirilor telefonice (și transcrierea acestora) dintre persoana vizată care solicită accesul și operator pot intra sub incidența dreptului de acces, cu condiția ca acestea din urmă să fie date cu caracter personal[66]. Cu condiția ca RGPD să se aplice și ca prelucrarea să nu facă obiectul excepției privind activitățile domestice prevăzute la articolul 2 alineatul (2) litera (c) din RGPD, dacă persoana vizată utilizează înregistrarea obținută care include date cu caracter personal ale interlocutorului în alte scopuri, de exemplu, prin publicarea înregistrării, persoana vizată va deveni operator pentru această prelucrare a datelor cu caracter personal referitoare la cealaltă persoană a cărei voce a fost înregistrată. Deși acest lucru nu îl va scuti pe operator de obligațiile sale în materie de

---

[63] Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD, p. 9: „*Numai datele cu caracter personal intră în domeniul de aplicare al unei cereri de portabilitate a datelor. Prin urmare, orice date care sunt anonime sau nu privesc persoana vizată nu se află în domeniul de aplicare. Cu toate acestea, datele pseudonime care pot fi legate în mod clar de o persoană vizată, [de exemplu, furnizând identificatorul respectiv, conform articolului 11 alineatul (2)] se află în domeniul de aplicare.*"

[64] Hotărârea CJUE în cauza C-434/16, Peter Nowa/Data Protection Commissioner, 2017, punctul 44.

[65] Ghidul GL29 privind dreptul la portabilitatea datelor – aprobat de CEPD, p. 9: *„În multe situații, operatorii vor prelucra informații care conțin datele cu caracter personal ale mai multor persoane vizate. În acest caz, operatorii nu ar trebui să abordeze o interpretare prea restrictivă a sintagmei «datele cu caracter personal referitoare la o persoană vizată». Ca exemplu, telefonul, mesajele interpersonale sau înregistrările VoIP pot include (în istoricul contului abonatului) detalii ale unor părți terțe implicate în apelurile primite sau efectuate. Cu toate că înregistrările vor conține date cu caracter personal referitoare la mai multe persoane, abonații ar trebui să poată să aibă aceste înregistrări furnizate ca răspuns la cererile de portabilitate a datelor, întrucât înregistrările se referă (de asemenea) la persoana vizată. Totuși, în situația în care aceste înregistrări sunt transmise către un nou operator, acest nou operator nu ar trebui să le prelucreze în alt scop care ar putea aduce atingere drepturilor și libertăților unor părți terțe (a se vedea mai jos: a treia condiție).*"

[66] A se vedea exemplul 34 din subsecțiunea 6.2.

protecție a datelor atunci când analizează în mod corespunzător dacă se poate acorda acces la înregistrarea completă, operatorul este încurajat să informeze persoana vizată cu privire la faptul că aceasta poate deveni operator în acest caz. Acest lucru nu aduce atingere niciunei evaluări suplimentare în temeiul articolului 15 alineatul (4) din RGPD, prezentată în detaliu în secțiunea 6. În aceeași ordine de idei, mesajele pe care persoanele vizate le-au trimis altor persoane sub formă de mesaje interpersonale și pe care le-au șters de pe dispozitivul lor, care sunt încă accesibile prestatorului de servicii, ar putea intra sub incidența dreptului de acces.

107. Din nou, există situații în care legătura dintre date și mai multe persoane poate părea neclară pentru operator, cum ar fi în cazul furtului de identitate. În cazul furtului de identitate, o persoană acționează în mod fraudulos în numele altei persoane. În acest context, este important să se reamintească faptul că victimei ar trebui să i se furnizeze informații cu privire la toate datele cu caracter personal pe care operatorul le stochează în legătură cu identitatea sa, inclusiv cele care au fost colectate pe baza acțiunilor autorului fraudei. Cu alte cuvinte, chiar și după ce operatorul a luat cunoștință de furtul de identitate, datele cu caracter personal care sunt asociate sau legate de identitatea victimei constituie date cu caracter personal ale persoanei vizate.

Exemplul 17: o persoană utilizează în mod fraudulos identitatea altcuiva pentru a juca poker online. Autorul infracțiunii efectuează plata către cazinoul online cu cardul de credit pe care l-a furat de la victimă. Atunci când află despre furtul de identitate, victima solicită furnizorului cazinoului online să îi ofere acces la datele sale cu caracter personal și, mai precis, la jocurile online jucate și informațiile despre cartea de credit utilizată de autor.

Există o legătură între datele colectate și victimă, deoarece identitatea acesteia din urmă a fost utilizată. După detectarea fraudei, datele cu caracter personal menționate mai sus au în continuare o legătură prin conținutul (cardul de credit al victimei se referă în mod clar la victimă), scopul și efectul lor (informațiile privind jocurile online jucate de autorul infracțiunii pot fi utilizate, de exemplu, pentru emiterea de facturi către victimă). Prin urmare, cazinoul online trebuie să acorde victimei acces la datele cu caracter personal menționate anterior.

108. Dacă este cazul, se pot utiliza jurnale interne de conectare pentru a ține evidența accesului la un fișier și pentru a identifica acțiunile întreprinse în legătură cu accesul la o înregistrare, cum ar fi prin imprimarea, copierea sau ștergerea datelor cu caracter personal. Aceste înregistrări pot include momentul înregistrării, motivul accesului la fișier, precum și informații de identificare a persoanei care a avut acces. Întrebări referitoare la acest subiect sunt în discuție într-o cauză aflată în prezent pe rolul CJUE (C-579/21). Punerea în aplicare, supravegherea și revizuirea registrelor de conectare intră în responsabilitatea operatorului și pot fi verificate de autoritățile de supraveghere. Prin urmare, operatorul ar trebui să se asigure că persoanele care acționează sub autoritatea sa și care au acces la datele cu caracter personal nu prelucrează date cu caracter personal decât la instrucțiunile operatorului, în conformitate cu articolul 29 din RGPD. În cazul în care persoana prelucrează totuși datele cu caracter personal în alte scopuri decât îndeplinirea instrucțiunilor operatorului, aceasta poate deveni operator pentru prelucrarea respectivă și poate face obiectul unor proceduri disciplinare sau penale sau al unor sancțiuni administrative emise de autoritățile de supraveghere. CEPD ia act de faptul că este responsabilitatea angajatorului în temeiul articolului 24 din RGPD să utilizeze măsuri adecvate, de la educație la proceduri disciplinare, pentru a se asigura că prelucrarea este în conformitate cu RGPD și că nu are loc nicio încălcare.

4.2.2 Date cu caracter personal care „se prelucrează”

109. Alineatul (1) de la articolul 15 din RGPD se referă, de asemenea, la datele cu caracter personal, care „se prelucrează”. Termenul de referință pentru stabilirea gamei de date cu caracter personal care se încadrează în cererea de acces a fost deja prezentat în subsecțiunea 2.3.3. Cu toate acestea, formularea sugerează, de asemenea, că dreptul de acces nu face distincție între scopurile operațiunilor de prelucrare.

Exemplul 18: o societate a prelucrat date cu caracter personal referitoare la o persoană vizată pentru a prelucra ordinul de achiziție și pentru a organiza expedierea la adresa de domiciliu a persoanei vizate. După ce aceste scopuri inițiale pentru care au fost colectate datele cu caracter personal nu mai există, operatorul păstrează unele dintre datele cu caracter personal exclusiv pentru a se conforma obligațiilor sale legale privind ținerea evidențelor.

Persoana vizată solicită acces la datele cu caracter personal care o privesc. Pentru a respecta obligația care îi revine în temeiul articolului 15 alineatul (1) din RGPD, operatorul trebuie să furnizeze persoanei vizate datele cu caracter personal solicitate care sunt stocate pentru a-și respecta obligațiile legale.

110. Datele cu caracter personal arhivate trebuie să fie diferențiate de datele de rezervă care sunt date cu caracter personal stocate exclusiv în scopul recuperării în cazul unui eveniment de pierdere a datelor. Trebuie subliniat că, în ceea ce privește principiile protecției datelor începând cu momentul conceperii și reducerii la minimum a datelor, datele de rezervă sunt, în principiu, similare cu datele din sistemul principal. În cazul în care există mici diferențe între datele cu caracter personal din sistemul de copii de rezervă și cele din sistemul principal de producție, acestea sunt, în general, legate de colectarea de date suplimentare de la ultima copie de rezervă. O scădere a datelor din sistemul principal (de exemplu, ștergerea datelor după încheierea perioadei de păstrare a unor date sau în urma unei cereri de ștergere) va fi, în unele cazuri, suprascrisă în datele de rezervă la momentul copierii ulterioare. Când se înaintează o cerere de acces în momentul în care există mai multe date cu caracter personal referitoare la persoana vizată în sistemul de copii de rezervă decât în sistemul principal sau date cu caracter personal diferite (care pot fi observate, de exemplu, prin înregistrarea ștergerilor din sistemul de producție principal, puse în aplicare cu respectarea deplină a principiului reducerii la minimum a datelor), operatorul trebuie să fie transparent cu privire la această situație și, dacă e fezabil din punct de vedere tehnic, să acorde accesul, astfel cum a solicitat persoana vizată, inclusiv la datele cu caracter personal stocate în sistemul de copii de rezervă. De exemplu, cu scopul de a asigura transparența pentru persoanele vizate care își exercită dreptul, o evidență a ștergerilor din sistemul de producție principal îi poate permite operatorului să vadă că există date în sistemul de copii de rezervă care nu mai sunt în sistemul principal, deoarece au fost șterse recent și nu au fost încă suprascrise în sistemul de copii de rezervă.

4.2.3 Domeniul de aplicare al unei noi cereri de acces

111. Rămâne de spus că persoanele vizate au dreptul de acces la toate datele prelucrate care le privesc sau la părți ale datelor, în funcție de domeniul de aplicare al cererii (a se vedea, de asemenea, subsecțiunea 2.3.1 privind caracterul complet al informațiilor și subsecțiunea 3.1.1 pentru analiza conținutului cererii). Drept consecință, în cazul în care un operator a dat deja curs unei cereri de acces în trecut și cu condiția ca cererea să nu fie excesivă, operatorul nu poate restrânge domeniul de aplicare al acestei noi cereri. Aceasta înseamnă că, în legătură cu orice cerere suplimentară de acces din partea aceleiași persoane vizate, operatorul nu ar trebui să informeze persoana vizată numai cu privire la simplele modificări ale datelor cu caracter personal prelucrate sau ale prelucrării în sine de la ultima cerere, cu excepția cazului în care persoana vizată este de acord în mod expres cu acest lucru.

În caz contrar, persoanele vizate ar fi obligate să își compileze datele cu caracter personal furnizate pentru a obține un set complet de date cu caracter personal referitoare la informațiile cu privire la prelucrare și la drepturile persoanelor vizate.

4.3 Informații privind prelucrarea și drepturile persoanelor vizate

112. Pe lângă accesul la datele cu caracter personal propriu-zise, operatorul trebuie să furnizeze informații cu privire la prelucrare și la drepturile persoanelor vizate, în conformitate cu articolul 15 alineatul (1) literele (a)-(h) și cu articolul 15 alineatul (2) din RGPD. Majoritatea informațiilor cu privire la aceste puncte specifice sunt deja compilate, cel puțin în formă generală, în evidențele operatorului privind activitățile de prelucrare menționate la articolul 30 din RGPD și/sau în declarația sa de confidențialitate elaborată în conformitate cu articolele 12-14 din RGPD. Prin urmare, ar putea fi util, ca prim pas, să se consulte „Orientările privind transparența în temeiul Regulamentului 2016/679”[67] ale Grupului de lucru „Articolul 29” cu privire la conținutul informațiilor care trebuie furnizate în temeiul articolelor 13 și 14 din RGPD.

113. Pentru a se conforma articolului 15 alineatul (1) literele (a)-(h) și articolului 15 alineatul (2), operatorii ar putea utiliza cu atenție modulele de text ale declarației lor de confidențialitate, atât timp cât se asigură că acestea sunt actualizate și precise în ceea ce privește cererea persoanei vizate. De multe ori, înainte de prelucrarea sau la începutul prelucrării datelor, unele informații, cum ar fi identificarea destinatarilor specifici sau durata specifică a prelucrării datelor, nu pot fi încă furnizate. Unele informații, cum ar fi, de exemplu, dreptul de a depune o plângere la o autoritate de supraveghere [a se vedea articolul 15 alineatul (1) litera (f)], nu se schimbă în funcție de persoana care înaintează cererea de acces. Prin urmare, acestea pot fi comunicate în termeni generali, astfel cum se procedează și în declarația de confidențialitate. Alte tipuri de informații, cum ar fi informațiile privind destinatarii, categoriile și sursa datelor, pot varia în funcție de persoana care înaintează cererea și de domeniul de aplicare al cererii. În contextul unei cereri de acces în temeiul articolului 15, orice informație privind prelucrarea de care dispune operatorul poate necesita, prin urmare, să fie actualizată și adaptată pentru operațiunile de prelucrare efectuate efectiv în ceea ce privește persoana vizată care înaintează cererea. Astfel, trimiterea la formularea declarației sale de confidențialitate nu ar fi o modalitate suficientă pentru ca operatorul să furnizeze informațiile prevăzute la articolul 15 alineatul (1) literele (a)-(h) și la articolul 15 alineatul (2), cu excepția cazului în care informațiile „adaptate și actualizate” sunt aceleași cu informațiile furnizate la începutul prelucrării. Pentru a oferi explicații cu privire la informațiile care se referă la persoana solicitantă, operatorul ar putea, după caz, să facă referire la anumite activități (de exemplu „dacă ați utilizat acest serviciu...”, „dacă ați plătit pe baza unei facturi”), atât timp cât acest lucru este evident pentru persoanele vizate și dacă se referă la acestea. În cele ce urmează, este explicat gradul de detaliere necesar în legătură cu tipurile individuale de informații.

114. Informațiile privind scopurile în conformitate cu articolul 15 alineatul (1) litera (a) trebuie să fie specifice în ceea ce privește scopul (scopurile) exact(e) în cazul efectiv al persoanei vizate solicitante. Nu ar fi suficient să se enumere scopurile generale ale operatorului fără a clarifica scopul (scopurile) urmărit(e) de operator în cazul de față al persoanei vizate solicitante. În cazul în care prelucrarea este efectuată în mai multe scopuri, operatorul trebuie să clarifice ce date sau ce categorii de date sunt prelucrate și scopul (scopurile) prelucrării. Spre deosebire de articolul 13 alineatul (1) litera (c) și articolul 14 alineatul (1) litera (c) din RGPD, informațiile privind prelucrarea menționate la articolul 15

[67] Grupul de lucru „Articolul 29”, GL260 rev.01, 11 aprilie 2018, Orientări privind transparența în temeiul Regulamentului 2016/679 – aprobate de CEPD (denumite în continuare „Orientările GL29 privind transparența – aprobate de CEPD”).

alineatul (1) litera (a) nu conțin informații privind temeiul juridic al prelucrării. Cu toate acestea, întrucât unele drepturi ale persoanelor vizate depind de temeiul juridic aplicabil, aceste informații sunt importante pentru ca persoanele vizate să verifice legalitatea prelucrării datelor și să determine care drepturi ale persoanei vizate sunt aplicabile în situația specifică. Prin urmare, pentru a facilita exercitarea drepturilor persoanelor vizate în conformitate cu articolul 12 alineatul (2) din RGPD, se recomandă operatorului să informeze, de asemenea, persoana vizată cu privire la temeiul juridic aplicabil pentru fiecare operațiune de prelucrare sau să indice de unde poate obține aceste informații. În orice caz, principiul prelucrării transparente impune ca informațiile privind temeiurile juridice ale prelucrării să fie puse la dispoziția persoanei vizate într-un mod accesibil (de exemplu, într-o declarație de confidențialitate).

115. Este posibil ca informațiile privind categoriile de date [articolul 15 alineatul (1) litera (b)] să trebuiască, de asemenea, să fie adaptate la situația persoanei vizate, astfel încât categoriile care s-au dovedit a nu fi relevante în cazul solicitantului să fie eliminate.

Exemplul 19: în contextul informațiilor menționate la articolele 13-14 din RGPD, un hotel declară că prelucrează o serie de categorii de date ale clienților (date de identificare, date de contact, date bancare și numerele cărților de credit etc.). În cazul în care se înaintează o cerere de acces în temeiul articolului 15, persoana vizată care înaintează cererea trebuie, pe lângă accesul la datele efective care sunt prelucrate (componenta 2), în conformitate cu articolul 15 alineatul (1) litera (b), să fie, de asemenea, informată cu privire la categoriile specifice de date care sunt prelucrate în cazul respectiv (de exemplu, neincluderea datelor bancare sau a datelor privind cartea de credit în cazul în care plata a fost efectuată în numerar).

116. Informațiile privind „destinatarii sau categoriile de destinatari" [articolul 15 alineatul (1) litera (c)] trebuie să țină seama în primul rând de definiția noțiunii de „destinatar" prevăzută la articolul 4 punctul 9 din RGPD. Definiția noțiunii de „destinatar" se bazează pe divulgarea datelor cu caracter personal către o persoană fizică sau juridică, o autoritate publică, o agenție sau un alt organism[68]. Din articolul 4 punctul 9 din RGPD rezultă că autoritățile publice care acționează în cadrul unei anumite anchete care face obiectul unor dispoziții naționale specifice nu trebuie considerate destinatari.

117. În ceea ce privește întrebarea dacă operatorul este liber să aleagă între informațiile privind destinatarii sau categoriile de destinatari, trebuie remarcat faptul că „spre deosebire de articolele 13 și 14 din RGPD, care stabilesc o obligație în sarcina operatorului [...], articolul 15 din RGPD prevede un veritabil drept de acces în favoarea persoanei vizate, astfel încât aceasta din urmă trebuie să dispună de alegerea de a obține fie informațiile cu privire la destinatarii specifici cărora le- au fost sau urmează să le fie divulgate datele respective, atunci când aceasta este posibilă, fie pe cele referitoare la categoriile de destinatari."[69] De asemenea, trebuie reamintit faptul că, astfel cum se menționează în orientările privind transparența menționate mai sus[70], informațiile privind destinatarii sau categoriile de destinatari prevăzute de articolele 13 și 14 din RGPD ar trebui să fie cât mai concrete posibil în ceea ce

[68] De asemenea, ar trebui remarcat faptul că în cadrul aceleiași societăți pot exista operatori diferiți, astfel cum sunt definiți la articolul 4 punctul 7 din RGPD. În acest caz, este posibilă divulgarea datelor de la un destinatar la altul în cadrul unei societăți.

[69] CJUE, C-154/21 (Österreichische Post AG), punctul 36.

[70] Grupul de lucru „Articolul 29", GL260 rev.01, 11 aprilie 2018, Orientări privind transparența în temeiul Regulamentului 2016/679 – aprobate de CEPD (denumite în continuare „Orientările GL29 privind transparența – aprobate de CEPD"), p. 37 (Anexă).

privește principiile transparenței și echității. În temeiul articolului 15, în cazul în care persoana vizată nu a ales altfel, operatorul este obligat să numească destinatarii efectivi, cu excepția cazului în care este imposibil să se identifice destinatarii respectivi sau dacă operatorul demonstrează că cererile de acces ale persoanei vizate sunt în mod vădit nefondate sau excesive în sensul articolului 12 alineatul (5) din RGPD[71] [72]. CEPD reamintește, în acest sens, că stocarea informațiilor referitoare la destinatarii reali este necesară, printre altele, pentru a se putea respecta obligațiile operatorului în temeiul articolului 5 alineatul (2) și al articolului 19 din RGPD.

Exemplul 20: în declarația sa de confidențialitate, un angajator oferă informații cu privire la categoriile de date care sunt transmise „agenților de voiaj" sau „hotelurilor" în cazul călătoriilor de afaceri, în conformitate cu articolul 13 alineatul (1) litera (e) și cu articolul 14 alineatul (1) litera (e) din RGPD. În cazul în care un angajat depune o cerere de acces la datele cu caracter personal după efectuarea călătoriilor de afaceri, angajatorul ar trebui, în ceea ce privește destinatarii datelor cu caracter personal în temeiul articolului 15 alineatul (1) litera (c), să indice în răspunsul său agenția (agențiile) de voiaj și hotelul (hotelurile) care au primit datele. Deși angajatorul a făcut referire în mod legitim la categorii de destinatari în declarația sa de confidențialitate în temeiul articolelor 13 și 14, deoarece, în această etapă, nu era încă posibil să-i numească pe destinatari, acesta ar trebui, cu excepția cazului în care angajatul a ales altfel, să furnizeze informații cu privire la destinatarii specifici (numele agenților de voiaj, hotelurilor etc.) atunci când angajatul înaintează o cerere de acces.

În cazul în care, respectând condițiile menționate mai sus, un operator poate furniza numai categoriile de destinatari, informațiile ar trebui să fie cât mai specifice posibil, indicând tipul de destinatar (și anume prin referire la activitățile pe care le desfășoară), industria, sectorul și subsectorul și localizarea destinatarilor[73].

118. În conformitate cu articolul 15 alineatul (1) litera (d), atunci când este posibil, trebuie furnizate informații cu privire la perioada pentru care se preconizează că vor fi stocate datele cu caracter personal. În caz contrar, trebuie furnizate criteriile utilizate pentru stabilirea acestei perioade. Informațiile furnizate de operator trebuie să fie suficient de precise pentru ca persoana vizată să știe cât timp vor continua să fie stocate datele referitoare la persoana vizată. În cazul în care nu este posibil să se specifice momentul ștergerii, se specifică durata termenelor de stocare și începutul acestei perioade sau evenimentul declanșator (de exemplu, rezilierea unui contract, expirarea unei perioade de garanție etc.). Simpla referire, de exemplu, la „ștergerea după expirarea termenelor legale de stocare" nu este suficientă. Indicațiile privind perioadele de stocare a datelor vor trebui să se axeze pe datele specifice referitoare la persoana vizată. În cazul în care datele cu caracter personal ale persoanei vizate fac obiectul unor termene diferite de ștergere (de exemplu, pentru că nu toate datele fac obiectul unor obligații legale de stocare), termenele de ștergere trebuie specificate în legătură cu operațiunile de prelucrare și categoriile de date respective.

119. În timp ce informațiile privind dreptul de a depune o plângere la o autoritate de supraveghere [articolul 15 alineatul (1) litera (f)] nu depind de circumstanțele specifice, drepturile persoanelor vizate menționate la articolul 15 alineatul (1) litera (e) variază în funcție de temeiul juridic care stă la baza prelucrării. În ceea ce privește obligația sa de a facilita exercitarea drepturilor persoanelor vizate în temeiul articolului 12 alineatul (2) din RGPD, răspunsul operatorului cu privire la aceste drepturi este

[71] CJUE, C-154/21 (Österreichische Post AG).

[72] Simplul fapt că datele au fost divulgate unui număr mare de destinatari nu ar face, în sine, cererea excesivă; a se vedea secțiunea 6 punctul 188.

[73] Orientările GL29 privind transparența – aprobate de CEPD, p. 37 (Anexă).

adaptat în mod individual la cazul persoanei vizate și se referă la operațiunile de prelucrare în cauză. Informațiile privind drepturile care nu sunt aplicabile persoanei vizate în situația specifică ar trebui evitate.

120. În conformitate cu articolul 15 alineatul (1) litera (g), trebuie furnizate „orice informații disponibile" cu privire la sursa datelor, în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată. Gradul disponibilității informațiilor se poate modifica în timp.

Exemplul 21: declarația de confidențialitate a unei întreprinderi mari prevede:

„Verificările solvabilității ne ajută să prevenim problemele legate de operațiunile de plată. Acestea garantează protecția societății noastre împotriva riscurilor financiare, care pot afecta, de asemenea, prețurile de vânzare pe termen mediu și lung. Verificarea solvabilității se efectuează neapărat în cazurile în care urmează să livrăm bunuri fără a primi prețul de achiziție respectiv în același timp, de exemplu în cazul unei achiziții pe credit. Fără efectuarea verificării solvabilității, este posibilă doar opțiunea de plată anticipată (transfer bancar imediat, furnizor de plăți online, card de credit).

În scopul verificării solvabilității, vom trimite numele, adresa și data nașterii dumneavoastră următorilor furnizori de servicii, de exemplu: (1) agenția de informații financiare X (2) furnizorul de informații comerciale Y, (3) agenția de referință pentru credite comerciale Z.

Datele sunt transmise instituțiilor de credit menționate mai sus numai în măsura a ceea ce este permis din punct de vedere legal și numai în scopul analizei comportamentului dumneavoastră anterior privind plățile, precum și pentru evaluarea riscului de neplată pe baza unor proceduri matematico-statistice care utilizează date privind adresele, precum și pentru verificarea adresei dumneavoastră (verificarea livrării). În funcție de rezultatul verificării solvabilității, este posibil să nu vă mai putem oferi metode de plată individuale, cum ar fi achizițiile pe bază de facturi."

Prin urmare, declarația de confidențialitate conține informații generale privind posibilitatea de a obține informații de la birourile de informații economice enumerate, în conformitate cu articolele 13 și 14 din RGPD. Dacă nu este clar *ex ante* care dintre societăți vor fi implicate în prelucrare, este suficient să se menționeze în declarația de confidențialitate denumirile societăților eligibile. În contextul unei cereri în temeiul articolului 15, pe lângă informațiile conform cărora au fost obținute informații privind bonitatea, ar fi necesar să se dezvăluie (*ex post*) care dintre societățile menționate au fost mai exact implicate. Articolul 15 alineatul (1) litera (g) prevede în mod clar că informațiile privind prelucrarea datelor cuprind „orice informații disponibile privind sursa acestora" în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată.

121. Articolul 15 alineatul (1) litera (h) prevede că orice persoană vizată ar trebui să aibă dreptul de a fi informată, într-un mod semnificativ, printre altele, cu privire la existența și logica subiacentă a procesului decizional automatizat, inclusiv crearea de profiluri referitoare la persoana vizată, precum și cu privire la importanța și consecințele preconizate pe care le-ar putea avea o astfel de prelucrare[74]. Dacă este posibil, informațiile prevăzute la articolul 15 alineatul (1) litera (h) trebuie să fie mai specifice în ceea ce privește raționamentul care a condus la decizii specifice privind persoana vizată care a solicitat accesul.

[74] A se vedea, în acest sens, Orientările privind transparența în temeiul Regulamentului 2016/679 (GL260), punctul 41, cu trimitere la Orientările privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului 2016/679 (GL251).

122. În temeiul articolului 13 alineatul (1) litera (f) și al articolului 14 alineatul (1) litera (f) din RGPD, trebuie furnizate informații cu privire la transferurile de date preconizate către o țară terță sau către o organizație internațională, inclusiv existența unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate. În contextul unei cereri de acces în temeiul articolului 15, articolul 15 alineatul (2) impune furnizarea de informații privind garanțiile adecvate în temeiul articolului 46 din RGPD numai în cazurile în care are loc efectiv un transfer către o țară terță sau o organizație internațională.

5 CUM POATE UN OPERATOR SĂ OFERE ACCES?

123. RGPD nu este foarte prescriptiv în ceea ce privește modul în care operatorul trebuie să ofere acces. Dreptul de acces poate fi ușor și direct de aplicat în anumite situații, de exemplu atunci când o organizație mică deține informații limitate cu privire la persoana vizată. În alte situații, dreptul de acces este mai complicat, deoarece prelucrarea datelor este mai complexă; în ceea ce privește numărul de persoane vizate, categoriile de date prelucrate, precum și fluxul de date în cadrul diferitelor organizații și între acestea. Având în vedere diferențele în ceea ce privește prelucrarea datelor cu caracter personal, modalitatea adecvată de a oferi acces poate varia în consecință.

124. Această secțiune urmărește să ofere orientări și exemple practice cu privire la diferitele modalități prin care operatorii pot să se conformeze unei cereri de acces, precum și cu privire la sensul articolului 12 alineatul (1) din RGPD în ceea ce privește dreptul de acces. Această secțiune va oferi, de asemenea, orientări cu privire la ceea ce se consideră a fi un format electronic utilizat în mod curent, precum și cu privire la calendarul pentru furnizarea accesului în temeiul articolului 12 alineatul (3) din RGPD.

5.1 Cum poate operatorul să extragă datele solicitate?

125. Persoanele vizate ar trebui să aibă acces la toate informațiile pe care operatorul le prelucrează în ceea ce le privește. Aceasta înseamnă, de exemplu, că operatorul este obligat să caute date cu caracter personal în sistemele sale informatice și neinformatice de evidență a datelor. Atunci când efectuează o astfel de căutare, operatorul ar trebui să utilizeze informațiile disponibile în cadrul organizației cu privire la persoana vizată, care ar putea genera concordanțe la nivelul sistemelor, în funcție de modul în care sunt structurate informațiile[75]. De exemplu, în cazul în care informațiile sunt sortate în fișiere în funcție de denumire sau de un număr de referință, căutarea s-ar putea limita la acești factori. Cu toate acestea, în cazul în care structura datelor depinde de alți factori, cum ar fi relațiile de familie sau titlurile profesionale sau orice tip de identificatori direcți sau indirecți (de exemplu, numărul de client, numele de utilizator sau adresele IP), căutarea trebuie extinsă pentru a include acești factori, cu condiția ca operatorul să dețină și aceste informații referitoare la persoana vizată sau ca informațiile respective să îi fie furnizate de către persoana vizată. Același lucru este valabil și în cazul în care este probabil ca înregistrările referitoare la persoane terțe să conțină date cu caracter personal referitoare la persoana vizată. Cu toate acestea, operatorul nu poate solicita persoanei vizate să furnizeze mai multe informații decât este necesar pentru identificarea persoanei vizate. În cazul în care un operator recurge la o persoană împuternicită de operator pentru activitățile sale de prelucrare a datelor, căutarea trebuie extinsă în mod firesc pentru a include și datele cu caracter personal prelucrate de persoana împuternicită de operator.

[75] O astfel de căutare ar trebui să includă, în mod firesc, și informațiile deținute de o persoană împuternicită de operator; a se vedea articolul 28 alineatul (3) litera (e) din RGPD.

126. În conformitate cu articolul 25 din RGPD privind protecția datelor începând cu momentul conceperii și în mod implicit, operatorul (și orice persoană împuternicită de operator pe care o utilizează) ar trebui, de asemenea, să fi pus deja în aplicare funcții care să permită respectarea drepturilor persoanelor vizate. Aceasta înseamnă, în acest context, că ar trebui să existe modalități adecvate de a găsi și de a extrage informații cu privire la o persoană vizată atunci când tratează o cerere. Cu toate acestea, ar trebui remarcat faptul că o interpretare excesivă în această privință ar putea conduce la funcții de căutare și de extragere a informațiilor care, în sine, prezintă un risc pentru viața privată a persoanelor vizate. Prin urmare, este important să se țină seama de faptul că procesul de extragere a datelor ar trebui, de asemenea, să fie conceput într-un mod favorabil protecției datelor, astfel încât să nu compromită viața privată a altor persoane, de exemplu a angajaților operatorului.

5.2 Măsuri adecvate pentru acordarea accesului

5.2.1 Luarea „măsurilor adecvate”

127. Articolul 12 din RGPD stabilește cerințele pentru acordarea accesului, și anume pentru furnizarea confirmării, a datelor cu caracter personal și a informațiilor suplimentare în temeiul articolului 15, și specifică, de asemenea, forma, modalitatea și termenul în ceea ce privește dreptul de acces. „Orientările privind transparența în temeiul Regulamentului 2016/679”[76] ale Grupului de lucru „Articolul 29” oferă orientări suplimentare în ceea ce privește articolul 12, în principal în ceea ce privește articolele 13 și 14 din RGPD, dar și în ceea ce privește articolul 15 și transparența în general. Astfel, ceea ce este definit în aceste orientări se poate aplica adesea în egală măsură în ceea ce privește acordarea accesului în temeiul articolului 15.

128. Articolul 12 alineatul (1) din RGPD prevede că operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice comunicare în temeiul articolului 15 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Articolul 12 alineatul (2) prevede că operatorul facilitează exercitarea dreptului de acces persoanei vizate. Cerințele mai precise în această privință vor trebui evaluate de la caz la caz. Atunci când decid ce măsuri sunt adecvate, operatorii trebuie să ia în considerare toate circumstanțele relevante, inclusiv, dar fără a se limita la volumul de date prelucrate, complexitatea prelucrării datelor și cunoștințele pe care le dețin cu privire la persoanele lor vizate, de exemplu dacă majoritatea persoanelor vizate sunt copii, persoane în vârstă sau persoane cu dizabilități. În plus, în situațiile în care operatorul este informat cu privire la oricare nevoi speciale ale persoanei vizate care înaintează cererea, de exemplu prin furnizarea de informații suplimentare în cererea depusă, operatorul trebuie să ia în considerare aceste circumstanțe. Drept urmare, măsurile adecvate vor varia.

129. Atunci când se efectuează evaluarea, este important să se țină seama de faptul că termenul „adecvate” nu ar trebui să fie înțeles niciodată ca o modalitate de limitare a domeniului de aplicare al datelor care fac obiectul dreptului de acces. Termenul „adecvate” nu înseamnă că eforturile de furnizare a informațiilor pot fi puse în balanță, de exemplu, cu vreun interes pe care persoana vizată l-ar putea avea în obținerea datelor cu caracter personal. În schimb, evaluarea ar trebui să aibă ca scop alegerea celei mai adecvate metode pentru furnizarea tuturor informațiilor acoperite de acest drept, în funcție de circumstanțele specifice fiecărui caz. În consecință, un operator care prelucrează un volum mare de date la scară largă trebuie să accepte să depună eforturi considerabile pentru a asigura dreptul de

[76] Grupul de lucru „Articolul 29”, GL260 rev.01, 11 aprilie 2018, Orientări privind transparența în temeiul Regulamentului 2016/679 – aprobate de CEPD (denumite în continuare „Orientările GL29 privind transparența – aprobate de CEPD”).

acces al persoanelor vizate într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

130. Trebuie să se evite îndrumarea persoanei vizate către diferite surse ca răspuns la o cerere de acces la date. Astfel cum s-a menționat anterior în Orientările GL29 privind transparența (în ceea ce privește noțiunea de „furnizare" de la articolele 13 și 14 din RGPD), noțiunea de „furnizare" implică faptul că *„[p]ersoana vizată nu trebuie să fie nevoită să caute în mod activ informațiile vizate de aceste articole printre alte informații, cum ar fi termenii și condițiile de utilizare a unui site sau ale unei aplicații"*[77]. Prin urmare, în ceea ce privește principiul transparenței, persoanele vizate trebuie să obțină de la operator informațiile și datele cu caracter personal prevăzute la articolul 15 alineatele (1), (2) și (3) într-un mod care să permită accesul complet la informațiile solicitate. În circumstanțe speciale, ar fi inadecvat sau chiar ilegal să se facă schimb de informații în cadrul operatorului, de exemplu din cauza caracterului sensibil al informațiilor (cum ar fi informațiile referitoare la avertizarea în interes public). În aceste cazuri, ar fi oportun să se împartă informațiile în mai multe răspunsuri ca răspuns la cererea de acces a persoanelor vizate. Metoda aleasă de operator trebuie să furnizeze efectiv persoanei vizate datele și informațiile solicitate și, prin urmare, nu ar fi adecvat ca persoana vizată să fie îndrumată exclusiv să verifice datele solicitate stocate pe propriul dispozitiv, inclusiv, de exemplu, să verifice istoricul activităților și adresele IP de pe telefonul său mobil.

131. În conformitate cu principiul responsabilității, un operator trebuie să își documenteze abordarea pentru a putea demonstra că mijloacele alese pentru a furniza informațiile necesare în temeiul articolului 15 sunt adecvate în circumstanțele respective.

5.2.2 Diferite mijloace de acordare a accesului

132. Astfel cum s-a explicat deja în subsecțiunea 2.2.2 de mai sus, atunci când înaintează o cerere de acces, persoanele vizate au dreptul de a primi o copie a datelor lor care fac obiectul prelucrării în temeiul articolului 15 alineatul (3), împreună cu informațiile suplimentare, care sunt considerate principala modalitate de acordare a accesului la datele cu caracter personal.

133. Cu toate acestea, în anumite circumstanțe, ar putea fi oportun ca operatorul să acorde acces prin alte mijloace decât furnizarea unei copii. Astfel de modalități nepermanente de acordare a accesului la date ar putea fi, de exemplu: informații transmise verbal, consultarea dosarelor, acces la fața locului sau de la distanță fără posibilitate de descărcare. Acestea pot fi modalități adecvate de acordare a accesului, de exemplu în cazurile în care acest lucru este în interesul persoanei vizate sau în cazul în care persoana vizată solicită acest lucru. Accesul la fața locului ar putea fi, de asemenea, adecvat, ca măsură inițială, atunci când un operator gestionează un volum mare de date nedigitalizate pentru a permite persoanei vizate să fie informată cu privire la datele cu caracter personal în curs de prelucrare și să poată lua o decizie în cunoștință de cauză cu privire la datele cu caracter personal pe care dorește să le furnizeze printr-o copie. Modalitățile de acces nepermanente pot fi suficiente și adecvate în anumite situații; de exemplu, pot satisface necesitatea persoanelor vizate de a verifica dacă datele prelucrate de operator sunt corecte, oferind-le acestora posibilitatea de a vizualiza datele inițiale. Un operator nu este obligat să furnizeze informațiile prin alte mijloace decât furnizarea unei copii, dar ar trebui să adopte o abordare rezonabilă atunci când examinează o astfel de cerere. Acordarea accesului prin alte mijloace decât furnizarea unei copii nu împiedică persoanele vizate să aibă, de asemenea, dreptul la o copie, cu excepția cazului în care acestea aleg să nu facă acest lucru.

[77] Orientările GL29 privind transparența – aprobate de CEPD, punctul 33.

134. Operatorul poate alege, în funcție de situația în cauză, să furnizeze o copie a datelor care fac obiectul prelucrării, împreună cu informațiile suplimentare, în diferite moduri, de exemplu prin e-mail, poștă fizică sau prin utilizarea unui instrument de *self-service*. În cazul în care persoana vizată introduce cererea în format electronic și cu excepția cazului în care persoana vizată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent, în conformitate cu articolul 15 alineatul (3). În orice caz, operatorul trebuie să ia în considerare măsurile tehnice și organizatorice adecvate, inclusiv criptarea adecvată, atunci când furnizează informații prin e-mail sau prin instrumente online de *self-service*.

135. În situația în care operatorul prelucrează date cu caracter personal referitoare la persoana care înaintează cererea numai la scară mică, copia datelor cu caracter personal și informațiile suplimentare pot și ar trebui să fie furnizate printr-o procedură simplă.

Exemplul 22: o librărie locală ține o evidență a numelor și adreselor clienților săi care au plasat comenzi cu livrare la domiciliu. Un client vizitează librăria și înaintează o cerere de acces. În această situație, ar fi suficient să se imprime datele cu caracter personal referitoare la client direct din sistemul comercial, furnizând, de asemenea, informațiile suplimentare prevăzute la articolul 15 alineatele (1) și (2).

Exemplul 23: o persoană care face lunar donații către o organizație caritabilă depune o cerere de acces prin e-mail. Organizația caritabilă deține informații cu privire la donațiile efectuate în ultimele douăsprezece luni, precum și numele și adresele de e-mail ale donatorilor. Operatorul ar putea furniza copia datelor cu caracter personal și informațiile suplimentare răspunzând e-mailului, cu condiția aplicării tuturor garanțiilor necesare, luând în considerare, de exemplu, natura datelor.

136. Chiar și operatorii care prelucrează un volum mare de date pot alege să se bazeze pe proceduri manuale pentru tratarea cererilor de acces. În cazul în care prelucrează date în mai multe departamente diferite, operatorul trebuie să colecteze datele cu caracter personal de la fiecare departament pentru a putea răspunde cererii persoanei vizate.

Exemplul 24: operatorul desemnează un administrator pentru a trata problemele practice legate de cererile de acces. Atunci când primește o cerere, administratorul trimite un mesaj prin e-mail diferitelor departamente ale organizației, solicitându-le să colecteze date cu caracter personal referitoare la persoana vizată. Reprezentanții fiecărui departament pun la dispoziția administratorului datele cu caracter personal prelucrate de departamentul lor. Administratorul transmite apoi toate datele cu caracter personal persoanei vizate, împreună cu informațiile suplimentare necesare, de exemplu și, dacă este cazul, prin e-mail.

137. Deși procesele manuale de tratare a cererilor de acces ar putea fi considerate adecvate, unii operatori pot beneficia de pe urma utilizării unor procese automatizate pentru a trata cererile persoanelor vizate. Acesta ar putea fi, de exemplu, cazul operatorilor care primesc un număr mare de cereri. O modalitate de a furniza informațiile prevăzute la articolul 15 este de a pune la dispoziția persoanei vizate instrumente de *self-service*. Acest lucru ar putea facilita tratarea eficientă și în timp util a cererilor de acces ale persoanelor vizate și, de asemenea, va permite operatorului să includă mecanismul de verificare în instrumentul de *self-service*.

Exemplul 25: un serviciu de comunicare socială dispune de un proces automat de tratare a cererilor de acces care permite persoanei vizate să își acceseze datele cu caracter personal din contul său de utilizator. Pentru a extrage datele cu caracter personal, utilizatorii platformelor de comunicare socială pot alege opțiunea „Descărcați datele dvs. cu caracter personal” atunci când se conectează la contul

lor de utilizator. Această opțiune de *self-service* le permite utilizatorilor să descarce un fișier care conține datele lor cu caracter personal direct din contul de utilizator în propriul computer.

138. Utilizarea instrumentelor de *self-service* nu ar trebui să limiteze niciodată domeniul de aplicare al datelor cu caracter personal primite. Dacă nu este posibil să se furnizeze toate informațiile prevăzute la articolul 15 prin intermediul instrumentului de *self-service*, informațiile rămase trebuie furnizate în mod diferit. Într-adevăr, operatorul poate încuraja persoana vizată să utilizeze un instrument de *self-service* pe care operatorul l-a instituit pentru tratarea cererilor de acces. Cu toate acestea, ar trebui remarcat faptul că operatorul trebuie, de asemenea, să trateze cererile de acces care nu sunt trimise prin canalul de comunicare stabilit[78].

5.2.3 Acordarea accesului într-o „formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu”

139. În conformitate cu articolul 12 alineatul (1) din RGPD, operatorul ia măsuri adecvate pentru a acorda accesul în temeiul articolului 15 într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

140. Cerința conform căreia acordarea accesului persoanei vizate trebuie efectuată într-o formă concisă și transparentă înseamnă că operatorii ar trebui să prezinte informațiile în mod eficient și succint pentru a fi ușor de înțeles de către persoana vizată, în special dacă este vorba despre un copil. Operatorul trebuie să țină seama de cantitatea și complexitatea datelor atunci când alege mijloacele de acordare a accesului în temeiul articolului 15.

Exemplul 26: un furnizor al unei platforme de comunicare socială prelucrează un volum mare de informații cu privire la o persoană vizată. O mare parte din aceste date cu caracter personal sunt informații conținute în sute de pagini de fișiere-jurnal în care sunt înregistrate activitățile persoanei vizate pe site. În cazul în care persoanele vizate solicită acces la datele lor cu caracter personal, datele cu caracter personal din aceste fișiere-jurnal intră, într-adevăr, sub incidența dreptului de acces. Prin urmare, dreptul de acces poate fi exercitat în mod formal în cazul în care aceste sute de pagini de fișiere-jurnal ar fi furnizate persoanei vizate. Cu toate acestea, dacă nu se iau măsuri pentru a facilita înțelegerea informațiilor din fișierele-jurnal, este posibil ca dreptul de acces al persoanei vizate să nu fie respectat în practică, deoarece din fișierele-jurnal nu se pot extrage cu ușurință cunoștințe și, prin urmare, nu se îndeplinește cerința de la articolul 12 alineatul (1) din RGPD. Prin urmare, operatorul trebuie să acționeze cu atenție și minuțiozitate atunci când alege modul în care informațiile și datele cu caracter personal sunt prezentate persoanei vizate.

141. În circumstanțele din exemplul de mai sus, utilizarea unei abordări pe mai multe niveluri, similară abordării pe mai multe niveluri promovate în Orientările privind transparența în ceea ce privește declarațiile de confidențialitate[79], ar putea fi o măsură adecvată atât pentru îndeplinirea cerințelor de la articolul 15, cât și a celor de la articolul 12 alineatul (1) din RGPD. Acest aspect va fi prezentat în detaliu în subsecțiunea 5.2.4 de mai jos. Cerința ca informațiile să fie „inteligibile” înseamnă că acestea ar trebui înțelese de către publicul vizat[80], ținând seama, în același timp, de oricare nevoi speciale pe

[78] A se vedea subsecțiunea 3.1.2.
[79] Orientările GL29 privind transparența – aprobate de CEPD, punctul 35.
[80] Inteligibilitatea este strâns legată de cerința de a utiliza un limbaj simplu și clar (Orientările GL 29 privind transparența – aprobate de CEPD, punctul 9). Afirmațiile despre limbajul simplu și clar de la alineatele (12)-(16)

care persoana vizată le-ar putea avea și care sunt cunoscute de operator[81]. Întrucât dreptul de acces permite adesea exercitarea altor drepturi ale persoanelor vizate, este esențial ca informațiile furnizate să fie ușor de înțeles și clare. Motivul în acest caz este faptul că persoanele vizate vor putea lua în considerare dacă să își invoce dreptul la rectificare, de exemplu, în temeiul articolului 16 din RGPD, după ce află care sunt datele cu caracter personal prelucrate, scopurile prelucrării etc. Drept rezultat, operatorul ar putea fi nevoit să furnizeze persoanei vizate informații suplimentare care să explice datele furnizate. Ar trebui subliniat faptul că gradul de complexitate al prelucrării datelor îl obligă pe operator să ofere mijloacele necesare pentru ca datele să fie ușor de înțeles și nu ar putea fi utilizat drept argument pentru a limita accesul la toate datele. În mod similar, obligația operatorului de a furniza date într-un mod concis nu poate fi utilizată drept argument pentru a limita accesul la toate datele.

Exemplul 27: un site de comerț electronic colectează în scopuri de marketing date cu privire la articolele vizualizate sau achiziționate de pe site-ul său. O parte din aceste date vor fi date în format brut[82], care nu au fost analizate și care ar putea să nu fie direct relevante pentru cititor (coduri, istoricul activității etc.). Astfel de date legate de activitățile persoanelor vizate sunt, de asemenea, acoperite de dreptul de acces și ar trebui, în consecință, să fie furnizate persoanei vizate ca răspuns la o cerere de acces. Atunci când furnizează date în format brut, este important ca operatorul să ia măsurile necesare pentru a se asigura că persoana vizată înțelege datele, de exemplu prin furnizarea unui document explicativ care traduce formatul brut într-o formă ușor de utilizat. De asemenea, un astfel de document ar putea explica faptul că abrevierile și alte acronime, de exemplu, „A” înseamnă că achiziția a fost întreruptă, iar „B” înseamnă că achiziția a fost realizată.

142. Elementul „ușor accesibil” înseamnă că informațiile prevăzute la articolul 15 ar trebui prezentate într-un mod ușor de accesat de către persoana vizată. Acest lucru este valabil, de exemplu, în ceea ce privește dispunerea, titlurile și împărțirea în paragrafe corespunzătoare. Informațiile ar trebui să fie întotdeauna furnizate într-un limbaj simplu și clar. Un operator care oferă un serviciu într-o țară ar trebui, de asemenea, să ofere răspunsuri în limba pe care o înțeleg persoanele vizate din țara respectivă. Utilizarea pictogramelor standardizate este, de asemenea, încurajată atunci când facilitează inteligibilitatea și accesibilitatea informațiilor. În cazul în care cererea de informații se referă la persoane vizate cu deficiențe de vedere sau la alte persoane vizate care ar putea întâmpina dificultăți în accesarea sau înțelegerea informațiilor, se așteaptă ca operatorul să ia măsuri care să faciliteze înțelegerea informațiilor furnizate, inclusiv a informațiilor transmise verbal, atunci când acest lucru este adecvat[83]. Operatorul ar trebui să acorde o atenție deosebită pentru a se asigura că persoanele în vârstă, copiii, persoanele cu deficiențe de vedere sau persoanele cu dizabilități cognitive sau de altă natură își pot exercita drepturile, de exemplu, furnizând în mod proactiv elemente ușor accesibile pentru a facilita exercitarea acestor drepturi.

în ceea ce privește informațiile menționate la articolele 13 și 14 din RGPD se aplică, de asemenea, comunicării în temeiul articolului 15.

[81] A se vedea punctul 128.

[82] Formatul brut din exemplu trebuie înțeles ca date neanalizate care stau la baza unei prelucrări, și nu cel mai scăzut nivel de date brute care pot fi citite automat (cum ar fi „biții”).

[83] A se vedea Orientările GL29 privind transparența – aprobate de CEPD, punctul 21.

5.2.4 Un volum mare de informații necesită cerințe specifice privind modul în care sunt furnizate informațiile.

143. Indiferent de mijloacele utilizate pentru acordarea accesului, ar putea exista o disproporționalitate între volumul de informații pe care operatorul trebuie să le furnizeze persoanelor vizate și cerința ca acestea să fie într-o formă concisă. O modalitate de a ține cont de ambele aspecte, precum și un exemplu de măsură adecvată pentru anumiți operatori, atunci când trebuie furnizat un volum mare de date, este de a utiliza o abordare pe mai multe niveluri. Această abordare poate facilita înțelegerea datelor de către persoanele vizate. Cu toate acestea, ar trebui subliniat faptul că această abordare poate fi utilizată numai în anumite circumstanțe și trebuie efectuată într-un mod care să nu limiteze dreptul de acces, astfel cum se explică mai jos. În plus, utilizarea unei abordări pe mai multe niveluri nu ar trebui să creeze o sarcină suplimentară pentru persoana vizată. Prin urmare, aceasta ar fi cea mai potrivită atunci când accesul este acordat într-un context online. O abordare pe mai multe niveluri este doar o modalitate de a prezenta informațiile prevăzute la articolul 15 într-un mod care respectă, de asemenea, cerințele de la articolul 12 alineatul (1) din RGPD și nu ar trebui confundată cu posibilitatea ca operatorii să solicite persoanei vizate să specifice informațiile sau activitățile de prelucrare la care se referă cererea, astfel cum se prevede în considerentul 63 din RGPD[84].

144. O abordare pe mai multe niveluri în ceea ce privește dreptul de acces înseamnă că un operator, în anumite circumstanțe, poate furniza datele cu caracter personal și informațiile suplimentare solicitate în temeiul articolului 15 pe diferite niveluri. Primul nivel ar trebui să includă informații privind prelucrarea și drepturile persoanei vizate în conformitate cu articolul 15 alineatul (1) literele (a)-(h) și cu articolul 15 alineatul (2), precum și o primă parte a datelor cu caracter personal prelucrate. La un al doilea nivel, ar trebui furnizate mai multe date cu caracter personal.

145. Atunci când decide ce informații ar trebui furnizate pe diferitele niveluri, operatorul ar trebui să ia în considerare informațiile pe care persoana vizată, în general, le-ar considera ca fiind cele mai relevante. În conformitate cu principiul echității, primul nivel ar trebui să conțină, de asemenea, informații privind prelucrarea care au cel mai mare impact asupra persoanei vizate[85]. Operatorii trebuie să fie în măsură să dea dovadă de responsabilitate în ceea ce privește raționamentul lor referitor la cele de mai sus.

> **Exemplul 28:** un operator analizează seturi de volume mari de date pentru a plasa clienții în diferite segmente, în funcție de comportamentul lor online. În această situație, se poate presupune că informațiile care sunt cele mai importante pentru persoanele vizate sunt informațiile despre segmentul în care au fost plasate. Prin urmare, aceste informații ar trebui incluse în primul nivel. Datele într-un format brut[86] care nu au fost încă analizate sau prelucrate suplimentar, cum ar fi activitatea utilizatorilor pe un site, sunt, de asemenea, date cu caracter personal care fac obiectul dreptului de acces; cu toate acestea, în unele cazuri, ar putea fi suficient să se furnizeze aceste informații într-un alt nivel.

146. Pentru ca utilizarea abordării pe mai multe niveluri să fie considerată o măsură adecvată, este necesar ca persoana vizată să fie informată de la bun început că informațiile prevăzute la articolul 15 sunt structurate pe niveluri diferite și să îi fie furnizată o descriere a datelor cu caracter personal și a informațiilor care vor fi incluse în diferitele niveluri. Astfel, persoana vizată va putea decide mai ușor ce niveluri dorește să acceseze. Descrierea ar trebui să reflecte în mod obiectiv toate categoriile de

[84] A se vedea, de asemenea, subsecțiunea 2.3.1.
[85] A se vedea Orientările GL29 privind transparența – aprobate de CEPD, punctul 36.
[86] A se vedea nota de subsol 82.

date cu caracter personal care sunt prelucrate efectiv de operator. De asemenea, trebuie să fie clar modul în care persoana vizată poate avea acces la diferitele niveluri. Accesul la diferitele niveluri nu implică niciun efort disproporționat pentru persoana vizată și nu este condiționat de înaintarea unei noi cereri de către persoana vizată. Aceasta înseamnă că persoanele vizate trebuie să aibă posibilitatea de a alege dacă să acceseze toate nivelurile simultan sau să acceseze unul sau două niveluri, dacă sunt mulțumite de acest lucru.

Exemplul 29: o persoană vizată înaintează o cerere de acces unui serviciu de redare de conținut video în flux continuu. Cererea este înaintată printr-o opțiune disponibilă la momentul conectării persoanelor vizate la conturile lor. Persoanei vizate i se prezintă două opțiuni care apar ca butoane pe pagina web. Prima opțiune este descărcarea părții 1 a datelor cu caracter personal și a informațiilor suplimentare. Aceasta conține, de exemplu, istoricul vizualizărilor recente, informații privind contul și informații privind plățile. Opțiunea a doua este descărcarea părții 2 a datelor cu caracter personal care conține fișiere-jurnal tehnice cu privire la activitățile persoanelor vizate și informații mai vechi privind contul. În acest caz, operatorul a permis persoanelor vizate să își exercite dreptul într-un mod care nu creează o sarcină suplimentară pentru persoana vizată.

Varianta 1: în cazurile în care persoana vizată alege doar butonul pentru descărcarea părții 1 a datelor cu caracter personal, operatorul este obligat să furnizeze doar partea 1 a datelor.

Varianta 2: În cazurile în care persoana vizată alege atât butonul pentru partea 1, cât și butonul pentru partea 2 a datelor, operatorul nu poate să transmită doar partea 1 a datelor și să solicite o nouă confirmare înainte de comunicarea părții 2 a datelor. În schimb, ambele părți ale datelor trebuie furnizate persoanei vizate, astfel cum rezultă din cererea înaintată.

147. Utilizarea unei abordări pe mai multe niveluri nu va fi considerată adecvată pentru toți operatorii sau în toate situațiile. Aceasta ar trebui utilizată numai atunci când ar fi dificil pentru persoana vizată să înțeleagă informațiile în integralitatea lor. Cu alte cuvinte, operatorul trebuie să fie în măsură să demonstreze că utilizarea abordării pe mai multe niveluri aduce o valoare adăugată pentru persoana vizată, ajutând-o să înțeleagă informațiile furnizate. Prin urmare, o abordare pe mai multe niveluri ar fi considerată adecvată numai în cazul în care un operator prelucrează un volum mare de date cu caracter personal cu privire la persoana vizată care înaintează o cerere și în cazul în care ar exista dificultăți evidente pentru persoana vizată de a obține sau de a înțelege informațiile dacă acestea ar fi furnizate toate în același timp. Faptul că aceasta ar presupune eforturi și resurse considerabile din partea operatorului pentru furnizarea informațiilor în temeiul articolului 15 nu este, în sine, un argument pentru utilizarea unei abordări pe mai multe niveluri.

5.2.5 Formatul

148. În conformitate cu articolul 12 alineatul (1) din RGPD, informațiile prevăzute la articolul 15 se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. În ceea ce privește accesul la datele cu caracter personal care fac obiectul prelucrării, articolul 15 alineatul (3) prevede că, în cazul în care persoana vizată introduce cererea în format electronic și cu excepția cazului în care persoana vizată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent. RGPD nu specifică ceea ce reprezintă un format electronic utilizat în mod curent. Astfel, există mai multe formate acceptabile care pot fi utilizate. Ceea ce se consideră a fi un format electronic utilizat în mod curent va varia, de asemenea, în timp.

149. Ceea ce ar putea fi considerat un format electronic utilizat în mod curent ar trebui să se bazeze pe o evaluare obiectivă, și nu pe formatul utilizat de operator în operațiunile sale zilnice. Pentru a stabili

formatul care trebuie considerat ca fiind un format utilizat în mod curent în situația de față, operatorul va trebui să evalueze dacă există formate specifice utilizate în general în domeniul de activitate al operatorului sau în contextul dat. În cazul în care nu există astfel de formate utilizate în general, formatele deschise stabilite într-un standard internațional, cum ar fi ISO, ar trebui, în general, să fie considerate formate electronice utilizate în mod curent. Cu toate acestea, CEPD nu exclude posibilitatea ca și alte formate să poată fi considerate ca fiind utilizate în mod curent în sensul articolului 15 alineatul (3). Atunci când evaluează dacă un format este un format electronic utilizat în mod curent, CEPD consideră că este important de știut cât de ușor poate accesa persoana informațiile furnizate în formatul actual. În acest sens, ar trebui observate informațiile pe care operatorul le-a furnizat persoanei vizate cu privire la modul de accesare a unui fișier care a fost furnizat într-un format specific, cum ar fi programele sau software-urile care ar putea fi utilizate, pentru a face formatul mai accesibil pentru persoana vizată. Cu toate acestea, persoana vizată nu ar trebui să fie obligată să achiziționeze un software pentru a obține acces la informații.

150. Atunci când decide cu privire la formatul în care ar trebui furnizate copia datelor cu caracter personal și informațiile în temeiul articolului 15, operatorul trebuie să țină seama de faptul că formatul trebuie să permită prezentarea informațiilor într-un mod inteligibil și ușor accesibil. Este important ca persoanei vizate să i se furnizeze informații în formă integrală, permanentă (text, electronic). Întrucât informațiile ar trebui să persiste în timp, informațiile în scris, inclusiv cele transmise în format electronic, sunt, în principiu, preferabile în raport cu alte formate. Copia datelor cu caracter personal ar putea fi stocată, după caz, pe un dispozitiv electronic de stocare, cum ar fi CD sau USB.

151. Ar trebui remarcat faptul că, pentru ca un operator să poată considera că persoanelor vizate li s-a furnizat o copie a datelor cu caracter personal, nu este suficient să li se fi oferit acces la datele lor cu caracter personal. Pentru ca cerința de a furniza o copie a datelor cu caracter personal să fie îndeplinită și în cazul în care datele sunt furnizate electronic/digital, persoanele vizate trebuie să își poată descărca datele într-un format electronic utilizat în mod curent.

152. Este responsabilitatea operatorului să decidă cu privire la formatul adecvat în care vor fi furnizate datele cu caracter personal. Operatorul poate, deși nu este neapărat obligat, să furnizeze documentele care conțin date cu caracter personal cu privire la persoanele vizate care înaintează cererea în forma lor originală. Operatorul ar putea, de exemplu, de la caz la caz, să acorde acces la o copie a suportului ca atare, având în vedere nevoia de transparență (de exemplu, pentru a verifica exactitatea datelor deținute de operator în cazul unei cereri de acces la dosarul medical sau la o înregistrare audio a cărei transcriere este contestată). Cu toate acestea, în interpretarea dată dreptului de acces în temeiul Directivei 95/46/CE, CJUE a afirmat că „pentru ca *[...] drept[ul] de acces* să fie respectat, este suficient ca solicitantul respectiv să fie pus în posesia unei prezentări complete privind datele menționate într- o formă inteligibilă, și anume într- o formă care să permită solicitantului amintit să ia cunoștință de aceste date și să verifice dacă ele sunt exacte și sunt prelucrate în conformitate cu această directivă, pentru ca solicitantul menționat să poată exercita, după caz, drepturile care îi sunt conferite de directiva respectivă”[87]. Spre deosebire de directivă, RGPD conține în mod expres o obligație de a furniza persoanei vizate o copie a datelor cu caracter personal care fac obiectul prelucrării. Totuși, aceasta nu înseamnă că persoana vizată are întotdeauna dreptul de a obține o copie a documentelor care conțin datele cu caracter personal, ci o copie nemodificată a datelor cu caracter personal prelucrate în aceste documente.[88] O astfel de copie a datelor cu caracter personal ar putea fi furnizată

[87] CJUE, cauzele conexate C-141/12 și C-372/12, YS și alții, punctul 60.

[88] Întrebările legate de acest subiect sunt în discuție în cauzele aflate în prezent pe rolul CJUE (C-487/21 și C-307/21).

sub forma unei compilații care să conțină toate datele cu caracter personal care fac obiectul dreptului de acces, atât timp cât compilația permite persoanei vizate să fie informată cu privire la prelucrare și să verifice legalitatea acesteia. Prin urmare, nu există nicio contradicție între formularea RGPD și hotărârea CJUE cu privire la această chestiune. Termenul „prezentare" din hotărâre nu ar trebui interpretat în mod eronat în sensul că această compilație nu ar include toate datele care intră sub incidența dreptului de acces, ci este doar o modalitate de a prezenta toate aceste date fără a permite accesul la documentele subiacente care conțin datele cu caracter personal. Întrucât compilația trebuie să conțină o copie a datelor cu caracter personal, ar trebui subliniat faptul că aceasta nu poate fi realizată într-un mod care să modifice sau să schimbe într-o oarecare măsură conținutul informațiilor.

Exemplul 30: o persoană vizată deține de mai mulți ani o asigurare de la o societate de asigurări. Au avut loc mai multe incidente asigurate. În fiecare caz, a existat o corespondență scrisă prin e-mail între persoana vizată și societatea de asigurări. Întrucât persoana vizată a trebuit să furnizeze informații cu privire la circumstanțele specifice ale fiecărui incident, corespondența implică multe informații cu caracter personal cu privire la persoana vizată (hobby-uri, colegi de apartament, obiceiuri zilnice etc.). În unele cazuri, a apărut un dezacord cu privire la obligația societății de asigurări de a o despăgubi pe persoana vizată, ceea ce a generat un volum mare de comunicări între cele două părți. Întreaga corespondență este stocată de societatea de asigurări. Persoana vizată înaintează o cerere de acces. În această situație, operatorul nu trebuie neapărat să furnizeze e-mailurile în forma lor originală prin retransmiterea lor către persoana vizată. În schimb, operatorul ar putea alege să compileze corespondența prin e-mail care conține datele cu caracter personal ale persoanei vizate într-un dosar care este furnizat persoanei vizate.

153. Fără a aduce atingere formatului în care operatorul furnizează datele cu caracter personal, de exemplu prin furnizarea documentelor propriu-zise care conțin datele cu caracter personal sau a unei compilații a datelor cu caracter personal, informațiile respectă cerințele de transparență prevăzute la articolul 12 din RGPD. Realizarea unui anumit tip de compilație și/sau extragere a datelor într-un mod care să faciliteze înțelegerea informațiilor ar putea fi, în unele cazuri, o modalitate de a respecta aceste cerințe. În alte cazuri, informațiile sunt mai bine înțelese prin furnizarea unei copii a documentului propriu-zis care conține datele cu caracter personal. Prin urmare, formatul cel mai adecvat trebuie decis de la caz la caz.

154. În acest context, este important de reținut că există o distincție între dreptul de acces în temeiul articolului 15 din RGPD și dreptul de a primi o copie a documentelor administrative reglementat de legislația națională, acesta din urmă fiind un drept de a primi o copie a documentului propriu-zis. Aceasta nu înseamnă că dreptul de acces în temeiul articolului 15 din RGPD exclude posibilitatea de a primi o copie a documentului/suporturilor pe care apar datele cu caracter personal.

155. În unele cazuri, datele cu caracter personal în sine stabilesc cerințele în ceea ce privește formatul în care ar trebui furnizate datele cu caracter personal. De exemplu, atunci când datele cu caracter personal constituie informații olografe furnizate de persoana vizată, ar putea fi necesar ca persoanei vizate să i se furnizeze o fotocopie a informațiilor olografe respective, deoarece scrierea de mână în sine se încadrează în categoria datelor cu caracter personal. Acest lucru ar putea fi valabil în special atunci când scrierea de mână este un aspect important pentru prelucrare, de exemplu pentru analiza scrisului. Același lucru este valabil, în general, pentru înregistrările audio, deoarece vocea persoanei vizate în sine se încadrează în categoria datelor cu caracter personal. Cu toate acestea, în unele cazuri, accesul poate fi acordat prin furnizarea unei transcrieri a conversației, de exemplu, dacă persoana vizată și operatorul convin astfel.

156. Ar trebui remarcat faptul că dispozițiile privind cerințele referitoare la format sunt diferite în ceea ce privește dreptul de acces și dreptul la portabilitatea datelor. În timp ce dreptul la portabilitatea datelor în temeiul articolului 20 din RGPD impune ca informațiile să fie furnizate într-un format care poate fi citit automat, dreptul la informare prevăzut la articolul 15 nu prevede acest lucru. Prin urmare, formatele care sunt considerate inadecvate atunci când se conformează unei cereri de portabilitate a datelor, de exemplu fișierele în format PDF, ar putea fi în continuare adecvate atunci când se dă curs unei cereri de acces.

5.3 Calendarul pentru acordarea accesului

157. Articolul 12 alineatul (3) din RGPD prevede că operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri în temeiul articolului 15, fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii. Acest termen poate fi prelungit cu maximum două luni, ținând seama de complexitatea și numărul cererilor, cu condiția ca persoana vizată să fi fost informată cu privire la motivele acestei întârzieri în termen de o lună de la primirea cererii. Această obligație de a informa persoana vizată cu privire la prelungire și la motivele acesteia nu ar trebui confundată cu informațiile care trebuie furnizate fără întârziere și cel târziu în termen de o lună dacă operatorul nu ia măsuri cu privire la cerere, astfel cum se specifică în detaliu la articolul 12 alineatul (4) din RGPD.

158. Operatorul reacționează și, ca regulă generală, furnizează informațiile prevăzute la articolul 15 fără întârzieri nejustificate, ceea ce înseamnă că informațiile ar trebui furnizate cât mai curând posibil. Aceasta înseamnă că, în cazul în care este posibil să se furnizeze informațiile solicitate într-un termen mai scurt de o lună, operatorul ar trebui să facă acest lucru. CEPD consideră, de asemenea, că termenul de răspuns la cerere în anumite situații trebuie adaptat la perioada de stocare pentru a putea acorda accesul[89].

159. Termenul începe să curgă din momentul în care operatorul a primit o cerere în temeiul articolului 15, adică atunci când cererea ajunge la operator prin intermediul unuia dintre canalele sale oficiale[90]. Nu este necesar ca operatorul să aibă efectiv cunoștință de cerere. Cu toate acestea, atunci când operatorul trebuie să comunice cu persoana vizată din cauza incertitudinii privind identitatea persoanei care înaintează cererea, poate exista o suspendare a termenului până când operatorul obține informațiile necesare de la persoana vizată, cu condiția ca operatorul să fi solicitat informații suplimentare fără întârzieri nejustificate. Același lucru este valabil și în cazul în care un operator a solicitat unei persoane vizate să precizeze operațiunile de prelucrare la care se referă cererea, atunci când sunt îndeplinite condițiile prevăzute în considerentul 63[91].

Exemplul 31: în urma primirii cererii, un operator reacționează imediat și solicită informațiile de care are nevoie pentru a confirma identitatea persoanei care înaintează cererea. Acesta din urmă răspunde câteva zile mai târziu, iar informațiile pe care persoana vizată le trimite pentru verificarea identității nu par suficiente, ceea ce impune operatorului să solicite clarificări. În această situație, va exista o suspendare a termenului până când operatorul obține suficiente informații pentru a verifica identitatea persoanei vizate.

[89] A se vedea subsecțiunea 2.3.3.
[90] În unele state membre există o legislație națională care stabilește momentul când un mesaj trebuie considerat ca fiind primit, ținând seama de weekenduri și de sărbătorile naționale.
[91] A se vedea, în continuare, subsecțiunea 2.3.1.

160. Termenul de răspuns la o cerere de acces trebuie calculat în conformitate cu Regulamentul (CEE, Euratom) nr. 1182/71[92].

Exemplul 32: o organizație primește o cerere la 5 martie. Termenul începe să curgă din aceeași zi. Acest lucru permite organizației să dea curs cererii până cel târziu la 5 aprilie inclusiv.

Exemplul 33: în cazul în care organizația primește o cerere la 31 august și, întrucât luna următoare este mai scurtă, nu există o dată corespunzătoare, data răspunsului este cel târziu ultima zi a lunii următoare, deci 30 septembrie.

161. În cazul în care ultima zi a acestei perioade coincide cu un weekend sau cu o sărbătoare legală, operatorul trebuie să răspundă până în următoarea zi lucrătoare.

162. În anumite circumstanțe, operatorul poate prelungi termenul de răspuns la o cerere de acces cu încă două luni, dacă este necesar, ținând seama de complexitatea și numărul cererilor. Ar trebui subliniat faptul că această posibilitate este o derogare de la regula generală și nu ar trebui să fie utilizată în mod excesiv. În cazul în care operatorii sunt adesea obligați să prelungească termenul, ar putea fi un indiciu al necesității de a-și dezvolta în continuare procedurile generale de tratare a cererilor.

163. Ceea ce constituie o cerere complexă variază în funcție de circumstanțele specifice fiecărui caz. Unii dintre factorii care ar putea fi considerați relevanți sunt, de exemplu:

- volumul de date prelucrate de operator;
- modul în care sunt stocate informațiile, în special atunci când este dificil să se extragă informațiile, de exemplu atunci când datele sunt prelucrate de unități diferite ale organizației;
- necesitatea de a cenzura informații atunci când se aplică o derogare, de exemplu informații privind alte persoane vizate sau care constituie secrete comerciale și
- situațiile în care informațiile necesită acțiuni suplimentare pentru a fi inteligibile.

164. Simplul fapt că pentru a da curs cererii ar fi necesar un efort considerabil nu face ca o cerere să fie complexă. În mod similar, faptul că o întreprindere de mari dimensiuni primește un număr mare de cereri nu ar declanșa automat o prelungire a termenului. Cu toate acestea, atunci când un operator primește temporar un număr mare de cereri, de exemplu din cauza unei publicități extraordinare cu privire la activitățile sale, acest lucru ar putea fi considerat un motiv legitim pentru prelungirea termenului de răspuns. Cu toate acestea, un operator, în special un operator care gestionează un volum mare de date, ar trebui să dispună de proceduri și mecanisme pentru a putea trata cererile în termenul stabilit în condiții normale.

6 LIMITĂRI ȘI RESTRICȚII PRIVIND DREPTUL DE ACCES

6.1 Observații generale

165. Dreptul de acces este supus limitărilor care rezultă din articolul 15 alineatul (4) din RGPD (drepturile și libertățile altora) și din articolul 12 alineatul (5) din RGPD (cereri în mod vădit nefondate sau excesive).

[92] Regulamentul (CEE, Euratom) nr. 1182/71 al Consiliului din 3 iunie 1971 privind stabilirea regulilor care se aplică termenelor, datelor și expirării termenelor.

În plus, dreptul Uniunii sau dreptul intern al statelor membre poate restricționa dreptul de acces în conformitate cu articolul 23 din RGPD. Derogările privind prelucrarea datelor cu caracter personal în scopuri științifice, de cercetare istorică sau statistică ori în scopuri de arhivare în interes public se pot întemeia în mod corespunzător pe articolul 89 alineatul (2) și pe articolul 89 alineatul (3) din RGPD, iar derogările pentru prelucrarea efectuată în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare se pot întemeia pe articolul 85 alineatul (2) din RGPD.

166. Este important de remarcat faptul că, în afară de limitările, derogările și posibilele restricții menționate mai sus, RGPD nu permite alte scutiri sau derogări de la dreptul de acces. Aceasta înseamnă, printre altele, că dreptul de acces nu are nicio rezervă generală în ceea ce privește proporționalitatea în legătură cu eforturile pe care operatorul trebuie să le depună pentru a da curs cererii persoanelor vizate în temeiul articolului 15 din RGPD[93]. În plus, nu este permisă limitarea sau restricționarea dreptului de acces în cadrul unui contract încheiat între operator și persoana vizată.

167. În conformitate cu considerentul 63, dreptul de acces este acordat persoanelor vizate pentru a fi informate cu privire la prelucrare și pentru a verifica legalitatea acesteia. Dreptul de acces permite, printre altele, persoanei vizate să obțină, după caz, rectificarea, ștergerea sau blocarea datelor cu caracter personal[94]. Cu toate acestea, persoanele vizate nu sunt obligate să își motiveze sau să își justifice cererea. Atât timp cât sunt îndeplinite cerințele de la articolul 15 din RGPD, scopurile cererii ar trebui considerate irelevante[95].

6.2 Articolul 15 alineatul (4) din RGPD

168. În conformitate cu articolul 15 alineatul (4) din RGPD, dreptul de a obține o copie nu aduce atingere drepturilor și libertăților altora. Explicații cu privire la această limitare sunt oferite în a cincea și a șasea teză de la considerentul 63. Acest drept nu ar trebui să aducă atingere drepturilor sau libertăților altora, inclusiv secretului comercial sau proprietății intelectuale și, în special, drepturilor de autor care asigură protecția programelor software.
Cu toate acestea, considerațiile de mai sus nu ar trebui să aibă drept rezultat refuzul de a furniza toate informațiile persoanei vizate. Atunci când se interpretează articolul 15 alineatul (4) din RGPD, trebuie să se acorde o atenție deosebită pentru a nu extinde în mod nejustificat restricțiile prevăzute la articolul 23 din RGPD, care sunt permise numai în condiții stricte.

169. Articolul 15 alineatul (4) din RGPD se aplică dreptului de a obține o copie a datelor, care este principala modalitate de acordare a accesului la datele prelucrate (a doua componentă a dreptului de acces). Aceasta este, de asemenea, aplicabilă, iar drepturile și libertățile altora sunt luate în considerare în cazul în care accesul la datele cu caracter personal este acordat în mod excepțional prin alte mijloace decât o copie. De exemplu, nu există nicio diferență justificată dacă secretele comerciale sunt afectate de furnizarea unei copii sau de acordarea accesului la fața locului persoanei vizate. Articolul 15 alineatul (4) din RGPD nu se aplică informațiilor suplimentare privind prelucrarea, astfel cum se prevede la articolul 15 alineatul (1) literele (a)-(h) din RGPD.

---

[93] Atunci când operatorul prelucrează un volum mare de informații privind persoana vizată, astfel cum se menționează în considerentul 63 din RGPD, operatorul poate solicita ca persoana vizată să precizeze informațiile sau activitățile de prelucrare la care se referă cererea sa. A se vedea, de asemenea, subsecțiunea 2.3.1.
[94] CJUE, cauzele conexate C-141/12 și C-372/12, YS și alții.
[95] Acest lucru nu aduce atingere dreptului intern aplicabil care respectă cerințele prevăzute la articolul 23 din RGPD; a se vedea secțiunea 6.4.

170. În conformitate cu considerentul 63, printre drepturile și libertățile care intră în conflict se numără secretul comercial sau proprietatea intelectuală și, în special, drepturile de autor care asigură protecția programelor software. Aceste drepturi și libertăți menționate în mod explicit ar trebui privite doar ca exemple, deoarece, în principiu, se poate considera că orice drept sau libertate în temeiul dreptului Uniunii sau al dreptului intern invocă limitarea prevăzută la articolul 15 alineatul (4) din RGPD[96]. Astfel, dreptul la protecția datelor cu caracter personal (articolul 8 din Carta drepturilor fundamentale a Uniunii Europene) poate fi considerat, de asemenea, un drept afectat în sensul articolului 15 alineatul (4) din RGPD. În ceea ce privește dreptul de a obține o copie, dreptul altora la protecția datelor este un caz tipic în care limitarea trebuie evaluată. În plus, trebuie să se țină seama de dreptul la confidențialitatea corespondenței, de exemplu în ceea ce privește corespondența privată prin e-mail în contextul ocupării forței de muncă[97]. Este important de remarcat faptul că nu orice interes reprezintă „drepturi și libertăți" în temeiul articolului 15 alineatul (4) din RGPD. De exemplu, interesele economice ale unei societăți de a nu divulga date cu caracter personal nu ating pragul pentru recurgerea la excepția prevăzută la articolul 15 alineatul (4), atât timp cât nu sunt afectate secrete comerciale, proprietate intelectuală sau alte drepturi protejate.

171. „Alții" înseamnă orice altă persoană sau entitate, cu excepția persoanei vizate, care își exercită dreptul de acces. Prin urmare, ar putea fi luate în considerare drepturile și libertățile operatorului sau ale persoanei împuternicite de operator (de exemplu, în ceea ce privește păstrarea confidențialității secretelor comerciale și a proprietății intelectuale). În cazul în care legiuitorul Uniunii ar fi dorit să excludă drepturile și libertățile operatorilor sau ale persoanelor împuternicite de operatori, acesta ar fi utilizat termenul „parte terță", care este definit la articolul 4 punctul 10 din RGPD.

172. Preocuparea generală potrivit căreia drepturile și libertățile altora ar putea fi afectate de respectarea cererii de acces nu este suficientă pentru a invoca articolul 15 alineatul (4) din RGPD. Operatorul trebuie să fie în măsură să demonstreze că, în situația concretă, drepturile sau libertățile altora ar fi, de fapt, afectate.

Exemplul 34: o persoană, care în prezent este adultă, s-a aflat în îngrijirea Oficiului de asistență socială pentru copii și tineret timp de mai mulți ani în trecut. Fișierele corespunzătoare pot conține informații sensibile cu privire la alte persoane (părinți, asistenți sociali, alți minori). Cu toate acestea, o cerere de informații din partea persoanei vizate nu poate fi, în general, respinsă din acest motiv în temeiul articolului 15 alineatul (4) din RGPD. Dimpotrivă, drepturile și libertățile altora trebuie examinate în detaliu și demonstrate de Oficiul de asistență pentru copii și tineret în calitate de operator. În funcție de interesele în cauză și de ponderea lor relativă, furnizarea unor astfel de informații specifice poate fi respinsă (de exemplu, prin cenzurarea numelor).

173. În ceea ce privește considerentul 4 din RGPD și raționamentul care stă la baza articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene, dreptul la protecția datelor cu caracter personal nu este un drept absolut[98]. Prin urmare, și exercitarea dreptului de acces trebuie să fie pusă în balanță cu alte drepturi fundamentale, în conformitate cu principiul proporționalității. Atunci când evaluarea în temeiul articolului 15 alineatul (4) din RGPD dovedește că respectarea cererii aduce atingere (are un impact negativ asupra) drepturilor și libertăților altor participanți (etapa 1),

[96] Ponderea sau prioritatea drepturilor și libertăților care intră în conflict nu este o chestiune de definire a termenilor „drepturi și libertăți". Cu toate acestea, evaluarea comparativă a acestor interese face parte dintr-o a doua etapă a evaluării aplicabilității articolului 15 alineatul (4). A se vedea punctul 173 de mai jos.

[97] CEDO, Bărbulescu/România, nr. 61496/08, punctul 80, 5 septembrie 2017.

[98] A se vedea, de asemenea, CJUE, cauzele conexate C-92/09 și C-93/09, Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen [Marea Cameră], 9 noiembrie 2010, punctul 48.

interesele tuturor participanților trebuie să fie evaluate ținând seama de circumstanțele specifice cazului și, în special, de probabilitatea și gravitatea riscurilor prezente în comunicarea datelor. Operatorul ar trebui să încerce să asigure un echilibru între drepturile care intră în conflict (etapa 2), de exemplu prin punerea în aplicare a unor măsuri adecvate de atenuare a riscului la adresa drepturilor și libertăților altora**.** Astfel cum se subliniază în considerentul 63, protejarea drepturilor și libertăților altora în temeiul articolului 15 alineatul (4) din RGPD nu ar trebui să conducă la refuzul de a furniza toate informațiile persoanei vizate. Aceasta înseamnă, de exemplu, în cazul în care se aplică limitarea, că informațiile referitoare la alte persoane trebuie să fie făcute ilizibile pe cât posibil, în loc să se refuze furnizarea unei copii a datelor cu caracter personal. Cu toate acestea, dacă este imposibil să se găsească o soluție de asigurare a unui echilibru între drepturile relevante, operatorul trebuie să decidă într-o etapă următoare care dintre drepturile și libertățile care intră în conflict prevalează (etapa 3).

Exemplul 35: un comerciant cu amănuntul oferă clienților săi posibilitatea de a comanda produse prin intermediul unei linii telefonice operate de serviciul său pentru clienți. Ca dovadă a tranzacțiilor comerciale, comerciantul cu amănuntul stochează o înregistrare a apelurilor, în conformitate cu cerințele stricte ale legislației aplicabile. Un client dorește să primească o copie a conversației pe care a avut-o cu un agent din cadrul serviciului pentru clienți. Într-o primă etapă, comerciantul cu amănuntul analizează cererea și își dă seama că înregistrarea conține date cu caracter personal care se referă și la altă persoană, și anume la agentul din cadrul serviciului pentru clienți. Într-o a doua etapă, pentru a evalua dacă furnizarea copiei ar aduce atingere drepturilor și libertăților altora, comerciantul cu amănuntul trebuie să pună în balanță interesele care intră în conflict, în special luând în considerare probabilitatea și gravitatea posibilelor riscuri la adresa drepturilor și libertăților agentului din cadrul serviciului pentru clienți, care sunt prezente în comunicarea dosarului către client. Comerciantul cu amănuntul concluzionează că în înregistrare există foarte puține date cu caracter personal referitoare la agentul din cadrul serviciului pentru clienți, respectiv doar vocea sa. Comerciantul cu amănuntul/operatorul constată că agentul nu este ușor de identificat. În plus, conținutul discuției este de natură profesională, iar persoana vizată a fost interlocutorul. Pe baza circumstanțelor menționate anterior, operatorul concluzionează în mod obiectiv că dreptul de acces nu aduce atingere drepturilor și libertăților agentului din cadrul serviciului pentru clienți și, prin urmare, operatorul poate furniza persoanei vizate înregistrarea completă, inclusiv părțile din înregistrarea vocală care se referă la agentul din cadrul serviciului pentru clienți.

Exemplul 36: un client al unui magazin de produse de uz medical dorește să aibă acces la rezultatele măsurătorilor referitoare la picioarele sale în temeiul articolului 15 din RGPD. În cadrul magazinului de produse de uz medical, persoanei vizate i-au fost măsurate picioarele în vederea fabricării unor ciorapi compresivi medicinali. Se pare că magazinul de produse de uz medical avea o experiență vastă și instituise o tehnică specială de măsurare cu precizie. După efectuarea măsurătorilor în magazinul de produse de uz medical, clientul dorește să utilizeze rezultatele măsurătorilor pentru a cumpăra ciorapi mai ieftini din altă parte (comandându-le de la un magazin online). Magazinul de produse de uz medical refuză parțial accesul la date în temeiul articolului 15 alineatul (4) din RGPD, susținând că, având în vedere tehnicile sale speciale și precise de măsurare, rezultatele sunt protejate ca secrete comerciale. Dacă și în măsura în care operatorul este în măsură să demonstreze că:

- furnizarea de informații persoanei vizate cu privire la rezultatele măsurătorilor nu este posibilă fără a dezvălui modul în care au fost efectuate măsurătorile și

- informațiile cu privire la modul în care au fost efectuate măsurătorile, inclusiv, dacă este relevant, determinarea exactă a punctelor de măsurare sunt secrete comerciale,

acesta poate aplica articolul 15 alineatul (4) din RGPD.

Operatorul ar trebui în continuare să furnizeze cât mai multe informații cu privire la rezultatele măsurătorilor care nu ar dezvălui secretul său comercial, chiar dacă acest lucru ar implica efortul de revizuire și de editare a rezultatelor.

Exemplul 37: JUCĂTORUL X este înregistrat ca utilizator pe o platformă de jocuri de noroc, PLATFORMA Y. Într-o zi, JUCĂTORUL X este informat că i-a fost restricționat contul online. Întrucât nu se mai poate conecta, JUCĂTORUL X solicită operatorului accesul la toate datele cu caracter personal care îl privesc. În plus, JUCĂTORUL X solicită acces la motivele restricționării contului. PLATFORMA Y, operatorul platformei de jocuri de noroc online la care a fost depusă cererea, informează utilizatorii în cadrul condițiilor sale generale disponibile pe site-ul său că trișatul prin orice metodă (în principal prin utilizarea unui software terț) va atrage o interdicție temporară sau permanentă de utilizare a platformei sale. De asemenea, în declarația sa de confidențialitate, PLATFORMA Y informează utilizatorii cu privire la prelucrarea datelor cu caracter personal în scopul detectării cazurilor de trișare, în conformitate cu cerințele prevăzute la articolul 13 din RGPD.

La primirea cererii de acces din partea JUCĂTORULUI X, PLATFORMA Y ar trebui să îi furnizeze JUCĂTORULUI X o copie a datelor cu caracter personal prelucrate cu privire la JUCĂTORUL X. În ceea ce privește motivul restricționării contului, PLATFORMA Y ar trebui să îi confirme JUCĂTORULUI X că a decis să restricționeze accesul JUCĂTORULUI X la jocurile de noroc online din cauza utilizării unuia sau a mai multor tipuri de trișare care încalcă condițiile generale de utilizare. Pe lângă informațiile furnizate cu privire la prelucrare în scopul detectării cazurilor de trișare, PLATFORMA Y ar trebui să acorde JUCĂTORULUI X acces la informațiile pe care le-a stocat cu privire la cazurile de trișare ale JUCĂTORULUI X care au condus la restricție. În special, PLATFORMA Y ar trebui să îi furnizeze JUCĂTORULUI X informațiile care au condus la restricționarea contului (de exemplu, prezentarea jurnalelor, data și ora trișării, detectarea unui software al unei părți terțe etc.) pentru ca persoana vizată (și anume JUCĂTORUL X) să verifice dacă prelucrarea datelor a fost corectă.

Cu toate acestea, în conformitate cu articolul 15 alineatul (4) din RGPD și cu considerentul 63 din RGPD, PLATFORMA Y nu are obligația de a dezvălui nicio parte din caracteristicile tehnice de funcționare a software-ului anti-trișare, chiar dacă aceste informații se referă la JUCĂTORUL X, atât timp cât acestea pot fi considerate secrete comerciale. Punerea în balanță necesară a intereselor în temeiul articolului 15 alineatul (4) din RGPD va avea drept rezultat faptul că secretele comerciale ale PLATFORMEI Y împiedică divulgarea acestor date cu caracter personal, deoarece cunoașterea caracteristicilor tehnice de funcționare a software-ului anti-trișare ar putea, de asemenea, să permită utilizatorului să eludeze pe viitor mecanismul de detectare a cazurilor de trișare sau de fraudă[99].

[99] Amploarea informațiilor furnizate persoanelor fizice va depinde în mare măsură de context, ținând seama de natura operatorului și de natura încălcării condițiilor de utilizare. În unele cazuri, operatorul poate furniza informații de bază numai ca răspuns la o cerere de acces căreia i se aplică articolul 15 alineatul (4).

174. În cazul în care operatorii refuză să dea curs unei cereri de acordare a dreptului de acces, integral sau parțial, în temeiul articolului 15 alineatul (4) din RGPD, aceștia trebuie să informeze persoana vizată cu privire la motive fără întârziere și în termen de cel mult o lună [articolul 12 alineatul (4) din RGPD]. Expunerea de motive trebuie să se refere la circumstanțele concrete pentru a permite persoanelor vizate să evalueze dacă doresc să ia măsuri împotriva refuzului. Aceasta trebuie să includă informații cu privire la posibilitatea de a depune o plângere la o autoritate de supraveghere (articolul 77 din RGPD) și de a introduce o cale de atac judiciară (articolul 79 din RGPD).

6.3 Articolul 12 alineatul (5) din RGPD

175. Articolul 12 alineatul (5) din RGPD permite operatorilor să refuze să dea curs cererilor de acordare a dreptului de acces care sunt în mod vădit nefondate sau excesive. Aceste concepte trebuie interpretate în sens restrâns, deoarece principiile transparenței și drepturilor gratuite ale persoanelor vizate nu trebuie să fie subminate.

176. Operatorii trebuie să fie în măsură să demonstreze persoanei fizice motivele pentru care consideră că cererea este în mod vădit nefondată sau excesivă și, dacă i se solicită acest lucru, să explice motivele autorității de supraveghere competente. Fiecare cerere ar trebui analizată de la caz la caz, în contextul în care este înaintată, pentru a decide dacă este în mod evident nefondată sau excesivă.

6.3.1 Ce înseamnă „în mod vădit nefondată”?

177. O cerere de acordare a dreptului de acces este în mod vădit nefondată dacă cerințele de la articolul 15 din RGPD nu sunt îndeplinite în mod clar și evident atunci când se aplică o abordare obiectivă. Cu toate acestea, astfel cum s-a explicat în special în secțiunea 3 de mai sus, există doar foarte puține condiții prealabile pentru cererile de acordare a dreptului de acces. Prin urmare, CEPD subliniază că posibilitatea de a se baza pe alternativa „în mod vădit nefondată” de la articolul 12 alineatul (5) din RGPD în ceea ce privește cererile de acordare a dreptului de acces este foarte limitată.

178. În plus, este important să se reamintească faptul că, înainte de a invoca restricția, operatorii trebuie să analizeze cu atenție conținutul și domeniul de aplicare al cererii. De exemplu, o cerere nu ar trebui să fie considerată în mod vădit nefondată dacă este legată de prelucrarea unor date cu caracter personal care nu fac obiectul RGPD (în acest caz, cererea nu ar trebui tratată deloc ca cerere în temeiul articolului 15).

179. Alte cazuri în care aplicabilitatea articolului 12 alineatul (5) din RGPD este discutabilă sunt cererile legate de activități de informare sau de prelucrare care, în mod clar și evident, nu fac obiectul activităților de prelucrare ale operatorului.

Exemplul 38: o persoană vizată adresează o cerere unei autorități municipale cu privire la datele prelucrate de o autoritate de stat. În loc să argumenteze că cererea este în mod vădit nefondată, ar fi mai adecvat și mai ușor pentru autoritatea solicitată să confirme că aceste date nu sunt prelucrate de autoritate (prima componentă a articolului 15 din RGPD: „dacă” se prelucrează sau nu date cu caracter personal)[100].

[100] O altă întrebare este dacă autoritatea căreia i-a fost adresată cererea de acces are dreptul să transmită cererea către autoritatea de stat competentă.

180. Un operator nu ar trebui să presupună că o cerere este în mod vădit nefondată deoarece persoana vizată a depus anterior cereri care au fost în mod vădit nefondate sau excesive sau dacă include un limbaj neobiectiv sau necorespunzător.

6.3.2 Ce înseamnă „excesivă”?

181. Nu există nicio definiție a termenului „excesivă” în RGPD. Pe de o parte, formularea „în special din cauza caracterului lor repetitiv” de la articolul 12 alineatul (5) din RGPD permite să se concluzioneze că principalul scenariu pentru aplicarea acestui aspect în ceea ce privește articolul 15 din RGPD este legată de numărul de cereri ale unei persoane vizate pentru dreptul de acces. Pe de altă parte, formularea menționată mai sus arată că nu sunt excluse *a priori* alte motive care ar putea cauza un caracter excesiv.

182. Desigur, în conformitate cu articolul 15 alineatul (3) din RGPD privind dreptul de a obține o copie, o persoană vizată poate depune mai multe cereri la un operator[101]. În cazul unor cereri care ar putea fi considerate excesive, evaluarea caracterului „excesiv” depinde de analiza efectuată de operator și de particularitățile sectorului în care acesta își desfășoară activitatea.

183. În cazul cererilor ulterioare, trebuie să se evalueze dacă pragul intervalelor rezonabile (a se vedea considerentul 63) a fost depășit sau nu. Operatorii trebuie să țină seama cu atenție de circumstanțele specifice fiecărui caz.

184. De exemplu, în cazul rețelelor sociale, se preconizează o modificare a setului de date la intervale mai scurte decât în cazul registrelor funciare sau al registrelor centrale ale societăților. În cazul partenerilor de afaceri, ar trebui luată în considerare frecvența contactelor cu clientul. În consecință, „intervalele rezonabile” în care persoanele vizate își pot exercita din nou dreptul de acces sunt, de asemenea, diferite. Cu cât apar mai multe modificări în baza de date a operatorului, cu atât mai des persoanelor vizate li se poate permite să solicite accesul la datele lor cu caracter personal fără ca cererile lor să fie excesive. Pe de altă parte, o a doua solicitare din partea aceleiași persoane vizate ar putea fi considerată repetitivă în anumite circumstanțe.

185. Atunci când decid dacă a trecut un interval rezonabil, operatorii ar trebui să ia în considerare următoarele, având în vedere așteptările rezonabile ale persoanei vizate:

- cât de des sunt modificate datele – este puțin probabil ca informațiile să se fi modificat de la înaintarea unei cereri până la alta? În cazul în care, în mod evident, o bază de date nu face obiectul unui alt tip de prelucrare decât stocarea, iar persoana vizată are cunoștință de acest lucru, de exemplu ca urmare a unei cereri anterioare pentru acordarea dreptului de acces, acesta ar putea reprezenta un indiciu al unei cereri excesive;
- natura datelor – aceasta ar putea include natura deosebit de sensibilă a datelor;
- scopurile prelucrării – acestea ar putea include posibilitatea ca prelucrarea să cauzeze prejudicii (să fie în detrimentul) solicitantului în cazul în care sunt dezvăluite;

[101] În conformitate cu articolul 15 alineatul (3) a doua teză, operatorul poate percepe o taxă rezonabilă pentru copiile suplimentare solicitate.

- dacă cererile ulterioare se referă la același tip de informații sau activități de prelucrare sau la activități diferite[102].

Exemplul 39 (tâmplar): o persoană vizată depune cereri de acces **o dată la două luni** la tâmplarul care a fabricat o masă pentru ea. Tâmplarul a răspuns integral la prima cerere. Atunci când se decide că a trecut un interval rezonabil, ar trebui să se ia în considerare faptul că tâmplarul colectează doar ocazional date cu caracter personal (primul punct marcator de mai sus), și nu ca parte a activității sale principale, și că este cu atât mai puțin probabil ca tâmplarul să furnizeze frecvent servicii aceleiași persoane vizate. Într-adevăr, în cazul de față, tâmplarul nu a furnizat mai mult de un serviciu persoanei vizate, ceea ce face improbabilă apariția unor modificări în setul de date privind persoana vizată. Având în vedere, în special, natura și volumul datelor cu caracter personal prelucrate, riscurile legate de prelucrare pot fi considerate atât de reduse (al doilea punct marcator de mai sus) încât scopul prelucrării (facturare și respectarea obligației de a ține evidențe) nu este de natură să cauzeze prejudicii persoanei vizate (al treilea punct marcator de mai sus). În plus, cererea se referă la aceleași informații ca și ultima cerere (al patrulea punct marcator de mai sus). În consecință, astfel de cereri pot fi considerate excesive din cauza caracterului lor repetitiv.

Exemplul 40 (platformă de comunicare socială): o platformă de comunicare socială a cărei activitate principală constă în colectarea și/sau prelucrarea datelor cu caracter personal ale persoanei vizate desfășoară activități de prelucrare complexe și continue pe scară largă. O persoană vizată care utilizează serviciile platformei depune cereri de acces **o dată la trei luni**. În acest caz, este foarte probabil să aibă loc modificări frecvente ale datelor cu caracter personal referitoare la persoana vizată (primul punct marcator de mai sus), gama largă de date colectate include date cu caracter personal sensibile deduse (al doilea punct marcator de mai sus) prelucrate în scopul prezentării conținutului și a membrilor rețelei relevanți către persoana vizată (al treilea punct marcator). În aceste condiții, cererile de acces înaintate din trei în trei luni pot, în principiu, să nu fie considerate excesive din cauza caracterului repetitiv.

Exemplul 41 (agenții de credit): ca și în cazul rețelelor sociale, nu se poate exclude posibilitatea ca modificările datelor relevante deținute de agențiile de credit să aibă loc la intervale mult mai scurte decât în alte domenii (primul punct marcator de mai sus). Acest lucru reiese din numeroși factori cu care persoana vizată, în calitate de persoană din exterior, nu este de obicei la curent din cauza complexității modelului de afaceri. Prin urmare, răspunsul la întrebarea cu privire la tipurile de date care au fost colectate pentru calcularea punctajului de către operator și care sunt în prezent incluse în calcul poate fi furnizat numai de agenția de credit însăși. În plus, prelucrarea datelor prin intermediul agențiilor de credit și punctajul rezultat pot avea consecințe profunde pentru persoana vizată în ceea ce privește tranzacțiile legale preconizate, cum ar fi încheierea de contracte de cumpărare, de închiriere sau de leasing (al treilea punct marcator de mai sus).

Nu este posibil să se stabilească, în general, niciun interval specific în care depunerea unei cereri suplimentare de acces ar putea fi considerată excesivă în temeiul articolului 12 alineatul (5) a doua teză din RGPD. Este necesară mai degrabă o analiză globală a circumstanțelor fiecărui caz în parte. Cu

[102] Dacă cererea ulterioară se referă la același tip de informații în ceea ce privește domeniul de aplicare ȘI momentul, aceasta nu se consideră a fi un exces, ci o solicitare a unei copii suplimentare; a se vedea subsecțiunea 2.2.2.2.

toate acestea, având în vedere importanța prelucrării datelor pentru realitatea vieții de zi cu zi a persoanelor vizate, se poate presupune că un **interval de un an** între informațiile furnizate în mod gratuit va fi, în orice caz, prea mare pentru ca cererea să fie considerată excesivă. În cazul în care o cerere este depusă într-un interval foarte scurt, factorul decisiv ar trebui să fie dacă persoana vizată are motive să presupună că au avut loc modificări în ceea ce privește informațiile sau prelucrarea de la ultima cerere. De exemplu, în cazul în care persoana vizată a efectuat o tranzacție financiară, cum ar fi contractarea unui împrumut, persoana vizată ar trebui să aibă dreptul de a solicita accesul la informațiile privind creditul, chiar dacă o astfel de cerere a fost depusă și a primit un răspuns cu puțin timp înainte.

186. Atunci când este posibil să se furnizeze informațiile cu ușurință în format electronic sau prin acces de la distanță la un sistem securizat, ceea ce înseamnă că respectarea unor astfel de cereri nu exercită de fapt presiuni asupra operatorului, este puțin probabil ca cererile ulterioare să poată fi considerate excesive.

187. În cazul în care o cerere se suprapune cu o cerere anterioară, cererea care se suprapune poate fi, în general, considerată excesivă dacă și în măsura în care aceasta acoperă exact aceleași informații sau activități de prelucrare, iar operatorul nu a dat curs încă cererii anterioare, fără însă ca aceasta să fi ajuns în stadiul de „întârzieri nejustificate" [a se vedea articolul 12 alineatul (3) din RGPD]. Prin urmare, în practică, cele două cereri ar putea fi combinate.

188. Faptul că operatorul ar avea nevoie de mult timp și efort pentru a furniza informațiile sau copia persoanei vizate nu poate, în sine, să facă o cerere să devină excesivă[103]. Un număr mare de activități de prelucrare implică, de regulă, eforturi mai mari atunci când se dă curs cererilor de acces. Cu toate acestea, astfel cum s-a menționat mai sus, în anumite circumstanțe, cererile pot fi considerate excesive din alte motive decât pentru caracterul lor repetitiv. În opinia CEPD, aceasta include în special cazurile în care persoanele vizate se bazează în mod abuziv pe articolul 15 din RGPD, ceea ce înseamnă cazuri în care persoanele vizate utilizează în mod excesiv dreptul de acces cu unicul scop de a cauza prejudicii sau daune operatorului.

189. În acest context, o cerere nu ar trebui considerată excesivă pentru motivul că:

- persoana vizată nu prezintă motive pentru cerere sau operatorul consideră că cererea este lipsită de sens;
- persoana vizată utilizează un limbaj necorespunzător sau nepoliticos;
- persoana vizată intenționează să utilizeze datele pentru a formula reclamații ulterioare împotriva operatorului[104].

190. Pe de altă parte, o cerere poate fi considerată excesivă, de exemplu, în cazul în care:

- o persoană înaintează o cerere, dar, în același timp, se oferă să o retragă în schimbul unei forme de beneficiu din partea operatorului sau
- cererea este rău intenționată și este utilizată pentru a hărțui operatorul sau angajații acestuia fără alte scopuri decât pentru a cauza perturbări, de exemplu pe baza faptului că:

[103] Fără test de proporționalitate; a se vedea punctul 166 de mai sus.
[104] Acest lucru nu aduce atingere dreptului intern aplicabil care respectă cerințele prevăzute la articolul 23 din RGPD; a se vedea secțiunea 6.4.

- persoana a declarat în mod explicit, în cererea propriu-zisă sau în alte comunicări, că intenționează să cauzeze perturbări și nimic altceva sau
- persoana transmite în mod sistematic diferite cereri unui operator în cadrul unei campanii, de exemplu o dată pe săptămână, cu intenția și efectul de a provoca perturbări[105].

6.3.3 Consecințe

191. În cazul unei cereri în mod vădit nefondate sau excesive privind dreptul de acces, operatorii pot, în conformitate cu articolul 12 alineatul (5) din RGPD, fie să perceapă o taxă rezonabilă (ținând seama de costurile administrative ale furnizării de informații sau ale comunicării sau ale luării măsurilor solicitate), fie să refuze să dea curs cererii.

192. CEPD subliniază că, pe de o parte, operatorii nu sunt obligați, în general, să perceapă o taxă rezonabilă înainte de a refuza să dea curs unei cereri. Pe de altă parte, nici nu sunt pe deplin liberi să aleagă între cele două opțiuni. De fapt, operatorii trebuie să ia o decizie adecvată în funcție de circumstanțele specifice ale cazului. Deși este greu de imaginat că perceperea unei taxe rezonabile este o măsură adecvată în cazul cererilor în mod vădit nefondate, în cazul cererilor excesive – în conformitate cu principiul transparenței – va fi adesea mai adecvat să se perceapă o taxă drept compensație pentru costurile administrative pe care le generează cererile repetitive.

193. Operatorii trebuie să fie în măsură să demonstreze caracterul vădit nefondat sau excesiv al unei cereri [articolul 12 alineatul (5) a treia teză din RGPD]. Prin urmare, se recomandă să se asigure documentarea corespunzătoare a faptelor subiacente. În conformitate cu articolul 12 alineatul (4) din RGPD, în cazul în care operatorii refuză, integral sau parțial, să dea curs unei cereri de acces, aceștia trebuie să informeze persoana vizată fără întârziere și cel târziu în termen de o lună de la primirea cererii cu privire la

- motivul refuzului;
- dreptul de a depune o plângere în fața unei autorități de supraveghere;
- posibilitatea de a introduce o cale de atac judiciară.

194. Înainte de a percepe o taxă rezonabilă în temeiul articolului 12 alineatul (5) din RGPD, operatorii ar trebui să ofere persoanelor vizate o indicație cu privire la planul lor în acest sens. Acestora din urmă trebuie să li se permită să decidă dacă vor retrage cererea pentru a evita să fie taxați.

195. Respingerea nejustificată a cererilor privind dreptul de acces poate fi considerată o încălcare a drepturilor persoanelor vizate în temeiul articolelor 12-22 din RGPD și, prin urmare, poate face obiectul exercitării competențelor corective de către autoritățile de supraveghere competente, inclusiv al amenzilor administrative în temeiul articolului 83 alineatul (5) litera (b) din RGPD. În cazul în care persoanele vizate consideră că există o încălcare a drepturilor lor, acestea au dreptul de a depune o plângere în temeiul articolului 77 din RGPD.

[105] „Transmiterea sistematică în cadrul unei campanii” înseamnă că cererile care ar putea fi combinate cu ușurință într-una singură sunt împărțite în mod artificial de către persoana vizată nu doar în câteva, ci în multe părți, cu intenția evidentă de a cauza perturbări.

6.4 Posibile restricții în dreptul Uniunii sau în dreptul intern al statelor membre în temeiul articolului 23 din RGPD și derogări

196. Domeniul de aplicare al obligațiilor și drepturilor prevăzute la articolul 15 din RGPD poate fi restrâns prin măsuri legislative prevăzute de dreptul Uniunii sau de dreptul intern al statelor membre[106].

197. Operatorii care intenționează să se bazeze pe o restricție întemeiată pe dreptul intern trebuie să verifice cu atenție cerințele prevăzute de dispozițiile legislației naționale respective. În plus, este important de remarcat faptul că restricțiile privind dreptul de acces prevăzute de dreptul intern al statelor membre (sau al Uniunii) care se întemeiază pe articolul 23 din RGPD trebuie să îndeplinească cu strictețe condițiile prevăzute în această dispoziție. CEPD a emis Orientările 10/2020 privind restricțiile în temeiul articolului 23 din RGPD, cu explicații suplimentare în acest sens. În ceea ce privește dreptul de acces, CEPD reamintește că operatorii ar trebui să ridice restricțiile de îndată ce circumstanțele care le justifică nu se mai aplică[107].

198. Măsurile legislative care stabilesc restricții în temeiul articolului 23 din RGPD pot prevedea, de asemenea, întârzierea exercitării unui drept, exercitarea parțială a unui drept sau exercitarea limitată la anumite categorii de date sau posibilitatea de exercitare indirectă a unui drept prin intermediul unei autorități de supraveghere independente[108].

---

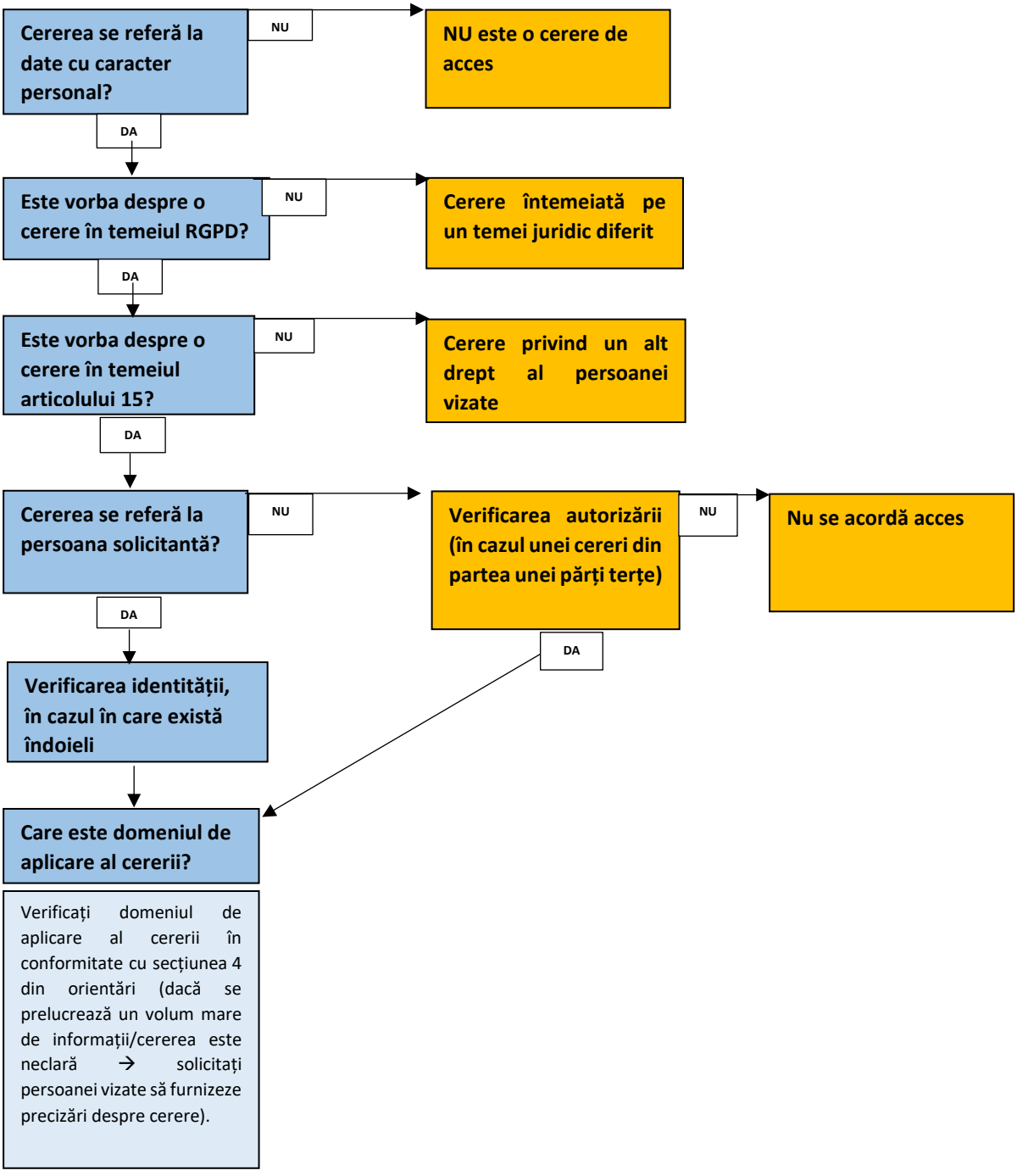
[106] A se vedea, de exemplu, secțiunile 32-37 din Legea federală germană privind protecția datelor (BDSG), secțiunile 16 și 17 din Legea norvegiană privind datele cu caracter personal și capitolul 5 din Legea suedeză privind protecția datelor.

[107] Punctul 76 din Orientările 10/2020 privind restricțiile în temeiul articolului 23 din RGPD, versiunea 2.0, adoptate la 13 octombrie 2021.

[108] Punctul 12 din Orientările 10/2020 privind restricțiile în temeiul articolului 23 din RGPD, versiunea 2.0, adoptate la 13 octombrie 2021. Secțiunea 34 alineatul (3) din Legea federală germană privind protecția datelor prevede, de exemplu, că, în cazul în care o autoritate publică nu furnizează informații unei persoane vizate pentru a da curs unei cereri privind dreptul de acces din cauza anumitor restricții, aceste informații sunt furnizate autorității federale de supraveghere la cererea persoanei vizate, cu excepția cazului în care autoritatea federală supremă responsabilă (a autorității care a făcut obiectul cererii) stabilește, în cazul individual, că o astfel de informare ar pune în pericol securitatea federației sau a unui land. Codul italian privind protecția datelor prevede accesul indirect (prin intermediul autorității) în cazul în care accesul ar putea avea consecințe negative asupra mai multor interese (de exemplu, interesul de a combate spălarea banilor); a se vedea articolul 2-L din Codul italian privind protecția datelor.

ANEXĂ – DIAGRAMĂ

Etapa 1: Cum se interpretează și se evaluează cererea?



Etapa 2: Cum se răspunde la cerere (1)?

Principalele 3 componente ale dreptului de acces (structura articolului 15)		
Confirmare că se prelucrează sau nu date cu caracter personal	Accesul la datele cu caracter personal	Informații suplimentare privind scopurile, destinatarii etc. [articolul 15 alineatul (1)

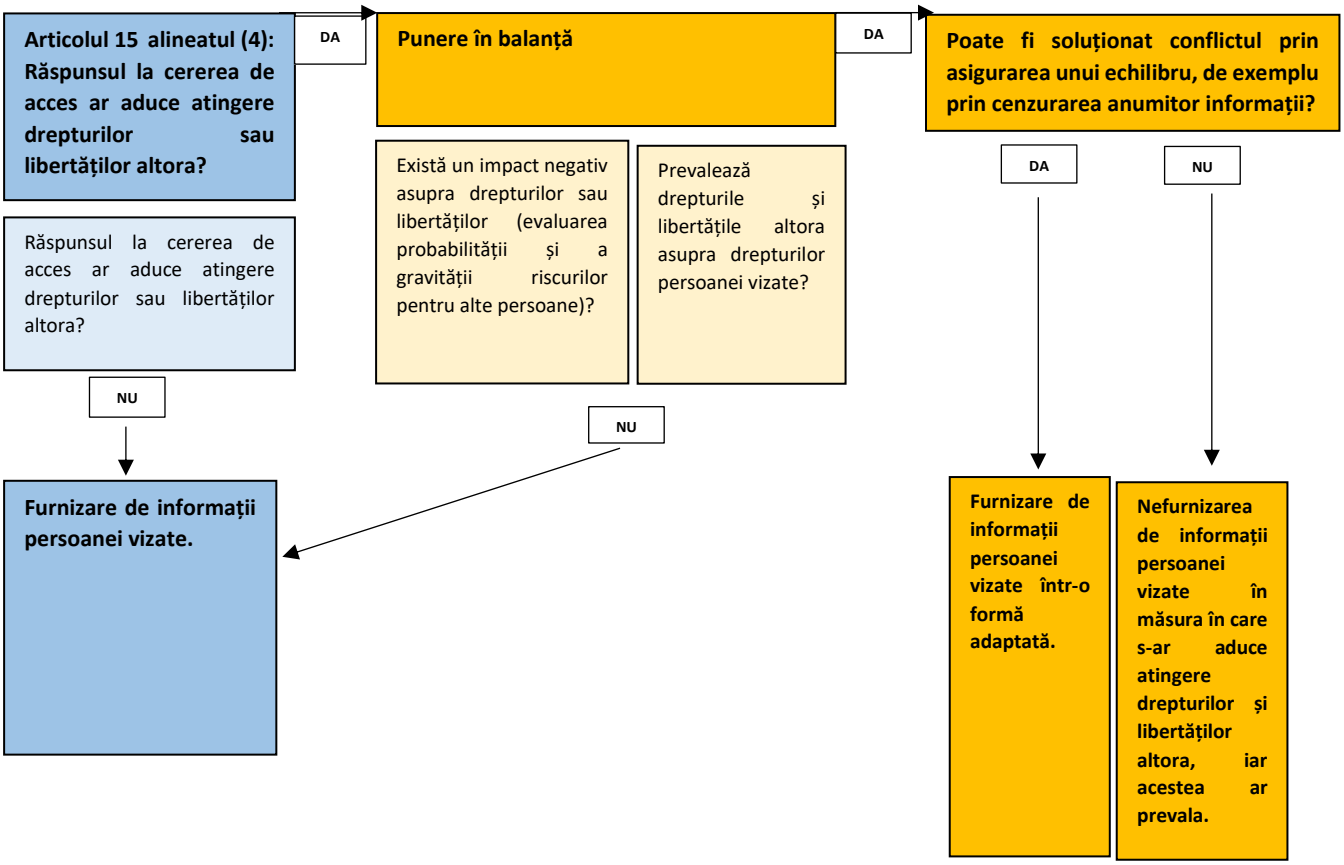
Etapa 2: Cum se răspunde la cerere (2)?

Luarea de măsuri adecvate			
Articolul 12 alineatul (1): formă concisă, transparentă, inteligibilă și ușor accesibilă	Articolul 12 alineatul (2): facilitarea exercitării dreptului de acces		
Alegerea între diferite mijloace	Furnizarea unei copii, cu excepția cazului în care se convine altfel [articolul 15 alineatul (3)]	Utilizarea unei abordări pe mai multe niveluri, dacă este cazul (cea mai relevantă în context online)	Termen – fără întârzieri nejustificate și în orice caz în cel mult o lună (prelungire cu două luni în cazuri excepționale) [articolul 12 alineatul (3)]

Etapa 2: Cum se răspunde la cerere (3)?

Cum poate operatorul să extragă toate datele referitoare la persoana vizată?			
Definirea criteriilor de căutare – pe baza informațiilor furnizate de persoana vizată, a altor informații pe care operatorul le deține cu privire la persoana vizată și a factorilor pe baza cărora sunt structurate datele (de exemplu, numărul de client, adresele IP, titlul profesional, relațiile de familie etc.).	Identificarea oricăror funcții tehnice care ar putea fi disponibile pentru extragerea datelor.	Căutare în toate sistemele informatice sau neinformatice relevante de evidență a datelor.	Compilarea, extragerea sau colectarea în alt mod a datelor care se referă la persoana vizată într-un mod care să reflecte pe deplin prelucrarea, și anume care să includă toate datele cu caracter personal referitoare la persoana vizată, și să permită persoanei vizate să fie informată cu privire la prelucrare și să verifice legalitatea acesteia. Extragerea informațiilor ar putea fi realizată de la caz la caz sau, atunci când este relevant, prin utilizarea unui instrument de protejare a vieții private începând cu momentul conceperii, implementat deja de operator.

Etapa 3: Verificarea limitărilor și a restricțiilor (1)



Etapa 3: Verificarea limitărilor și a restricțiilor (2)