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

Versiunea 2.0

Adoptată la 28 martie 2023

Istoricul versiunilor

Versiunea 1.0	18 ianuarie 2022	Adoptarea Ghidului pentru consultare publică
Versiunea 2.0	28 martie 2023	Adoptarea Ghidului după consultare publică

Traducerea dată nu este o traducere oficială a Comitetului European pentru Protecția Datelor (EDPB) și a fost asigurată, în cadrul unui schimb între GIZ și EDPB, ca rezultat al unui acord reciproc între GIZ și CNPDCP, cu sprijinul financiar al GIZ în cadrul proiectului "Re-ingineria serviciilor publice în cadrul Parteneriatului Estic" din cadrul Fondului Regional pentru Reformele Administrației Publice al Parteneriatului Estic, comandat și finanțat de BMZ.

SUMAR EXECUTIV

Dreptul de acces al persoanelor vizate este consacrat în Carta drepturilor fundamentale a UE la art. 8. A făcut parte din cadrul legal european de protecție a datelor încă de la început și este dezvoltat în continuare prin reguli mai specializate și mai precise în art. 15 din RGPD.

Scopul și structura generală a dreptului de acces

Scopul 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 acestea să poată cunoaște și verifica legalitatea prelucrării și acuratețea datelor prelucrate. Acest lucru va facilita – dar nu ca o condiție – exercitarea de către persoanele fizice a altor drepturi, cum ar fi dreptul la ștergerea sau rectificarea datelor.

Dreptul de acces conform legislației privind protecția datelor trebuie să fie diferențiat de drepturi similare cu alte obiective, de exemplu dreptul de acces la documentele publice, care are ca scop garantarea transparenței în procesul decizional al autorităților publice și a bunei practici administrative.

Cu toate acestea, persoana vizată nu trebuie să motiveze cererea de acces și nu este la latitudinea operatorului să analizeze dacă cererea va ajuta efectiv persoana vizată să verifice legalitatea prelucrării relevante sau să-și exercite alte drepturi. Operatorul va trebui să gestioneze cererea, cu excepția cazului în care este clar că cererea este depusă în conformitate cu alte reguli decât normele de protecție a datelor.

Dreptul de acces include trei componente diferite:

- Confirmarea dacă datele despre persoana fizică sunt sau nu prelucrate,
- Accesul la aceste date cu caracter personal și
- Accesul la informații despre prelucrare, cum ar fi scopul, categoriile de date și destinatarii, durata prelucrării, drepturile persoanelor vizate și garanțiile corespunzătoare în cazul transferurilor în țări terțe.

Considerații generale privind evaluarea cererii persoanei vizate

Atunci când analizează conținutul cererii, operatorul trebuie să evalueze dacă cererea se referă la date cu caracter personal ale solicitantului, dacă cererea intră în sfera de aplicare a art. 15 și dacă există alte prevederi, mai specifice, care reglementează accesul într-un anumit sector. De asemenea, trebuie să evalueze dacă cererea se referă la toate datele sau doar la anumite părți ale datelor prelucrate despre persoana vizată.

Nu există cerințe specifice privind formatul unei cereri. Operatorul ar trebui să ofere canale de comunicare adecvate și ușor de utilizat de persoana vizată. Cu toate acestea, persoana vizată nu este obligată să utilizeze aceste canale specifice și, în schimb, poate trimite cererea unui punct de contact oficial al operatorului. Operatorul nu este obligat să acționeze în cazul cererilor care sunt 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 cu privire la acest lucru și poate refuza să acorde acces, cu excepția cazului în care persoana vizată furnizează informații suplimentare care permit identificarea. Mai mult, în cazul în care operatorul are îndoieli cu privire la faptul că persoana vizată este cine pretinde că este, operatorul poate solicita informații suplimentare pentru a confirma identitatea persoanei vizate.

Solicitarea de informații suplimentare trebuie să fie proporțională cu tipul de date prelucrate, prejudiciul care s-ar putea produce etc. pentru a evita colectarea excesivă a datelor.

Sfera de aplicare a dreptului de acces

Sfera de aplicare a dreptului de acces este determinată de sfera de aplicare a conceptului de date cu caracter personal, astfel cum este definit la art. 4(1) din RGPD. Pe lângă datele cu caracter personal de bază, cum ar fi numele, adresa, numărul de telefon etc., o mare varietate de date pot intra 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 supuse pseudonimizării sunt încă date cu caracter personal spre deosebire de datele anonimizate. Dreptul de acces se referă la datele cu caracter personal ce privesc solicitantul. Acest lucru nu trebuie interpretat excesiv de restrictiv și poate include date care ar putea viza și alte persoane, de exemplu istoricul comunicării care implică mesajele primite și trimise.

Pe lângă furnizarea accesului la date cu caracter personal, operatorul trebuie să furnizeze informații suplimentare despre prelucrare și despre drepturile persoanelor vizate. Astfel de informații se pot baza pe ceea ce este deja compilat în evidența activităților de prelucrare a operatorului (art. 30 din RGPD) și în notificarea de confidențialitate (art. 13 și 14 din RGPD). Cu toate acestea, este posibil ca aceste informații generale să fie actualizate la momentul solicitării sau adaptate pentru a reflecta operațiunile de prelucrare care sunt efectuate în legătură cu anumitul solicitant.

Cum se oferă accesul

Modalitățile de furnizare a accesului pot varia în funcție de cantitatea de date și de complexitatea prelucrării efectuate. Cu excepția cazului în care se specifică în mod explicit altfel, cererea ar trebui să fie înțeleasă ca vizând *toate* datele cu caracter personal referitoare la persoana vizată, iar operatorul poate solicita persoanei vizate să specifice cererea dacă prelucrează o cantitate mare de date.

Operatorul va trebui să caute date cu caracter personal în toate sistemele IT și non-IT de evidență, pe baza unor criterii de căutare care reflectă modul în care sunt structurate informațiile, de exemplu numele și numărul de client. Comunicarea datelor și a altor informații despre prelucrare trebuie să fie furnizată într-o formă concisă, transparentă, inteligibilă și ușor de accesat, folosind un limbaj clar și simplu. Cerințele mai precise în acest sens depind de circumstanțele prelucrării datelor, precum și de capacitatea persoanei vizate de a sesiza și înțelege comunicarea (de exemplu, luând în considerare faptul că persoana vizată este un copil sau o persoană cu nevoi speciale). Dacă datele constau din coduri sau alte „date brute”, acestea pot fi explicate pentru a fi înțelese de persoana vizată.

Principala modalitate de furnizare a accesului este de a furniza persoanei vizate o copie a datelor sale, însă pot fi prevăzute și alte modalități (cum ar fi informații orale și acces pe site), la solicitarea persoanei vizate. Datele pot fi transmise prin e-mail, cu condiția ca toate măsurile de protecție necesare să fie aplicate luând în considerare, de exemplu, natura datelor, sau în alte moduri, de exemplu, un instrument de autoservire.

Uneori, atunci când există o cantitate mare de date și ar fi dificil pentru persoana vizată să înțeleagă informațiile dacă sunt oferite într-un singur volum – în special în contextul online – cea mai potrivită măsură ar putea fi o abordare stratificată. Furnizarea de informații în diferite straturi poate facilita înțelegerea datelor de către persoana vizată. Operatorul trebuie să fie capabil să demonstreze că abordarea stratificată are o valoare adăugată pentru persoana vizată și toate straturile ar trebui furnizate în același timp dacă persoana vizată alege această opțiune.

Copia datelor și informațiile suplimentare ar trebui furnizate într-o formă permanentă, cum ar fi textul scris, care ar putea fi într-o formă electronică utilizată în mod curent, astfel încât persoana vizată să o

poată descărca cu ușurință. Datele pot fi oferite într-o transcriere sau într-o formă compilată atât timp cât toate informațiile sunt incluse și acest lucru nu modifică sau schimbă conținutul informațiilor.

Cererea trebuie să fie îndeplinită cât mai curând posibil și, în orice caz, în termen de o lună de la recepționarea cererii. Acesta poate fi prelungit cu încă două luni, dacă este necesar, ținând cont de complexitatea și numărul cererii. Persoana vizată trebuie apoi informată cu privire la motivul întârzierii. Operatorul trebuie să implementeze măsurile necesare pentru a prelucra cererile cât mai curând posibil și să adapteze aceste măsuri la circumstanțele prelucrării. În cazul în care datele sunt stocate pentru o perioadă foarte scurtă, trebuie să existe măsuri care să garanteze că o cerere de acces poate fi îndeplinită fără ca datele să fie șterse în timp ce cererea este în curs de prelucrare. În cazul în care se prelucrează o cantitate mare de date, operatorul va trebui să pună în aplicare rutine și mecanisme care sunt adaptate complexității prelucrării.

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

Limite și restricții

RGPD permite anumite limitări ale dreptului de acces. Nu există alte scutiri sau derogări. Dreptul de acces este fără nicio rezervă generală la proporționalitate în ceea ce privește eforturile pe care operatorul trebuie să le depună pentru a se conforma cererii persoanei vizate.

Conform art. 15(4), dreptul de a obține o copie nu afectează în mod negativ drepturile și libertățile altora. CEPD este de părere că aceste drepturi trebuie luate în considerare nu numai la acordarea accesului prin furnizarea unei copii, ci și în cazul în care accesul la date este asigurat prin alte mijloace (acces la fața locului, de exemplu). Articolul 15(4) nu este, însă, aplicabil informațiilor suplimentare privind prelucrarea menționată la art. 15(1) lit. a – h. Operatorul trebuie să fie capabil să demonstreze că drepturile sau libertățile altora ar fi afectate negativ în situația concretă. Aplicarea art. 15(4) nu ar trebui să aibă ca rezultat refuzul total al cererii persoanei vizate; ar avea ca rezultat doar omiterea sau facerea ilizibilă a acelor părți care pot avea efecte negative asupra drepturilor și libertăților altora.

Articolul 12(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 mod restrâns. Întrucât există foarte puține condiții prealabile în ceea ce privește cererile de acces, sfera de aplicare a considerării unei cereri ca fiind vădit nefondată este destul de limitată. Cererile excesive depind de specificul sectorului în care funcționează operatorul. Cu cât mai des apar modificări în baza de date a operatorului, cu atât mai des i se poate permite persoanei vizate să solicite acces fără a considera acest lucru excesiv. În loc să refuze accesul, operatorul poate decide să perceapă o taxă de la persoana vizată. Acest lucru ar fi relevant doar în cazul cererilor excesive pentru a acoperi costurile administrative pe care aceste cereri le pot genera. Operatorul trebuie să poată demonstra caracterul vădit nefondat sau excesiv al unei cereri.

Restricții ale dreptului de acces pot exista și în legislația națională a statelor membre, conform art. 23 din RGPD și derogărilor acestuia. Operatorii care intenționează să se bazeze pe astfel de restricții trebuie să verifice cu atenție cerințele dispozițiilor naționale și să ia act de orice condiții specifice care se pot aplica. Astfel de condiții pot fi ca dreptul de acces să fie doar temporar amânat sau ca restricția să se aplice doar anumitor categorii de date.

Cuprins

Comitetul European pentru Protecția Datelor

având în vedere articolul 70(1)(e) din Regulamentul 2016/679/UE 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 SEE și în special Anexa XI și Protocolul 37 la acesta, astfel cum a fost modificat prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

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

întrucât lucrările pregătitoare ale prezentului ghid au implicat colectarea de contribuții de la părțile interesate, atât în scris, cât și la un eveniment dedicat părților interesate privind drepturile persoanelor vizate, pentru a identifica provocările și problemele de interpretare în aplicarea dispozițiilor relevante ale RGPD;

A ADOPTAT URMĂTORUL GHID

1 INTRODUCERE – OBSERVAȚII GENERALE

1. În societatea actuală, datele cu caracter personal sunt prelucrate de entități publice și private, în timpul multor activități, pentru o gamă largă de scopuri și în multe moduri diferite. Persoanele fizice pot fi adesea într-o poziție dezavantajată în ceea ce privește înțelegerea modului în care sunt prelucrate datele lor cu caracter personal, inclusiv tehnologia utilizată în cazul respectiv, indiferent dacă este vorba de o entitate privată sau de o entitate publică. Pentru a proteja datele cu caracter personal ale persoanelor fizice în aceste situații, RGPD a creat un cadru legal coerent și robust, aplicabil în general în ceea ce privește diferitele tipuri de prelucrare, inclusiv prevederile specifice referitoare la drepturile persoanelor vizate.

2. Dreptul de acces la datele cu caracter personal este unul dintre drepturile persoanelor vizate prevăzute la 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 de a obiecta sau dreptul de a nu fi supus luării de decizii individuale automate, inclusiv profilare[2]. Dreptul de acces al persoanei vizate este consacrat atât în Carta drepturilor fundamentale a UE (Carta)[3] cât și în RGPD la art. 15, unde este formulat cu precizie ca drept de acces la date cu caracter personal și la alte informații conexe.

3. Conform RGPD, dreptul de acces constă din trei componente și anume confirmarea faptului că datele cu caracter personal sunt sau nu prelucrate, accesul la acestea și informațiile despre prelucrarea în sine. Persoana vizată poate obține și o copie a datelor cu caracter personal prelucrate, în timp ce această posibilitate nu este un drept suplimentar al persoanei vizate, ci modalitatea de furnizare 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 despre acesta, cât și ca posibilitatea de a

[1] Referirile la „state membre" făcute în acest document ar trebui înțelese ca referiri la „state membre ale SEE".
[2] Art. 15-22 din RGPD.
[3] În temeiul art. 8 alin. 1 din Carta Drepturilor Fundamentale a Uniunii Europene Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc. În temeiul art. 8 alin. 2 propoziția 2, orice persoană are dreptul de acces la datele care au fost colectate care o privesc, precum și dreptul de a obține rectificarea acestora.

accesa și de a verifica aceste date. Operatorul furnizează persoanei vizate, la cererea acesteia, informațiile care intră sub incidența art. 15(1) și (2) din RGPD.

4. Exercitarea dreptului de acces se realizează atât în cadrul legislației privind protecția datelor, în conformitate cu obiectivele legii privind protecția datelor, cât și în special, în cadrul *„drepturilor și libertăților fundamentale ale persoanelor fizice și, mai ales, al dreptului acestora la protecția datelor cu caracter personal”*, astfel cum este prevăzut de art. 1(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 a pune în aplicare acest obiectiv în mod eficient, RGPD urmărește să faciliteze această exercitare printr-un număr de garanții care să permită persoanelor 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 aplicarea mai eficientă a dreptului de acces al persoanei vizate în era digitală, o parte din care, într-un sens mai larg, este și 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, trebuie subliniat 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 stabilite în RGPD a fost atât perfecționat, cât și consolidat; acest lucru se aplică și dreptului de acces. Întrucât modalitățile dreptului de acces sunt acum specificate mai detaliat 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 art. 15, precum și termenul exact de furnizare a datelor conform art. 12(3) din RGPD, obligă operatorul să fie pregătit pentru întrebările persoanelor vizate prin elaborarea unor proceduri de prelucrare a cererilor.

7. Dreptul de acces nu ar trebui privit izolat, deoarece este strâns legat de alte prevederi ale RGPD, în special de principiile de protecție a datelor, inclusiv de corectitudinea și legalitatea prelucrării, de obligația de transparență a operatorului și de alte drepturi ale persoanelor vizate prevăzute la capitolul III din RGPD.

8. În cadrul drepturilor persoanelor vizate, este de asemenea important să se sublinieze importanța art. 12 din RGPD, care stabilește cerințele pentru măsurile corespunzătoare adoptate de operator la furnizarea informațiilor menționate la art. 13 și 14 din RGPD, precum și comunicările prevăzute la art. 15-22 și 34 din RGPD; aceste cerințe specifică, în general, forma, modalitatea și termenul pentru răspunsurile către persoana vizată și, în special, pentru orice informație adresată copilului.

9. CEPD consideră că este necesar să se ofere îndrumări mai precise cu privire la modul în care dreptul de acces trebuie pus în aplicare în diferite situații. Aceste îndrumări urmăresc să analizeze diferitele aspecte ale dreptului de acces. Mai precis, secțiunea de mai jos este menită să ofere o prezentare de ansamblu și o explicație generală a conținutului art. 15 în sine, în timp ce secțiunile ulterioare oferă o analiză mai profundă a celor mai frecvente întrebări practice și probleme privind punerea în aplicare a dreptului de acces.

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

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

2 SCOPUL DREPTULUI DE ACCES, STRUCTURA ARTICOLULUI 15 DIN RGPD SI PRINCIPIILE GENERALE

2.1 Scopul dreptului de acces

10. Dreptul de acces este astfel conceput pentru a permite persoanelor fizice să dețină control asupra datelor cu caracter personal care le privesc, în măsura în care le permite *„să cunoască și să verifice legalitatea prelucrării”*[6]. Mai exact, scopul dreptului de acces este de a face posibil ca persoanele vizate să înțeleagă modul în care sunt prelucrate datele lor cu caracter personal, precum și consecințele unei astfel de prelucrări și să verifice acuratețea datelor prelucrate fără a fi nevoie să justifice intenția lor. Cu alte cuvinte, scopul dreptului de acces este de a oferi persoanelor fizice informații despre prelucrarea datelor suficiente, transparente și ușor accesibile, indiferent de tehnologiile utilizate, și de a le permite să verifice diferite aspecte ale unei anumite activități de prelucrare în conformitate cu RGPD (ex. legalitatea, acuratețea).

11. Interpretarea RGPD prevăzută în prezentul ghid se bazează pe jurisprudența CJUE care a fost aplicată până în prezent. Ținând cont de importanța dreptului de acces, se poate aștepta ca jurisprudența aferentă să evolueze semnificativ în viitor.

12. În conformitate cu deciziile CJUE[7], dreptul de acces are scopul de a garanta protecția dreptului la viață privată al persoanelor vizate și la protecția datelor cu privire la prelucrarea datelor care le privesc [8] și pot facilita exercitarea drepturilor care decurg, de exemplu, din RGPD, articolele 16-19, 21, 22 și 82. Cu toate acestea, exercitarea dreptului de acces este un drept al unei persoane fizice și nu este condiționată de exercitarea celorlalte drepturi, iar exercitarea celorlalte drepturi nu depinde de exercitarea dreptului de acces.

13. Având în vedere scopul larg al dreptului de acces, scopul dreptului de acces nu este adecvat pentru a fi analizat ca o condiție prealabilă pentru exercitarea dreptului de acces de către operator în cadrul evaluării de către acesta a 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 deține date cu caracter personal referitoare la acea persoană fizică (a se vedea secțiunea 4). Prin urmare, de exemplu, operatorul nu ar trebui să refuze accesul pe motiv 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 sau daca suspectează acest lucru.[9] În ceea ce privește limitele și restricțiile dreptului de acces, vă rugăm să consultați secțiunea 6.

Exemplul 1: Un angajator a concediat o persoană. O săptămână mai târziu, persoana decide să colecteze probe pentru a intenta un proces de concediere abuzivă împotriva fostului angajator. Având în vedere acest lucru, persoana îi scrie fostului angajator, solicitând acces la toate datele cu caracter personal ce o privesc, în calitate de persoană vizată, pe care fostul angajator, în calitate de operator, le prelucrează.

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

[6] Considerentul 63 din RGPD.

[7] CJUE, C-434/16, Nowak, și cauzele conexe C-141/12 și C-372/12, YS și Alții.

[8] CJUE, C-434/16, Nowak, alin. 56.

[9] Întrebări legate de acest subiect sunt în discuție într-o cauză aflată în prezent pe rolul CJUE (C-307/22).

vedea secțiunea 3), operatorul trebuie să se conformeze cererii, cu excepția cazului în care cererea se dovedește a fi vădit nefondată sau excesivă în conformitate cu art. 12(5) din RGPD (a se vedea secțiunea 6.3), aspect pe care operatorul trebuie să îl demonstreze.

Variație: Persoana vizată își exercită dreptul de acces cu privire la datele cu caracter personal care o privesc pe parcursul procesului. Cu toate acestea, legislația națională a statului membru, care reglementează relația de muncă dintre operator și persoana vizată, conține anumite dispoziții care limitează sfera informațiilor care trebuie furnizate sau schimbate între părțile la procedurile legale în curs sau viitoare, care sunt aplicabile la procesul de concediere abuzivă pe care persoana vizată l-a intentat. În acest context și cu condiția ca aceste dispoziții naționale să se conformeze cerințelor prevăzute de art. 23 din RGPD[10], persoana vizată nu are dreptul să primească de la operator mai multe informații decât sunt prevăzute de dispozițiile de drept intern ale statului membru care reglementează schimbul de informații între părțile la litigii juridice.

14. Deși scopul dreptului de acces este larg, CJUE a ilustrat, de asemenea, limitele competenței legislației privind protecția datelor și ale dreptului de acces. De exemplu, CJUE a constatat că obiectivul dreptului de acces garantat de legislația UE privind protecția datelor trebuie să fie diferit de cel al dreptului de acces la documentele publice stabilit de legislația UE și cea națională, acesta din urmă vizând „cel mai înalt grad posibil de transparență a procesului decizional al autorităților publice și promovarea bunelor practici administrative”[11], un obiectiv care nu este urmărit de legea privind protecția datelor. CJUE a concluzionat că dreptul de acces la datele cu caracter personal este valabil indiferent dacă se aplică 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 la o cerere de acces și pentru a se asigura că niciunul dintre aspectele acesteia nu poate fi ignorat, este necesar să se înțeleagă mai întâi structura art. 15 și componentele constitutive ale dreptului de acces prevăzute în acest articol.

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

1.	Confirmarea dacă operatorul prelucrează sau nu date cu caracter personal ce privesc solicitantul	Art. 15(1), prima jumătate a propoziției
2.	Accesul la datele cu caracter personal ce privesc solicitantul	Art. 15(1), a doua jumătate a propoziției (prima parte)

[10] Ghidul CEPD 10/2020 privind restricțiile în temeiul art. 23 din RGPD, versiunea pentru consultare publică, 18 decembrie 2020.

[11] CJUE, Cauzele conexe C-141/12 și C-372/12, YS și Alții, alin. 47.

3.	Accesul la următoarele informații despre prelucrare: (a) scopurile prelucrării; (b) categoriile de date cu caracter personal; (c) destinatarii sau categoriile de destinatari; (d) durata preconizată a prelucrării sau criteriile de determinare a duratei; (e) existența drepturilor de rectificare, ștergere, restricționare a prelucrării și obiecție la prelucrare; (f) dreptul de a depune o plângere la o autoritate de supraveghere; (g) orice informații disponibile cu privire la sursa datelor, dacă nu sunt colectate de la persoana vizată; (h) existența unui proces decizional automatizat, inclusiv crearea de profiluri și alte informații referitoare la acestea.	Art. 15(1), a doua jumătate a propoziției (a doua parte)
4.	Informațiile privind garanțiile în temeiul art. 46 în cazul în care datele cu caracter personal sunt transferate către o țară terță sau către o organizație internațională	Art. 15(2)
5.	Obligația operatorului de a furniza o copie a datelor cu caracter personal în curs de prelucrare	Art. 15(3), prima propoziție
6.	Perceperea unei taxe rezonabile de către operator pe baza costurilor administrative pentru orice alte copii solicitate de persoana vizată	Art.15(3), a doua propoziție
7.	Furnizarea de informații în formă electronică	Art. 15(3), a treia propoziție
8.	Ținând cont de drepturile și libertățile celorlalți	Art. 15(4)

În timp ce toate elementele art. 15(1) și (2) definesc împreună conținutul dreptului de acces, art. 15(3) se referă la modalitățile de acces, pe lângă cerințele generale prevăzute la art. 12 din RGPD. Articolul 15(4) completează limitele și restricțiile prevăzute de art. 12(5) din RGPD la drepturile tuturor persoanelor vizate, cu accent special pe drepturile și libertățile altora în contextul accesului.

2.2.1 Definirea conținutului dreptului de acces

17. Articolele 15(1) și (2) cuprind următoarele trei aspecte: în primul rând, confirmarea dacă datele cu caracter personal ale solicitantului sunt în curs de prelucrare, în al doilea rând, accesul la aceste date și, în al treilea rând, informațiile privind prelucrarea. Ele pot fi considerate trei componente diferite care, împreună, construiesc dreptul de acces.

2.2.1.1 Confirmarea „dacă” sunt sau nu prelucrate datele cu caracter personal

18. Atunci când depun o cerere de acces la date cu caracter personal, primul lucru pe care persoanele vizate trebuie să-l știe este dacă operatorul prelucrează sau nu date care le privesc. În consecință, aceste informații constituie prima componentă a dreptului de acces în temeiul art. 15(1). În cazul în care operatorul nu prelucrează date cu caracter personal ce privesc persoana vizată care solicită accesul, informațiile care trebuie furnizate ar fi limitate la confirmarea faptului că nu sunt prelucrate date cu caracter personal ce privesc persoana vizată. În cazul în care operatorul prelucrează date ce privesc solicitantul, operatorul trebuie să confirme acest fapt solicitantului. 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 în curs de prelucrare

19. Accesul la datele cu caracter personal este a doua componentă a dreptului de acces conform art. 15(1) și constituie nucleul acestui drept. Se referă la noțiunea de date cu caracter personal astfel cum este definită de art. 4(1) din RGPD. Pe lângă datele cu caracter personal de bază, cum ar fi numele și adresa, o varietate nelimitată de date pot fi vizate de această definiție, cu condiția ca acestea să intre în sfera de aplicare materială a RGPD, în special în ceea ce privește modul în care sunt prelucrate (art. 2 din RGPD). Accesul la datele cu caracter personal înseamnă astfel accesul la datele cu caracter personal efective în sine, nu doar o descriere generală a datelor și nici o simplă referire la categoriile de date cu caracter personal prelucrate de operator. Dacă nu se aplică limite sau restricții[12], persoanele vizate au dreptul să acceseze toate datele prelucrate ce le privesc sau părți ale acestora, în funcție de sfera de aplicare a cererii (a se vedea secț. 2.3.1). Obligația de a oferi acces la date nu depinde de tipul sau sursa acestor date. Se aplică în întregime chiar și în cazurile în care solicitantul a furnizat inițial datele operatorului, deoarece scopul său este să informeze persoana vizată despre prelucrarea efectivă a acestor date de către operator. Sfera de aplicare a datelor cu caracter personal conform art. 15 este explicată detailat în secț. 4.1 și 4.2.

2.2.1.1 Informații privind prelucrarea și drepturile persoanelor vizate

20. A treia componentă a dreptului de acces este informațiile privind prelucrarea și drepturile persoanelor vizate pe care operatorul trebuie să le furnizeze în temeiul art. 15(1)(a) – (h) și 15(2). Astfel de informații s-ar putea baza pe text preluat, de exemplu, din notificarea de confidențialitate a operatorului[13] sau din înregistrările operatorului privind activitățile de prelucrare menționate la art. 30 din RGPD, dar poate fi necesar să fie actualizate și adaptate la solicitarea persoanei vizate. Conținutul și gradul de specificare a informațiilor sunt detaliate în secțiunea 4.3.

2.2.2 Dispoziții privind modalitățile

21. Articolul 15(3) completează cerințele privind modalitățile de răspuns la cererile de acces prevăzute la art. 12 din RGPD prin unele specificații în contextul cererilor de acces.

2.2.2.1 Furnizarea unei copii

22. În conformitate cu prima propoziție a art. 15(3) din RGPD, operatorul trebuie să furnizeze o copie gratuită a datelor cu caracter personal la care se referă prelucrarea. Prin urmare, copia se referă doar 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 atunci când consideră că costul reproducerii este ridicat (de exemplu: costul furnizării unei copii a înregistrării unei convorbiri telefonice).

23. Obligația de a furniza o copie nu trebuie înțeleasă ca un drept suplimentar al persoanei vizate, ci ca o modalitate de asigurare a accesului la date. Aceasta întărește dreptul de acces la date[14] și ajută la interpretarea acestui drept, deoarece arată clar că accesul la date conform art. 15(1) cuprinde

[12] A se vedea secțiunea 6 din prezentul Ghid.

[13] A se vedea pentru informații Orientările Grupului de lucru instituit în temeiul articolului 29 WP260 rev.01, 11 aprilie 2018 privind transparența în temeiul Regulamentului 2016/679 - aprobate de CEPD (denumite în continuare „Orientările WP29 privind transparența – aprobate de CEPD”).

[14] Obligația de a furniza o copie nu a fost menționată în Directiva 95/46/CE privind protecția datelor.

informații complete cu privire la toate datele și nu poate fi înțeles ca furnizând doar un rezumat al datelor. Totodată, obligația de a furniza o copie nu este menită să lărgească sfera dreptului de acces: se referă (doar) la o copie a datelor cu caracter personal în curs de prelucrare, nu neapărat la o reproducere a documentelor originale (a se vedea secțiunea 5, alin. 152). În termeni mai generali, nu există informații suplimentare care trebuie furnizate persoanei vizate la oferirea unei copii: sfera de aplicare a informațiilor care trebuie conținute în copie este sfera de aplicare a accesului la date conform articolului 15(1) (a doua componentă a dreptului de acces menționat mai sus, a se vedea alineatul 19), care include toate informațiile necesare pentru a permite persoanei vizate să înțeleagă și să verifice legalitatea prelucrării.[15]

24. În lumina celor de mai sus, dacă accesul la date în sensul art. 15(1) se interpretează ca furnizând o copie, obligația de a furniza o copie menționată la 15(3) trebuie respectată. Obligația de a furniza o copie servește obiectivelor dreptului de acces pentru a permite persoanei vizate să cunoască și să verifice legalitatea prelucrării (considerentul 63). Pentru a atinge aceste obiective, persoana vizată, în cele mai multe cazuri, trebuie să vadă informațiile nu numai temporar. Prin urmare, persoana vizată va trebui să obțină accesul la informații prin primirea unei copii a datelor cu caracter personal.

25. Având în vedere cele de mai sus, noțiunea de copie trebuie interpretată într-un sens larg și include diferitele tipuri de acces la datele cu caracter personal atât timp cât este completă (adică include toate datele cu caracter personal solicitate) și posibil de păstrat de către persoana vizată. Astfel, cerința de a furniza o copie înseamnă că informațiile despre datele cu caracter personal ce privesc solicitantul sunt furnizate persoanei vizate într-un mod care să permită persoanei vizate să păstreze toate informațiile și să le acceseze din nou.

26. În pofida acestei interpretări cuprinzătoare a noțiunii de copie și având în vedere că aceasta este modalitatea principală prin care ar trebui să se asigure accesul, în anumite circumstanțe , alte modalități de acces ar putea fi mai potrivite. Explicații suplimentare cu privire la copii și alte modalități de furnizare a accesului sunt oferite în secțiunea 5, în special alin. 5.2.2 – 5.2.5.

2.2.2.2 Furnizarea copiilor suplimentare

27. A doua propoziție din articolul 15(3) se referă la situațiile în care persoana vizată solicită operatorului mai mult de o copie, de exemplu în cazul în care prima copie a fost pierdută sau deteriorată sau persoana vizată dorește să predea o copie unei alte persoane sau unei autorități de supraveghere. Pe baza faptului că la cererea persoanei vizate trebuie furnizate copii suplimentare de către operator, art. 15(3) prevede că, pentru orice copie suplimentară solicitată, operatorul poate percepe o taxă rezonabilă bazată pe costurile administrative (art. 15(3), a doua propoziție).

28. În cazul în care persoana vizată solicită o copie suplimentară după formularea primei cereri, pot apărea întrebări dacă aceasta ar trebui considerată o nouă cerere sau dacă persoana vizată dorește o copie suplimentară a datelor în sensul art. 15(3), a doua propoziție, caz în care se poate percepe o taxă pentru o copie suplimentară. Răspunsul la aceste întrebări depinde exclusiv de conținutul cererii: cererea trebuie interpretată ca solicitarea unei copii suplimentare, în măsura în care, din punctul de vedere al timpului și al sferei de aplicare, se referă la aceeași prelucrare a datelor cu caracter personal ca și cererea anterioară. În cazul în care, totuși, persoana vizată își propune să obțină informații cu privire la datele prelucrate într-un moment diferit de timp sau referitoare la un set de date diferit de cel solicitat inițial, se aplică din nou dreptul de a obține o copie gratuită conform art. 15(3). Acest lucru este valabil și în cazurile în care persoana vizată a depus o primă cerere cu puțin timp înainte. O persoană vizată își

[15] Întrebări legate de subiectul acestui alineat sunt în discuție într-o cauză aflată în prezent pe rolul CJUE (C487/21).

poate exercita dreptul de acces printr-o cerere ulterioară și poate obține o copie gratuită, cu excepția cazului în care cererea este considerată excesivă în temeiul art. 12(5) cu posibilitatea de a percepe o taxă rezonabilă în conformitate cu art. 12(5)(a) (cu privire la caracterul excesiv al cererilor repetitive, a se vedea secțiunea 6).

Exemplul 2: Un client trimite o cerere de acces la o societate comercială. După un an de la răspunsul societății, același client depune o cerere de acces conform art. 15 către aceeași societate. Indiferent dacă au existat noi tranzacții comerciale sau alte contacte între părți de la cererea anterioară, această a doua cerere trebuie considerată o nouă cerere. Chiar dacă societatea nu a operat nicio modificare în prelucrarea datelor – ceea ce nu este neapărat evident pentru persoana vizată – persoana vizată are dreptul să obțină o copie gratuită a datelor.

Variația 1: Chiar dacă clientul în cazurile de mai sus depune noua cerere, de exemplu, la numai o săptămână după prima cerere, aceasta poate fi considerată o nouă cerere conform art. 15 alin. (1) și (3), prima propoziție, dacă nu se interpretează ca un simplu memento al primei cereri. În ceea ce privește intervalul scurt și în funcție de circumstanțele specifice noii cereri, caracterul excesiv al acesteia conform art. 12(5) este pus în discuție (a se vedea secțiunea 6).

Variația 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, desigur, să fie considerată o cerere de copie suplimentară, deoarece se referă la cererea anterioară în domeniul și timpul prelucrării.

29. În cazul în care persoana vizată trimite din nou o cerere de acces pe motiv că răspunsul primit nu a fost complet sau că refuzul nu a fost motivat, această cerere nu trebuie considerată o nouă cerere, întrucât este doar o reamintire a unei prime cereri nesatisfăcute.

30. Referitor la repartizarea costurilor în cazul cererilor de furnizare a unei copii suplimentare, art. 15(3) stabilește că operatorul poate percepe o taxă rezonabilă pe baza costurilor administrative pe care cererea le implică. Aceasta înseamnă că costurile administrative reprezintă un criteriu relevant pentru stabilirea sumei taxei. În același timp, la stabilirea taxei ar trebui să se țină cont de importanța dreptului de acces ca fiind un drept fundamental al persoanei vizate. Operatorul nu ar trebui să transfere costurile generale sau alte cheltuieli generale persoanei vizate, ci ar trebui să se concentreze pe costurile specifice care au fost 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 scăzute, inclusiv atunci când operatorul implică suport extern.

31. În cazul în care operatorul decide să perceapă o taxă, acesta trebuie să notifice în prealabil despre acest lucru și să indice valoarea cât mai exactă a costurilor pe care intenționează să le perceapă de la persoana vizată pentru a-i oferi acesteia din urmă posibilitatea de a stabili dacă va menține sau retrage cererea.

2.2.2.3 Punerea la dispoziție a informațiilor într-o formă electronică utilizată în mod curent

32. În cazul unei cereri transmise prin mijloace electronice, informațiile la fel vor fi furnizate prin mijloace electronice, acolo unde este posibil, și cu excepția cazului în care persoana vizată solicită altfel [a se vedea art. 12(3) din RGPD]. Articolul 15(3), propoziția a treia, completează această cerință în contextul cererilor de acces prin precizarea că operatorul este, de asemenea, obligat să furnizeze răspunsul într-o formă electronică utilizată în mod curent, cu excepția cazului în care persoana vizată solicită altfel. Articolul 15(3) presupune că pentru operatorii care pot primi cereri electronice va fi posibilă furnizarea răspunsului la cerere într-un format electronic utilizat în mod curent (pentru detalii a se vedea secț. 5.2.5). Această prevedere vizează toate informațiile care trebuie furnizate în conformitate cu art. 15(1)

și (2). Prin urmare, în cazul în care persoana vizată depune cererea de acces prin mijloace electronice, toate informațiile trebuie furnizate într-o formă electronică utilizată în mod curent. Chestiunile de format sunt dezvoltate în continuare în secțiunea 5. Operatorul ar trebui, ca de obicei, să aplice măsuri de securitate adecvate, în special atunci când gestionează categorii speciale de date cu caracter personal (a se vedea punctul 2.3.4 de mai jos).

2.2.3 Posibila limitare a dreptului de acces

33. În cele din urmă, în contextul dreptului de acces, o limitare specifică este prevăzută la art. 15(4). Acesta afirmă că trebuie luate în considerare posibilele efecte negative asupra drepturilor și libertăților altora. Întrebări cu privire la sfera de aplicare și consecințele acestei limitări, precum și la limitele și restricțiile suplimentare prevăzute la art. 12(5) sau art. 23 din RGPD sunt explicate în secțiunea 6.

2.3 Principiile generale ale dreptului de acces

34. Atunci când persoanele vizate depun o cerere de acces la datele lor, în principiu, informațiile menționate la art. 15 din RGPD trebuie întotdeauna furnizate în întregime. În consecință, în cazul în care operatorul prelucrează date ce privesc persoana vizată, operatorul trebuie să furnizeze toate informațiile menționate la art. 15(1) și, după caz, informațiile prevăzute la art. 15(2). Operatorul trebuie să ia măsurile corespunzătoare pentru a se asigura că informațiile sunt complete, corecte și actualizate, și că acestea corespund cât mai îndeaproape posibil stării de prelucrare a datelor la momentul recepționării cererii [16]. În cazul în care doi sau mai mulți operatori prelucrează date în comun, aranjamentul operatorilor în comun cu privire la responsabilitățile lor legate de exercitarea drepturilor persoanelor vizate, în special în ceea ce privește răspunsul la cererile de acces, nu afectează drepturile persoanelor vizate față de operatorul căruia îi adresează cererea[17].

2.3.1 Exhaustivitatea informațiilor

35. Persoanele vizate au dreptul, cu excepțiile menționate mai jos, să li se dezvăluie toate datele ce 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 altfel, o cerere de exercitare a dreptului de acces trebuie înțeleasă în termeni generali, cuprinzând toate datele cu caracter personal ce privesc persoana vizată[18]. Limitarea accesului la o parte a informațiilor poate fi luată în considerare în următoarele cazuri:

a) Persoana vizată a limitat în mod explicit cererea la o subcategorie. Pentru a 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 doleanței persoanei vizate (pentru detalii suplimentare, a se vedea secțiunea 3.1.1, alin. 51). În principiu, persoana vizată nu trebuie să trimită repetat cererea de transmitere a tuturor datelor pe care persoana vizată are dreptul să le obțină.

b) În situațiile în care operatorul prelucrează o cantitate mare de date ce privesc persoana vizată, operatorul poate avea îndoieli dacă o cerere de acces, care este exprimată în termeni foarte generali, vizează într-adevăr primirea de informații cu privire la toate tipurile de date în curs de prelucrare sau pe toate ramurile de activitate ale operatorului în detaliu. Acestea pot apărea în special în situațiile în care nu a existat posibilitatea de a furniza persoanei vizate instrumente pentru a-și specifica cererea de

[16] Pentru îndrumări privind măsurile corespunzătoare a se vedea secț. 5 alin. 123 – 129

[17] Orient[rile CEPD 07/2020 privind conceptele de operator și persoană împuternicită de către operator în cadrul RGPD, alin. 162f. Persoanele împuternicite de către operator trebuie să asiste operatorul, ibd., alin. 129.

[18] Pentru detalii, a se vedea secțiunea 5.2.3 de mai jos pe tema abordării stratificate.

la început sau în care persoana vizată nu a făcut uz de acestea. Operatorul se confruntă apoi cu probleme privind modul de a oferi un răspuns complet, evitând în același timp crearea unei supraîncărcări a fluxului de informații pentru persoana vizată de care persoana vizată nu este interesat și pe care nu le poate gestiona eficient. Pot exista modalități de a rezolva această problemă, în funcție de circumstanțe și de posibilitățile tehnice, de exemplu prin furnizarea de instrumente de autoservire în contexte online (a se vedea secțiunea 5 despre abordarea stratificată). Dacă astfel de soluții nu sunt aplicabile, un operator care prelucrează o cantitate mare de informații ce privesc persoana vizată poate solicita persoanei vizate să specifice informațiile sau prelucrarea la care se referă cererea înainte ca informațiile să fie livrate (a se vedea considerentul 63 din RGPD). Exemple în acest sens pot include o companie cu mai multe domenii de activitate sau o autoritate publică cu unități administrative diferite, dacă operatorul a constatat că în acele sucursale sunt prelucrate numeroase date ce privesc persoana vizată. În plus, o mare cantitate de date poate fi prelucrată de către operatori care colectează date privind activitățile frecvente ale persoanei vizate pe o perioadă prelungită de timp.

Exemplul 3: O autoritate publică prelucrează date despre persoana vizată într-un număr de departamente diferite, în diferite contexte. Gestionarea și păstrarea fișierelor este parțial prelucrată prin mijloace neautomatizate și majoritatea datelor sunt stocate doar în fișiere de hârtie. În ceea ce privește formularea generală a cererii, autoritatea publică se îndoiește că persoana vizată este la curent cu amploarea cererii, în special varietatea operațiunilor de prelucrare pe care aceasta le-ar cuprinde, cantitatea de informații și numărul de pagini pe care persoana vizată le-ar primi.

Exemplul 4: O mare companie de asigurări primește o cerere de acces general prin scrisoare de la o persoană care este client de mulți ani. Chiar dacă perioadele de ștergere sunt respectate pe deplin, compania prelucrează de fapt o mare cantitate de date ce privesc clientul, deoarece prelucrarea este încă necesară pentru îndeplinirea obligațiilor contractuale care decurg din relația contractuală cu clientul (inclusiv, de exemplu, obligații continue, comunicarea pe probleme controversate cu clientul și cu terțe părți, …) sau pentru a se conforma obligațiilor legale (date arhivate care trebuie stocate în scopuri fiscale etc.). Compania de asigurări poate avea îndoieli că cererea, care a fost formulată în termeni foarte generali, este cu adevărat destinată să cuprindă toate tipurile de date respective. Acest lucru poate fi mai ales problematic dacă compania de asigurări deține doar adresa poștală a persoanei vizate și, prin urmare, trebuie să trimită orice informații pe suport de hârtie. Cu toate acestea, aceleași îndoieli pot fi relevante și în cazul furnizării informațiilor prin alte mijloace.

Dacă, în astfel de cazuri, operatorul decide să solicite persoanei vizate să depună o cerere mai exactă, pentru a-și îndeplini obligația de a facilita exercitarea dreptului de acces (art. 12(2) din RGPD), operatorul trebuie în același timp să ofere informații semnificative despre operațiunile sale de prelucrare care ar putea viza persoana vizată informând despre ramurile relevante ale activităților sale, bazele de date etc.

Exemplul 5: Într-un raport de muncă, în cazul unei cereri de acces general formulate, nu este clar în sine că angajatul dorește să primească toate datele de autentificare a utilizatorului, datele despre accesul la un loc de muncă, datele despre decontările în cantină, datele despre plățile de salariu etc. O cerere de specificare făcută de angajator ar putea duce, de exemplu, la clarificarea faptului că interesul angajatului este să înțeleagă sau să verifice cui i-a fost transmisă evaluarea performanței sale. Fără cerere de specificare, angajatul ar primi o cantitate mare de informații, fără a avea un interes pentru majoritatea datelor. În același timp, angajatorul ar trebui să ofere informații cu privire la diferitele contexte de prelucrare care l-ar putea preocupa pe angajat, pentru a-i permite acestuia să precizeze în mod rațional cererea.

Este important de subliniat faptul că cererea de specificare nu are ca scop limitarea răspunsului la cererea de acces și nu va fi utilizată pentru a ascunde nicio informație cu privire la date sau la prelucrarea ce privește persoana vizată. Dacă persoana vizată, căreia i s-a cerut să precizeze sfera de aplicare a cererii sale, confirmă că își dorește să caute toate datele cu caracter personal care o privesc, operatorul este obligat să le furnizeze în întregime.

În orice caz, operatorul ar trebui să fie întotdeauna în măsură să demonstreze că modalitatea de prelucrare a cererii urmărește să ofere cel mai larg efect dreptului de acces și că este în conformitate cu obligația sa de a facilita exercitarea drepturilor persoanelor vizate [art. 12(2) din RGPD]. Sub rezerva acestor principii, operatorul poate aștepta răspunsul persoanei vizate înainte de a furniza date suplimentare conform doleanței persoanei vizate, dacă operatorul a oferit persoanei vizate o imagine de ansamblu clară a tuturor operațiunilor de prelucrare care ar putea să privească persoana vizată, inclusiv în special cele la care persoana vizată s-ar putea să nu se aștepte, dacă operatorul a dat, 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 indicarea clară a modului în care dorește să obțină acces la celelalte părți ale datelor prelucrate.

c) Se aplică excepții sau restricții la dreptul de acces (a se vedea mai jos în secțiunea 6). În astfel de cazuri, operatorul trebuie să verifice cu atenție la ce părți ale informațiilor 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) poate să nu fie afectată de excepție. Ca urmare, trebuie furnizate informații cu privire la toate datele cu caracter personal și toate informațiile menționate la art. 15(1) și (2) care nu sunt vizate de excepție sau restricție.

2.3.2 Corectitudinea informațiilor

36. Informațiile incluse în copia datelor cu caracter personal furnizate persoanei vizate trebuie să cuprindă informațiile reale sau datele cu caracter personal deținute despre persoana vizată. Acestea includ obligația de a furniza informații despre datele incorecte sau despre prelucrarea datelor care nu este sau nu mai este legală. Persoana vizată poate folosi, de exemplu, dreptul de acces pentru a afla care este sursa datelor incorecte care circulă între diferiți operatori. Dacă operatorul a corectat datele eronate înainte de a informa persoana vizată despre aceasta, persoana vizată ar fi lipsită de această posibilitate. Același lucru este valabil și în cazul prelucrării ilegale. Posibilitatea de a fi la curent cu prelucrarea ilegală referitoare la persoana vizată este unul dintre scopurile principale ale dreptului de acces. Obligația de a informa cu privire la starea neschimbată a prelucrării nu aduce atingere obligației operatorului de a înceta prelucrarea ilegală sau de a corecta datele eronate. Întrebările referitoare la ordinea în care acele obligații trebuie îndeplinite își găsesc răspunsul în cele ce urmează.

2.3.3 Momentul de referință al evaluării

37. Evaluarea datelor în curs de prelucrare reflectă cât mai aproape posibil situația în care operatorul primește cererea, iar răspunsul ar trebui să acopere toate datele disponibile la acel moment. Aceasta înseamnă că operatorul trebuie să încerce să afle fără întârzieri nejustificate toate activitățile de prelucrare a datelor ce privesc persoana vizată. Prin urmare, operatorii nu sunt obligați să furnizeze datele cu caracter personal pe care le-au prelucrat în trecut, dar pe care nu le mai au la dispoziție[19]. De

[19] A se vedea, în acest sens, precizări suplimentare în secțiunea 4 din prezentul ghid, precum și în Curtea de Justiție a Uniunii Europene, C-553/07, 7 mai 2009, *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer* privind dreptul de acces la informații despre destinatari sau categorii de destinatari în ceea ce privește trecutul.

exemplu, operatorul poate să fi șters datele cu caracter personal în conformitate cu politica sa de păstrare a datelor și/sau cu prevederile statutare și, prin urmare, ar putea să nu mai poată furniza datele cu caracter personal solicitate. În acest context, trebuie reamintit că perioada de păstrare a datelor trebuie stabilită în conformitate cu art. 5(1)(e) din RGPD, deoarece orice păstrare a datelor trebuie să fie justificată în mod obiectiv.

38. Totodată, operatorul va implementa în prealabil măsurile necesare pentru a facilita exercitarea dreptului de acces și pentru a soluționa astfel de cereri în cel mai scurt timp posibil [a se vedea art. 12(3)] și înainte să fie nevoie ca datele să fie șterse. Prin urmare, în cazul unor perioade scurte de păstrare, măsurile luate pentru a răspunde la cerere ar trebui adaptate la perioada de păstrare adecvată pentru a facilita exercitarea dreptului de acces și pentru a evita imposibilitatea permanentă de a asigura accesul la datele prelucrate la momentul cererii[20]. În unele cazuri, s-ar putea, totuși, să nu fie posibil să se răspundă la o cerere înainte de momentul în care datele sunt programate pentru ștergere. De exemplu, dacă în cursul răspunsului la o cerere cât mai prompt posibil, un operator preia date cu caracter personal care au fost programate pentru a fi șterse în ziua următoare, operatorul poate avea nevoie de timp suplimentar pentru a analiza dacă trebuie făcute redactări pentru a proteja libertățile altora înainte de a elibera solicitantului o copie a datelor cu caracter personal. În cazul în care datele au fost preluate în perioada de păstrare programată, operatorul poate continua să prelucreze acele date în scopul îndeplinirii obligației sale de a răspunde la cerere. Prelucrarea în astfel de cazuri se poate baza pe art. 6(1)(c) în combinație cu articolul 15 din RGPD și durata acesteia trebuie să se conformeze cerințelor art. 12(3) din RGPD[21]. Aplicarea acestui temei legal se limitează la prelucrarea datelor identificate a fi necesare pentru a răspunde la cererea concretă și nu se va utiliza ca justificare a prelungirii generale a perioadelor de păstrare.

39. În plus, operatorul nu trebuie să evite în mod deliberat obligația 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 2.3.2). Dacă, în cursul prelucrării cererii de acces, operatorul descoperă date incorecte sau prelucrare ilegală, operatorul trebuie să evalueze starea prelucrării și să informeze persoana vizată în mod corespunzător înainte de a-și îndeplini celelalte obligații. Pentru propriul interes, pentru a evita necesitatea unei comunicări ulterioare în acest sens, precum și pentru a se conforma principiului transparenței, operatorul ar trebui să adauge informații despre rectificările sau ștergerile ulterioare.

Exemplul 6: În cazul răspunsului la o cerere de acces, un operator își dă seama că în compania operatorului a fost stocată o cerere de candidatură a persoanei vizate la o ofertă de muncă după perioada de păstrare. În acest caz, operatorul nu poate șterge mai întâi și apoi răspunde persoanei vizate că nu sunt date prelucrate (referitoare la cerere). Mai întâi trebuie să acorde acces și apoi să șteargă datele. Pentru a preveni o cerere ulterioară de ștergere, ar fi recomandat să se adauge informații despre faptul și momentul ștergerii.

Pentru a se conforma cu principiul transparenței, operatorii ar trebui să informeze persoana vizată cu privire la momentul specific al prelucrării la care se referă răspunsul operatorului. În unele cazuri, de exemplu în contexte de activități de comunicare frecvente, pot apărea prelucrări suplimentare sau modificări ale datelor între acest moment de referință la care a fost evaluată prelucrarea și răspunsul

[20] De exemplu, implementarea unui instrument de autoservire care să permită subiectului de date să acceseze cu ușurință datele cu caracter personal solicitate și un sistem de notificare care alertează operatorul cu privire la o cerere care se referă la date cu caracter personal cu perioade scurte de păstrare ar putea fi luată în considerare pentru a facilita o acțiune promptă.

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

operatorului. Dacă operatorul este la curent cu astfel de modificări, se recomandă să includă informații despre acele modificări, precum și informații despre prelucrarea suplimentară necesară pentru a răspunde la cerere.

2.3.4 Respectarea cerințelor de securitate a datelor

40. Întrucât comunicarea și punerea la dispoziția persoanei vizate a datelor cu caracter personal este o operațiune de prelucrare, operatorul este întotdeauna obligat să implementeze măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate corespunzător riscului prelucrării [a se vedea art. 5(1)(f), 24 și 32 din RGPD]. Acest lucru se aplică independent de modalitatea în care este asigurat accesul. În cazul transmiterii non-electronice a datelor către persoana vizată, în funcție de riscurile pe care le prezintă prelucrarea, operatorul poate lua în considerare utilizarea scrisorii recomandate sau, alternativ, să ofere, dar nu să oblige persoana vizată, să ridice fișierul contra semnătură direct de la unul dintre sediile operatorului. Dacă, în conformitate cu art. 12(1) și (3), informațiile sunt furnizate prin mijloace electronice, operatorul alege mijlocul electronic care se conformează cerințelor de securitate a datelor. De asemenea, în cazul furnizării unei copii a datelor într-o formă electronică utilizată în mod curent [a se vedea art. 15(3)], operatorul trebuie să țină cont de cerințele de securitate a datelor atunci când alege modalitatea de transmitere a fișierului electronic către persoana vizată. Aceasta poate include aplicarea criptării, protecției cu parolă 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 securitate a datelor ar necesita criptarea integrală a e-mailurilor, dar operatorul ar putea trimite doar un e-mail obișnuit, operatorul va trebui să recurgă la alte mijloace, cum ar fi trimiterea unui stick USB prin scrisoare (recomandată) către persoana vizată.

3 CONSIDERAȚII GENERALE PRIVIND EVALUAREA CERERILOR DE ACCES

3.1 Introducere

41. La primirea cererilor de acces la date cu caracter personal, operatorul trebuie să evalueze fiecare cerere în mod individual. Operatorul ia în considerare, printre altele, următoarele aspecte, dezvoltate în continuare în următoarele paragrafe: dacă cererea se referă la date cu caracter personal ce privesc solicitantul și cine este solicitantul. Această secțiune își propune să clarifice ce elemente ale cererii de acces ar trebui să ia în considerare operatorul în procesul de evaluare și să abordeze posibile scenarii pentru o astfel de evaluare, precum și consecințele acesteia. Atunci când evaluează o cerere de acces la date cu caracter personal, operatorul va lua în considerare, în temeiul art. 12(2) din RGPD, și obligația de a facilita exercitarea drepturilor persoanelor vizate respectând în același timp securitatea datelor cu caracter personal[22].

[22] Operatorul asigură securitatea corespunzătoare a datelor cu caracter personal, în conformitate cu principiul integrității și confidențialității [art. 5 alineatul (1) litera (f) din RGPD], prin implementarea măsurilor tehnice și organizatorice corespunzătoare, astfel cum se prevede la art. 32 din RGPD și astfel cum este detailat la art. 24 din RGPD. Operatorul trebuie să poată demonstra 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 Art. 29 privind principiul responsabilității, adoptat la 13 iulie 2010, 00062/10 /EN WP 173 și Ghidul CEPD nr 07/2020 privind conceptele de operator și persoană împuternicită de către operator în RGPD).

42. Prin urmare, operatorii ar trebui să fie pregătiți în mod proactiv să gestioneze 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 constituie obiectul acestei secțiuni a ghidului) și să ofere un răspuns corespunzător solicitantului, 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, sfera de aplicare, contextul și scopurile prelucrării, precum și de riscurile la adresa drepturilor și libertăților persoanelor fizice, în conformitate cu art. 24 din RGPD. În funcție de circumstanțele particulare, operatorilor li se poate cere, de exemplu, să implementeze o procedură corespunzătoare, a cărei implementare ar trebui să garanteze securitatea datelor fără a împiedica exercitarea drepturilor persoanei vizate.

3.1.1 Analiza conținutului cererii

43. Această problemă poate fi evaluată în mod specific prin adresarea următoarelor întrebări.

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

44. În conformitate cu RGPD, sfera de aplicare a cererii acoperă numai datele cu caracter personal[23]. Prin urmare, orice solicitare de informații despre 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 să fie considerată o cerere formulată în temeiul art. 15 din RGPD. În plus, o solicitare de informații despre date anonime sau date care nu privesc persoana vizată sau persoana în numele căreia persoana împuternicită a depus cererea, nu va intra în sfera 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 unor informații suplimentare, sunt date cu caracter personal[24]. Astfel, datele pseudonimizate care pot fi legate de un persoană vizată – de ex. atunci când persoana vizată furnizează identificatorul respectiv care să permită identificarea acesteia sau când operatorul este în măsură să conecteze datele cu solicitantul prin mijloace proprii – vor fi considerate a intra în sfera de aplicare a cererii[25].

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

46. Ca regulă generală, o cerere poate viza numai datele solicitantului. Accesul la datele altor persoane poate fi solicitat numai cu autorizarea corespunzătoare [26].

Exemplul 7: Persoana vizată X lucrează în calitate de manager de departament pentru o companie care oferă locuri de parcare pentru managerii săi la o parcare a companiei. Deși persoana vizată X are un loc de parcare permanent, atunci când persoana vizată ajunge la birou pentru a doua tură, acest spațiu

[23] Cu excepția cazului în care cererea acoperă și date nepersonale legate indisolubil de datele cu caracter personal ale persoanei vizate. Pentru explicații suplimentare, a se vedea alin. 100.

[24] A se vedea considerentul 26 din RGPD. Explicații suplimentare cu privire la conceptele de date anonime și date pseudonimizate pot fi găsite în Avizul WP29 4/2007 privind conceptul de date cu caracter personal, p. 18 – 21.

[25] Orientările Grupului de lucru Art. 29, WP242 rev.01, 5 aprilie 2017, privind dreptul la portabilitatea datelor - adoptate de CEPD (denumite în continuare „Orientările WP29 privind dreptul la portabilitatea datelor – aprobate de CEPD"), p. 9.

[26] A se vedea secțiunea 3.4 („Solicitări efectuate prin intermediul terților/ mandatarilor").

este adesea ocupat de o altă mașină. Întrucât această situație este repetitivă, pentru a identifica șoferul care neautorizat îi ocupă locul, persoana vizată solicită operatorului sistemului de supraveghere video care acoperă zona de parcare a biroului, accesul la datele cu caracter personal ale acestui șofer. 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 solicitantului, ci datele unei alte persoane – și, prin urmare, nu ar trebui să fie considerată o cerere conform art. 15 din RGPD.

c) Se aplică prevederi, altele decât RGPD, care reglementează accesul la o anumită categorie de date?

47. Persoanele vizate nu sunt obligate să precizeze temeiul legal în cererea lor. Cu toate acestea, în cazul în care persoanele vizate clarifică că cererea lor se bazează pe legislația sectorială sau pe legislația națională care reglementează problema specifică a accesului la anumite categorii de date, și nu pe RGPD, o astfel de cerere va fi examinată de operator în conformitate cu astfel de norme sectoriale sau naționale, după caz. Adesea, în funcție de legislația națională relevantă, operatorilor li se poate cere să furnizeze răspunsuri separate fiecare tratând cerințele specifice stabilite de diferitele acte legislative. Acest lucru nu trebuie confundat cu legislația națională sau legislația UE ce stabilesc 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 ce drept dorește să exercite persoana vizată, se recomandă să îi ceară solicitantului să explice obiectul solicitării. O astfel de corespondență cu persoana vizată nu afectează obligația operatorului de a acționa fără întârzieri nejustificate[27]. Cu toate acestea, în caz de îndoieli, dacă operatorul cere persoanei vizate explicații suplimentare și nu primește niciun răspuns, ținând cont de obligația de a facilita exercitarea dreptului de acces al persoanei, operatorul ar trebui să interpreteze informațiile conținute în prima cerere și să acționeze în bază acestora. În conformitate cu principiul responsabilității, operatorul poate stabili un interval de timp corespunzător în care persoana vizată poate oferi explicații suplimentare. Atunci când stabilește un astfel de interval de timp, operatorul ar trebui să lase suficient timp pentru a se conforma cererii după expirarea acesteia și, prin urmare, să ia în considerare cât timp este în mod obiectiv necesar pentru a compila și furniza datele solicitate odată ce specificația a fost furnizată (sau nu) de către persoana vizată.

49. Dacă cererea intră în sfera de aplicare a RGPD, existența unei astfel de legislații specifice nu prevalează asupra aplicării generale a dreptului de acces, astfel cum este prevăzut de RGPD. Pot exista restricții stabilite de legislația UE sau națională, atunci când este permis de art. 23 din RGPD (a se vedea secțiunea 6.4).

d) Cererea intră în sfera de aplicare a articolului 15?

50. Trebuie menționat că RGPD nu introduce nicio cerință formală pentru solicitanții accesului la date. Pentru a depune cererea de acces, este suficient ca solicitanții să precizeze că doresc să afle ce date cu caracter personal care le privesc prelucrează operatorul. Prin urmare, operatorul nu poate refuza furnizarea datelor prin referire la lipsa indicării temeiului legal al cererii, în special la lipsa unei referiri specifice la dreptul de acces sau la RGPD.

De exemplu, pentru a depune o cerere, ar fi suficient ca solicitantul să indice că:

- dorește să obțină acces la datele cu caracter personal care îl privesc;
- își exercită dreptul de acces; sau

[27] A se vedea orientările cu privire la termen în secțiunea 5.3.

- dorește să cunoască informațiile care îl privesc pe care operatorul le prelucrează.

Trebuie avut în vedere faptul că este posibil ca solicitanții să nu fie la curent cu complexitatea RGPD și, respectiv, se recomandă să se dea dovadă de indulgență față de persoanele care își exercită dreptul de acces, în special atunci când acesta este exercitat de minori. După cum s-a indicat mai sus, în cazul oricăror îndoieli, operatorului i se recomandă să ceară îi ceară solicitantului să precizeze obiectul solicitării.

e) Persoanele vizate doresc să acceseze toate informațiile sau o parte din informațiile prelucrate care le privesc?

51. În plus, operatorul trebuie să evalueze dacă cererile formulate de solicitanți se referă la toate informațiile sau la o parte din informațiile prelucrate care le privesc. Orice limitare a sferei de aplicare a unei cereri la o prevedere specifică a art. 15 din RGPD, realizată de persoanele vizate, trebuie să fie clară și neechivocă. De exemplu, în cazul în care persoanele vizate solicită verbatim „informații despre datele prelucrate care le privesc", operatorul ar trebui să presupună că persoanele vizate intenționează să își exercite integral dreptul în temeiul art. 15 alin. (1) și (2) din RGPD. O astfel de cerere nu trebuie interpretată în sensul că persoanele vizate doresc să primească numai categoriile de date cu caracter personal care sunt în curs de prelucrare și să renunțe la dreptul lor de a primi informațiile enumerate la art. 15 alin. (1) lit. a)-h). Acest lucru ar fi diferit, 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. În acest caz, operatorul își poate limita răspunsul la informațiile specifice solicitate.

3.1.2 Forma cererii

52. După cum s-a menționat anterior, RGPD nu impune nicio cerință persoanelor vizate cu privire la forma cererii de acces la date cu caracter personal. Prin urmare, în principiu, nu există cerințe în temeiul RGPD pe care persoanele vizate trebuie să le respecte atunci când aleg un canal de comunicare prin care intră în contact cu operatorul.

53. CEPD încurajează operatorii să ofere cele mai adecvate și mai ușor de utilizat canale de comunicare, în conformitate cu art. 12(2) și art. 25 din RGPD, pentru a permite persoanei vizate să depună o cerere eficientă. Cu toate acestea, dacă o persoană vizată depune o cerere utilizând un canal de comunicare furnizat de operator[28], care este diferit de cel indicat ca fiind cel preferat, o astfel de cerere va fi, în general, considerată eficientă și operatorul trebuie să gestioneze o astfel de cerere în mod corespunzător (a se vedea exemplele de mai jos). Operatorii ar trebui să depună toate eforturile rezonabile pentru a se asigura că exercitarea drepturilor persoanei vizate este facilitată (de exemplu, atunci când persoana vizată trimite o cerere de acces unui angajat aflat în concediu, un mesaj automat care informează persoana vizată despre un canal de comunicare alternativ pentru cererea dată ar putea fi un efort rezonabil).

54. Trebuie remarcat faptul că operatorul nu este obligat să acționeze la o cerere trimisă la o adresă de e-mail (sau poștală) aleatorie sau incorectă, nefurnizată direct de către operator, sau către orice canal de

[28] Acestea pot 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 politica de confidențialitate a operatorului sau în alte notificări legale obligatorii ale operatorului (de exemplu, informațiile de contact ale proprietarului sau ale companiei de pe un site web).

comunicare care în mod evident nu este destinat să primească cereri privind drepturile persoanei vizate dacă operatorul a furnizat un canal de comunicare adecvat, care poate fi utilizat de persoana vizată.

55. De asemenea, operatorul nu este obligat să acționeze la o cerere trimisă la adresa de e-mail a angajatului unui operator care poate să nu fie implicat în prelucrarea cererilor privind drepturile persoanelor vizate (de exemplu, șoferi, personal de curățenie etc.). Astfel de cereri nu vor fi considerate eficiente, dacă operatorul a furnizat în mod clar persoanei vizate un canal de comunicare corespunzător. Cu toate acestea, dacă persoana vizată trimite o cerere angajatului operatorului care i-a fost desemnat ca persoană de contact (cum ar fi, de exemplu, un manager de cont personal la o bancă sau un consultant la un operator de telefonie mobilă), acest contact nu ar trebui să fie considerat unul aleatoriu, iar operatorul ar trebui să depună toate eforturile rezonabile pentru a gestiona o astfel de cerere, astfel încât aceasta să poată fi redirecționată către punctul de contact și să i se răspundă în termenele prevăzute de RGPD.

56. Cu toate acestea, CEPD recomandă, ca bună practică, ca operatorii să introducă mecanisme corespunzătoare pentru a facilita exercitarea drepturilor persoanelor vizate, inclusiv sisteme cu răspuns automat pentru a informa despre absențe ale personalului și contact alternativ adecvat și, acolo unde este posibil, mecanisme pentru a îmbunătăți comunicarea internă între angajații cu privire la cererile primite de cei care ar putea să nu fie competenți să gestioneze astfel de cereri.

Exemplul 8: Operatorul X furnizează, atât pe site-ul său web, cât și în notificarea de confidențialitate, două adrese de e-mail – adresa generală de e-mail 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 web că, pentru a trimite orice întrebări sau pentru a depune o cerere cu privire la prelucrarea datelor cu caracter personal, persoanele fizice trebuie 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 generală de e-mail a operatorului: CONTACT@X.COM.

Într-un astfel de caz, operatorul trebuie să depună toate eforturile rezonabile pentru a-și informa serviciile cu privire la cerere care a fost depusă prin e-mailul general, astfel încât să poată fi redirecționată către punctul de contact pentru protecția datelor și să i se răspundă în termenele limită prevăzute de RGPD. În plus, operatorul nu are dreptul să prelungească perioada de răspuns la o cerere, doar pentru 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 conduce o rețea de cluburi de fitness. Operatorul Y indică pe site-ul său web și în avizul de confidențialitate pentru clienții clubului de fitness că pentru a trimite orice întrebări sau pentru a depune o cerere cu privire la prelucrarea datelor cu caracter personal, persoanele fizice trebuie 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 găsită în vestiar, unde a găsit o notificare pe care scrie „Dacă nu sunteți mulțumit de curățenia camerei, vă rugăm să ne contactați la: CLEANERS@Y.COM, care este adresa de e-mail a personalului responsabil de curățenie angajat de Y. Personalul responsabil de curățenie, evident, nu este implicat în gestionarea problemelor privind exercitarea drepturilor persoanelor vizate – clienți ai 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 solicitări, deoarece site-ul web și notificarea de confidențialitate informau în mod clar despre canalul de comunicare care trebuia utilizat pentru exercitarea drepturilor persoanelor vizate.

57. Data primirii cererii de către operator declanșează, de regulă, termenul de o lună pentru ca operatorul să furnizeze informații cu privire la acțiunile întreprinse în urma unei cereri, în conformitate cu art. 12(3) din RGPD (îndrumări suplimentare privind calendarul sunt oferite în secțiunea 5.3). CEPD consideră o practică bună pentru operatori să confirme primirea cererilor în scris, de exemplu prin trimiterea de e-mailuri (sau informații prin poștă, dacă este cazul) către solicitanți, care să confirme că cererile lor au fost primite și că perioada de o lună se desfășoară din ziua X până în ziua Y.

3.2 Identificarea și autentificarea

58. Pentru a asigura securitatea prelucrării și a minimiza riscul dezvăluirii neautorizate a datelor cu caracter personal, operatorul trebuie să poată afla ce date privesc persoana vizată (identificare) și să confirme identitatea acelei persoane (autentificare).

59. Se poate reaminti faptul că, în situațiile în care scopul pentru care datele cu caracter personal sunt prelucrate nu necesită sau nu mai necesită identificarea unei persoane vizate, operatorul nu are nevoie să mențină identificarea în scopul exclusiv de a se conforma drepturilor persoanelor vizate, de asemenea, în lumina principiului minimizării datelor. Aceste situații sunt abordate în art. 11(1) din RGPD.

60. Articolul 12(2) din RGPD prevede că operatorul nu va refuza să acționeze la cererea 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. În astfel de circumstanțe, persoana vizată poate decide, totuși, să furnizeze informații suplimentare care să permită această identificare [art. 11(2) din RGPD][29].

61. Operatorul nu este obligat să obțină astfel de informații suplimentare pentru a identifica persoana vizată în scopul unic de a se conforma cererii persoanei vizate, inclusiv în lumina principiului minimizării datelor. Cu toate acestea, nu ar trebui să refuze să preia astfel de informații suplimentare furnizate de persoana vizată pentru a sprijini exercitarea drepturilor sale (considerentul 57 din RGPD).

Exemplul 10: X este operatorul datelor prelucrate în legătură cu supravegherea video a unei clădiri. În conformitate cu art. 11(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 date cu caracter personal de la persoana care susține că a fost înregistrată de supravegherea video a operatorului. Acțiunile operatorului vor depinde de informațiile suplimentare furnizate. În cazul în care solicitantul indică o anumită zi și oră în care camerele ar fi putut înregistra evenimentul în cauză, este probabil ca operatorul să poată furniza astfel de date [art. 11(2) din RGPD]. Cu toate acestea, dacă operatorul nu este în măsură să identifice persoana vizată (de exemplu, dacă este imposibil pentru operator să fie sigur că persoana vizată este de fapt persoana vizată sau dacă cererea se referă, de exemplu, la o perioadă lungă de înregistrări și operatorul nu este în măsură să prelucreze o cantitate atât de mare de date), operatorul poate refuza să ia măsuri dacă demonstrează că nu este în măsură să identifice persoana vizată [art. 12(2) din RGPD].

Exemplul 11: Un operator C prelucrează date cu caracter personal în scopul de a furniza publicitate comportamentală utilizatorilor săi web. Datele cu caracter personal colectate pentru publicitatea comportamentală sunt de obicei colectate prin intermediul cookie-urilor și asociate cu identificatori aliatori pseudonimi. O persoană vizată, domnul X, își exercită dreptul de acces cu C prin intermediul

[29] Orientările WP29 privind dreptul la portabilitatea datelor - aprobate de CEPD, p. 13.

site-ului web al C. C poate să îl identifice cu exactitate pe domnul X pentru a arăta publicitatea comportamentală a persoanei vizate, conectând echipamentul terminal al domnului X la profilul său de publicitate cu cookie-urile introduse în terminal. C ar trebui, de asemenea, să îl poată identifica cu exactitate pe domnul X pentru a-i acorda acces la datele sale cu caracter personal, deoarece poate fi găsită o legătură între datele prelucrate și persoana vizată. Prin urmare, și ținând cont de principiile RGPD, exemplul de mai sus nu ar intra în sfera de aplicare a art. 11 din RGPD. Mai precis, în exemplul de mai sus, scopurile C impun identificarea persoanelor vizate în timp ce art. 11 din RGPD abordează situația prelucrării care nu necesită identificare atunci când operatorul nu este obligat să prelucreze date suplimentare în sensul art. 11(1) din RGPD cu unicul scop de a putea să se conformeze RGPD. În consecință, în unele cazuri, nu ar trebui solicitate date suplimentare pentru a exercita drepturile persoanei vizate.

Totuși, dacă domnul X încearcă să își exercite dreptul de acces prin e-mail sau prin poștă obișnuită, atunci, în acest context, C nu va avea altă opțiune decât să îi ceară domnului X să furnizeze „informații suplimentare" [art. 12(6) din RGPD] pentru a putea identifica profilul publicitar asociat domnului X. În acest caz, informațiile suplimentare vor fi identificatorul cookie stocat în echipamentul terminal al domnului X.

62. În cazul imposibilității demonstrate de identificare a persoanei vizate (art. 11 din RGPD), operatorul trebuie să informeze persoana vizată în mod corespunzător, dacă este posibil, deoarece operatorul răspunde la cererile persoanei vizate fără întârzieri nejustificate și oferă motive atunci când nu intenționează să se conformeze unei astfel de cereri. Aceste informații trebuie furnizate doar „dacă este posibil", deoarece operatorul poate să nu fie în măsură să informeze persoanele vizate dacă identificarea lor este imposibilă.

63. Atât în cazul în care prelucrarea nu necesită identificare, cât și în cazul în care este nevoie de identificare, dacă operatorul are îndoieli rezonabile cu privire la identitatea solicitantului, operatorul poate cere furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate [art. 12(6) din RGPD].

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

65. Trebuie reamintit că, de regulă, operatorul nu poate solicita mai multe date cu caracter personal decât este necesar pentru a permite autentificarea dată și că utilizarea acestor informații ar trebui să se limiteze strict la îndeplinirea cererii persoanelor vizate.

66. Între persoanele vizate și operatori adesea sunt deja stabilite proceduri de autentificare. Operatorii pot utiliza aceste proceduri de autentificare pentru a constata identitatea persoanelor vizate care solicită datele cu caracter personal sau își exercită drepturile acordate de RGPD[30]. În caz contrar, operatorii ar trebui să implementeze o procedură de autentificare pentru a face acest lucru[31].

67. În cazurile în care operatorul solicită sau i se furnizează de către persoana vizată informații suplimentare necesare pentru a confirma identitatea persoanei vizate, operatorul trebuie, de fiecare dată, să evalueze ce informații îi vor permite să confirme identitatea persoanei vizate și, eventual, să adreseze

[30] Orientările WP29 privind dreptul la portabilitatea datelor - aprobate de CEPD, p. 14.

[31] A se vedea îndrumări suplimentare privind autentificarea în secțiunea 3.3.

întrebări suplimentare solicitantului sau să ceară persoanei vizate să prezinte unele elemente suplimentare de identificare, dacă 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 solicitate inițial pentru autentificarea persoanei vizate. În general, faptul că operatorul poate cere informații suplimentare pentru a evalua identitatea persoanei vizate nu poate conduce la cereri excesive și la colectarea de date cu caracter personal care nu sunt relevante sau necesare pentru a consolida legătura dintre persoana fizică și datele cu caracter personal solicitate.[32]

69. În consecință, în cazul în care informațiile colectate online sunt legate de pseudonime sau de alți identificatori unici, operatorul poate implementa proceduri corespunzătoare care să îi permită solicitantului să depună o cerere de acces la date și să primească datele ce îl privesc[33].

Exemplul 12: Persoana vizată, doamna X, cere accesul la datele sale în timp ce vorbește cu un consultant telefonic al unei companii de energie electrică cu care a încheiat un contract. Consultantul, având îndoieli cu privire la identitatea solicitantului, generează în sistemul companiei un cod unic de folosință trimis la numărul de telefon mobil al utilizatorului, furnizat la crearea contului, ca parte a sistemului de dublă verificare, acțiune care ar trebui considerată proporțională în acest caz.

3.3 Evaluarea proporționalității în ceea ce privește autentificarea solicitantului

70. După cum s-a indicat mai sus, dacă operatorul are motive întemeiate să se îndoiască de identitatea solicitantului, acesta poate cere informații suplimentare pentru a confirma identitatea persoanei vizate. Totuși, operatorul trebuie să se asigure în același timp că nu colectează mai multe date cu caracter personal decât este necesar pentru a permite autentificarea solicitantului. Prin urmare, operatorul va efectua o evaluare a proporționalității, care trebuie să țină cont de tipul de date cu caracter personal care sunt prelucrate (de exemplu, categorii speciale de date sau nu), natura cererii, contextul în care se depune cererea, precum și orice daune care ar putea rezulta din dezvăluirea necorespunzătoare. Atunci când se evaluează proporționalitatea, trebuie reținut să se evite colectarea excesivă a datelor asigurând în același timp un nivel corespunzător de securitate a prelucrării.

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

[32] Ibid, p. 14.

[33] Ibid, p. 13 – 14.

[34] Orientările WP29 privind dreptul la portabilitatea datelor - aprobate de CEPD, p. 14.

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

73. În practică, procedurile de autentificare sunt deja stabilite, 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 de socializare sau magazine online), operatorii cel mai probabil solicită înregistrarea prin login-ul și parola utilizatorului, care în astfel de cazuri ar trebui să fie suficiente pentru a autentifica persoana vizată[36]. În plus, persoanele vizate sunt adesea deja autentificate de către operator înainte de a încheia un contract sau de a li se colecta consimțământul pentru prelucrare și, în consecință, datele cu caracter personal utilizate pentru înregistrarea persoanei fizice la care se referă prelucrarea pot fi, de asemenea, utilizate ca dovezi pentru autentificarea persoanei vizate în scopuri de acces.[37] În consecință, este disproporționat să se ceară o copie a unui act de identitate în cazul în care persoana vizată care depune o cerere este deja autentificată de către operator.

74. Ar trebui subliniat faptul că utilizarea unei copii a unui document de identitate ca parte a procesului de autentificare generează riscuri pentru securitatea datelor cu caracter personal și poate duce la o prelucrare neautorizată sau ilegală și, ca atare, ar trebui considerată inadecvată, cu excepția cazului în care este necesar, adecvat și în conformitate cu legislația națională. În astfel de cazuri, operatorii ar trebui să dispună de sisteme care să asigure un nivel de securitate corespunzător pentru a atenua riscurile mai mari pentru drepturile și libertățile persoanei vizate de a primi astfel de date. De asemenea, este important de reținut că autentificarea prin intermediul unui act de identitate nu ajută neapărat în contextul online (de exemplu, cu utilizarea pseudonimelor) dacă persoana în cauză nu poate contribui cu alte dovezi, de ex. alte caracteristici care se potrivesc cu contul de utilizator.

75. Ținând cont de faptul că multe organizații (de exemplu, hoteluri, bănci, închirieri auto) solicită copii ale actului de identitate ale clienților lor, în general, aceasta nu ar trebui să fie considerată o modalitate adecvată de autentificare. În mod alternativ, operatorul poate implementa o măsură de securitate rapidă și eficientă pentru a identifica persoana vizată pe baza autentificării pe care a efectuat-o anterior, de ex. prin e-mail sau mesaj text care conține link-uri de confirmare, întrebări de securitate sau coduri de confirmare[38].

76. Informații despre actul de identitate care nu sunt necesare pentru confirmarea identității persoanei vizate, cum ar fi numărul de acces și de serie, naționalitatea, înălțimea, culoarea ochilor, fotografia și zona de citire automată, în funcție de evaluarea de la caz la caz, pot fi redactate sau ascunse de persoana vizată înainte de a le transmite operatorului, cu excepția cazului în care legislația națională cere o copie completă neredactată a actului de identitate (a se vedea punctul 78 de mai jos). În general, data emiterii sau data expirării, autoritatea emitentă și numele complet care se potrivesc cu contul

[35] A se vedea îndrumări 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 virtuali vocali, Versiunea 2.0, Adoptată la 7 iulie 2021, secțiunea 3.7.

[36] Orientările WP29 privind dreptul la portabilitatea datelor - aprobate de CEPD, p. 14.

[37] Orientările WP29 privind dreptul la portabilitatea datelor - aprobate de CEPD, p. 14.

[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 creat diferite servicii care permite identificarea securizată de la distanță.

online sunt suficiente pentru ca operatorul să verifice identitatea, întotdeauna cu condiția ca să fie asigurată autenticitatea copiei și relația cu solicitantul. Informații suplimentare, cum ar fi data nașterii persoanei vizate, pot fi solicitate numai în cazul în care riscul de identitate greșită persistă, dacă operatorul este capabil să le compare cu informațiile pe care le prelucrează deja.

77. Pentru a urma principiul minimizării datelor, operatorul ar trebui să informeze persoana vizată despre informațiile care nu sunt necesare și despre posibilitatea de a redacta sau ascunde acele părți ale documentului de identitate. Într-un astfel de caz, dacă persoana vizată nu știe cum sau nu este în măsură să redacteze astfel de informații, este o bună practică ca operatorul să le redacteze la primirea documentului, dacă acest lucru este posibil pentru operator ținând cont de mijloacele disponibile operatorului în circumstanțele date.

Exemplul 13: Utilizatorul doamna Y și-a creat un cont protejat cu parolă în magazinul online furnizând adresa de e-mail și/sau numele de utilizator. Ulterior, titularul contului solicită operatorului informații dacă prelucrează datele cu caracter personal ale acestuia și, în caz afirmativ, cere accesul la acestea în sfera indicată la art. 15. Operatorul cere actul de identitate al solicitantului pentru a-i confirma identitatea. Acțiunea operatorului în acest caz este disproporționată și duce la colectarea inutilă de date.

Cu toate acestea, pentru a confirma identitatea solicitantului, prevenind în același timp colectarea inutilă de date, operatorul i-ar putea cere acestuia să se autentifice prin logare la cont sau să-i pună întrebări de securitate (neintruzive), răspunsul la care numai persoana vizată ar trebui să-l cunoască, sau să folosească autentificarea multifactorială care a fost configurată atunci când persoana vizată și-a înregistrat contul sau să folosească alte mijloace de comunicare existente cunoscute ca 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 unei bănci, domnul Y, planifică să obțină un credit de consum. În acest scop, domnul Y vizitează o sucursală bancară pentru a obține informații, inclusiv datele sale cu caracter personal, necesare pentru evaluarea bonității sale. Pentru verificarea identității persoanei vizate, consultantul cere o certificare legalizată a identității sale pentru a-i putea furniza informațiile solicitate.

Operatorul nu ar trebui să ceară confirmarea legalizată a identității, cu excepția cazului în care este necesar, adecvat și în conformitate cu legislația națională (de exemplu, în cazul în care o persoană nu deține temporar niciun act de identitate și dovada identității persoanei vizate este cerută de către legislația națională pentru efectuarea unui act juridic). O astfel de practică expune solicitanții la costuri suplimentare și impune o povară excesivă pe umerii 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 act 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 prelucrări de date care pot prezenta un risc pentru persoana vizată (de exemplu, informații medicale sau de sănătate). Totuși, în același timp, trebuie avut în vedere faptul că anumite prevederi naționale prevăd restricții privind prelucrarea datelor conținute în documentele publice, inclusiv documentele care confirmă identitatea unei persoane (de asemenea în baza art. 87 din RGPD). Restricțiile privind prelucrarea datelor din

aceste documente se pot referi în special la scanarea sau fotocopierea actelor de identitate sau la prelucrarea numerelor oficiale de identificare personală[39].

79. Ținând cont de cele de mai sus, în cazul în care se solicită un act de identitate (și acest lucru este atât în conformitate cu legislația națională, cât și justificat și proporțional în temeiul RGPD), operatorul trebuie să pună în aplicare măsuri de protecție pentru a preveni prelucrarea ilegală a actului de identitate. Fără a aduce atingere oricăror prevederi naționale aplicabile privind autentificarea actului de identitate, aceasta poate include abținerea de la a face o copie sau ștergerea unei copii a unui act de identitate imediat după autentificarea cu succes a identității persoanei vizate. Acest lucru se datorează faptului că stocarea ulterioară a unei copii a unui act de identitate poate echivala cu o încălcare a principiilor limitării scopului și limitării stocării [art. 5(1)(b) și (e) RGPD] și, în plus, a legislației naționale privind prelucrarea numărului național de identificare (art. 87 din RGPD). CEPD recomandă, ca bună practică, ca operatorul, după verificarea actului de identitate, să noteze de ex. „Actul de identitate a fost verificat" pentru a evita copierea sau stocarea inutilă a copiilor actelor de identitate.

3.4 Cererile depuse prin terțe părți/mandatari

80. Deși dreptul de acces este exercitat în general de persoanele vizate în măsura în care le vizează, este posibil ca o terță parte să depună o cerere în numele persoanei vizate. Acest lucru se poate aplica, printre altele, acționării prin intermediul unui mandatar sau a tutorilor legali în numele minorilor, precum și acționării prin alte entități prin intermediul portalurilor online. În anumite circumstanțe, identitatea persoanei autorizate să-și exercite dreptul de acces, precum și autorizarea de a acționa în numele persoanei vizate poate necesita verificare, atunci când aceasta este adecvată și proporțională (a se vedea secțiunea 3.3 de mai sus)[40]. Trebuie reamintit că punerea datelor cu caracter personal la dispoziția unei persoane care nu are dreptul să le acceseze poate echivala cu o încălcare a datelor cu caracter personal[41].

81. În acest sens, ar trebui luate în considerare legile naționale care reglementează reprezentarea juridică (de exemplu, procuri), care pot impune cerințe specifice pentru demonstrarea autorizației de a depune o cerere în numele persoanei vizate, deoarece RGPD nu reglementează acest lucru. În conformitate cu principiul responsabilității, precum și cu celelalte principii de protecție a datelor, operatorii trebuie să poată demonstra existența autorizației relevante de a depune o cerere în numele persoanei vizate și de a primi informațiile solicitate, cu excepția cazului în care: legislația națională diferă (de exemplu, legislația națională conține reguli specifice cu privire la credibilitatea avocaților), lăsând operatorul să verifice identitatea mandatarului (de exemplu, în cazul avocaților care verifică înscrierea la barou). Prin urmare, se recomandă colectarea documentației corespunzătoare în acest sens, în raport cu regulile generale indicate anterior privind confirmarea identității unei persoane fizice care depune o cerere și, dacă operatorul are îndoieli rezonabile cu privire la identitatea unei persoane care acționează în numele persoanei vizate, va cere informații suplimentare pentru a confirma identitatea acestei persoane.

82. În timp ce exercitarea dreptului de acces la datele cu caracter personal ale persoanelor decedate echivalează cu un alt exemplu de acces al unei terțe părți, alta decât persoana vizată, considerentul 27 precizează că RGPD nu se aplică datelor cu caracter personal ale persoanelor decedate. Prin urmare,

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

[40] În ceea ce privește termenele de exercitare a dreptului de acces atunci când operatorul are nevoie să obțină informații suplimentare, a se vedea alin. 157.

[41] Articolul 4(12) din RGPD.

chestiunea este tratată de legislația națională, iar statele membre pot prevedea norme privind prelucrarea datelor cu caracter personal ale persoanelor decedate. Cu toate acestea, trebuie luat în considerare faptul că datele se pot referi, în plus, la terți în viață, de ex. în contextul accesului solicitat la corespondența unei persoane decedate. Confidențialitatea acestor date trebuie încă protejată.

3.4.1 Exercitarea dreptului de acces în numele copiilor

83. Copiii merită protecție specifică în ceea ce privește datele lor cu caracter personal, deoarece pot fi mai puțin conștienți de riscurile, consecințele și garanțiile privind drepturile lor în legătură cu prelucrarea datelor cu caracter personal[42]. Orice informație și comunicare către un copil, în care sunt prelucrate datele cu caracter personal ale unui copil, ar trebui să fie într-un limbaj clar și simplu, astfel încât copilul să poată înțelege cu ușurință[43].

84. Copiii sunt și ei persoane vizate și, ca atare, dreptul de acces îi aparține copilului. În funcție de maturitatea și capacitatea copilului, acesta poate avea nevoie de o terță parte care să acționeze în numele său, de ex. titularul răspunderii părintești.

85. Interesul superior al copilului ar trebui să fie un aspect important în toate deciziile luate cu privire la exercitarea dreptului de acces atunci când este vorba de copii, în special atunci când dreptul de acces este exercitat în numele copilului, de exemplu, de către titularul autorității părintești.

86. Datorită protecției speciale a datelor cu caracter personal ale copiilor cuprinse în RGPD, operatorul va lua măsurile corespunzătoare pentru a evita orice dezvăluire a datelor cu caracter personal ale unui minor către o persoană neautorizată (în acest sens, a se vedea și secțiunea 3.4 de mai sus).

87. În cele din urmă, dreptul titularului răspunderii părintești de a acționa în numele copilului nu trebuie 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 ce privesc copilul (de exemplu, performanța copilului la școală).

3.4.2 Exercitarea dreptului de acces prin portaluri/canale furnizate de o terță parte

88. Există companii care furnizează servicii care permit persoanelor vizate să depună cereri de acces prin intermediul unui portal. Persoana vizată se conectează și obține acces la un portal prin care poate trimite, de exemplu, o cerere de acces, poate solicita rectificarea sau ștergerea datelor de la diferiți operatori. Diferite întrebări apar din utilizarea portalurilor furnizate de o terță parte.

89. Prima problemă pe care trebuie să o rezolve operatorii atunci când se confruntă cu astfel de circumstanțe este să se asigure că terța parte acționează în mod legitim în numele persoanei vizate, deoarece este necesar să se asigure că niciun fel de date nu sunt dezvăluite unor părți neautorizate.

90. În plus, un operator care primește o cerere depusă printr-un astfel de portal trebuie, în mod invariabil, să gestioneze acea cerere în timp util[44]. Cu toate acestea, nu există nicio obligație pentru operator de a

[42] Considerentul 38 din RGPD. După cum se prevede în programul de lucru al CEPD, intenția sa este de a oferi îndrumări cu privire la datele despre copii. Se așteaptă ca un astfel de document să ofere mai multe îndrumări cu privire la condițiile în care un copil își poate exercita dreptul de acces, iar titularul răspunderii părintești poate exercita dreptul de acces în numele copilului.

[43] Considerentul 58 din RGPD. Orientările CEPD 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, secțiunea 7.

[44] În ceea ce privește termenele de exercitare a dreptului de acces atunci când operatorul are nevoie să obțină informații suplimentare, a se vedea alin. 157

furniza datele conform art. 15 din RGPD direct către portal, în cazul în care operatorul, de exemplu, stabilește că măsurile de securitate sunt insuficiente sau s-ar considera oportun să se folosească o altă modalitate de dezvăluire a datelor către persoana vizată. În astfel de circumstanțe, atunci când operatorul are alte proceduri în vigoare pentru a gestiona cererile de acces într-un mod eficient și sigur, operatorul poate furniza informațiile solicitate prin aceste proceduri.

4 SFERA DE APLICARE A DREPTULUI DE ACCES ȘI A DATELOR ȘI INFORMAȚIILOR CU CARACTER PERSONAL LA CARE SE REFERĂ

91. Prezenta secțiune urmărește să pună în lumină definiția datelor cu caracter personal (4.1) și să clarifice sfera de aplicare a informațiilor acoperite de dreptul de acces în general (4.2 și 4.3). De remarcat este faptul că sfera de aplicare a conceptului de date cu caracter personal și, prin urmare, diferențierea între datele cu caracter personal și alte date, este o parte integrantă a evaluării efectuate de operator pentru a identifica sfera de aplicare a datelor la care persoana vizată are dreptul să obțină acces[45].

92. Ca titlu preliminar, trebuie reamintit că dreptul de acces poate fi exercitat numai cu privire la prelucrarea datelor cu caracter personal care intră în sfera de aplicare materială și teritorială a RGPD. Prin urmare, datele cu caracter personal care nu sunt prelucrate prin mijloace automate sau care nu fac parte sau nu intenționează să devină parte a unui sistem de evidență conform art. 2(1) din RGPD sau prelucrate de o persoană fizică în cadrul unei activități pur personale sau casnice conform art. 2(2) din RGPD, nu sunt acoperite de dreptul de acces.

4.1 Definiția datelor cu caracter personal

93. Articolul 15(1) și (3) din RGPD se referă la „date cu caracter personal", respectiv „date cu caracter personal în curs de prelucrare". Prin urmare, sfera dreptului de acces este determinată în primul rând de sfera de aplicare a conceptului de date cu caracter personal, definit la art. 4(1) din RGPD[46]. Conceptul de date cu caracter personal a făcut deja obiectul mai multor articole din cadrul documentelor[47] Grupului de lucru Art. 29[48] și a fost interpretat de CJUE, inclusiv în contextul dreptului de acces în temeiul art. 12 din Directiva 95/46/CE.

[45] În conformitate cu principiul confidențialității până la concepție, o astfel de analiză face parte din evaluarea măsurilor și garanțiilor corespunzătoare pentru protejarea principiilor de protecție a datelor și a drepturilor persoanelor vizate, care se efectuează *„la momentul determinării mijloacelor de prelucrare și la timpul prelucrării în sine"*, de ex. reducerea timpului de răspuns atunci când persoanele vizate își exercită drepturile poate fi una dintre metrici. Pentru explicații suplimentare, a se vedea Orientările 4/2019 privind Articolul 25 Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit.

[46] Conform art. 4(1) din RGPD, «„date cu caracter personal" înseamnă orice informație referitoare la o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este acea persoană care poate fi identificată, direct sau indirect, în special prin referire la un identificator cum ar fi un nume, un număr de identificare, date de localizare, un identificator online sau la unul sau mai mulți factori specifici persoanei fizice din punct de vedere fizic, fiziologic, al identității genetice, mental, economic, cultural sau social»

[47] Grupul de lucru Art. 29 (WP Art. 29) este grupul de lucru european independent care s-a ocupat de problemele legate de protecția vieții private și a datelor cu caracter personal până la 25 mai 2018 (intrarea în aplicare a RGPD), predecesorul CEPD.

[48] De ex. Orientările WP251 rev01 privind procesul decizional individual automatizat și crearea de profiluri în scopurile stabilite de Regulamentul 2016/679, adică p. 19; Orientările WP29 privind dreptul la portabilitatea datelor - aprobate de CEPD, p. 9.

94. WP29 a considerat că definiția datelor cu caracter personal din Directiva 95/46/CE «reflectă intenția legiuitorului european pentru o noțiune largă de „date cu caracter personal”»[49]. Conform RGPD, definiția se referă în continuare la „orice informații ce privesc o persoană fizică identificată sau identificabilă”. În afară de datele cu caracter personal de bază, cum ar fi numele și adresa, numărul de telefon etc., o varietate nelimitată de date pot fi acoperite de această definiție, inclusiv constatări medicale, istoricul achizițiilor, indicatorii de bonitate, conținutul unei comunicări etc. Având în vedere sfera de aplicare largă a definiției datelor cu caracter personal, o evaluare restrictivă a acestei definiții de către operator ar duce la o clasificare eronată a datelor cu caracter personal[50] și, în cele din urmă, la o încălcare a dreptului de acces.

95. În cauzele conexe C-141/12 și C-372/12,[51] CJUE a hotărât că dreptul de acces acoperă datele cu caracter personal conținute în procese-verbale, și anume *„numele, data nașterii, naționalitatea, sexul, etnia, religia și limba solicitantului” «și, „dacă este cazul, datele din analiza juridică” cuprinse în procesul-verbal»,* dar nu și analiza juridică în sine[52]. Analiza juridică nu era, în acest context, responsabilă în sine să facă obiectul unei verificări a exactității acesteia de către persoana vizată și nici al rectificării. În plus, oferirea accesului la analiza juridică nu îndeplinește scopul de a garanta confidențialitatea, 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 orice comentarii ale unui examinator cu privire la aceste răspunsuri constituie date cu caracter personal privind candidatul la examen. Mai precis, astfel de informații subiective sunt date cu caracter personal *«sub formă de opinii și evaluări, cu condiția că „se referă” la persoana vizată»*[54] spre deosebire de întrebările de examen, care nu sunt considerate date cu caracter personal[55]. Astfel, o evaluare contextuală ar trebui să pună în lumină efectul sau rezultatul pe care o informație îl poate avea asupra unei persoane fizice și, prin urmare, asupra sferei de aplicare a dreptului de acces.

Exemplul 15: O persoană are un interviu de angajare cu o companie. În acest context, solicitantul depune un CV și o scrisoare de intenție. În timpul interviului, responsabilul de resurse umane ia notițe pe computer pentru a documenta interviul. Ulterior, solicitantul, în calitate de persoană vizată, solicită accesul la datele cu caracter personal care îl privesc pe care compania, în calitate de operator, le-a colectat în cursul procedurii de recrutare.

Operatorul este obligat să furnizeze persoanei vizate datele cu caracter personal comunicate activ de către aceasta în CV-ul și scrisoarea de intenție. În plus, operatorul trebuie să furnizeze persoanei vizate rezumatul interviului, inclusiv comentariile subiective cu privire la comportamentul persoanei vizate pe care responsabilul de resurse umane le-a scris în timpul interviului de angajare, sub rezerva oricăror derogări în temeiul legislației naționale și în conformitate cu art. 23 din RGPD.

[49] Avizul WP29 4/2007 privind conceptul de date cu caracter personal, p. 4.
[50] informații care nu au legătură cu o persoană fizică identificată sau identificabilă.
[51] CJUE, Cauzele conexe C-141/12 și C-372/12, YS v Minister voor Immigratie, Integratie en Asiel și Minister voor Immigratie, Integratie en Asiel v M și S, 17 iulie 2014.
[52] CJUE, Cauzele conexe C-141/12 și C-372/12, YS și Alții, para. 38 și 48.
[53] CJUE, C-434/16, Peter Nowak v Data Comisarul pentru protecția datelor, 20 decembrie 2017.
[54] CJUE, C 434/16, Nowak, alin. 34-35.
[55] CJUE, C-434/16, Nowak, alin. 58.

97. Astfel, sub rezerva faptelor specifice ale cauzei, la evaluarea unei cereri specifice de acces, următoarele tipuri de date urmează, printre altele, să fie furnizate de către operatori fără a aduce atingere art. 15(4) din RGPD:

- Categorii speciale de date cu caracter personal conform art. 9 din RGPD;
- Date cu caracter personal referitoare la condamnări penale și infracțiuni conform art. 10 din RGPD;
- Date furnizate în mod conștient și activ de către persoana vizată (de exemplu, datele contului transmise prin formulare, răspunsuri la un chestionar)[56];
- Date observate sau date brute furnizate de persoana vizată în virtutea utilizării serviciului sau a dispozitivului (de exemplu, date prelucrate de obiectele conectate, istoricul tranzacțiilor, jurnalele de activitate, cum ar fi jurnalele de acces, istoricul utilizării site-ului web, activitățile de căutare, datele despre locație), activitate de clic, aspecte unice ale comportamentului unei persoane, cum ar fi scrierea de mână, apăsarea tastelor, un anumit mod de a merge sau de a vorbi[57];
- Date derivate din alte date, în loc de cele furnizate direct de persoana vizată (de exemplu, raportul de credit, clasificarea bazată pe atributele comune ale persoanelor vizate, țara de reședință derivată din codul poștal)[58];
- Date deduse din alte date, și nu cele furnizate direct de persoana vizată (de exemplu, pentru a atribui un scor de credit sau pentru a respecta regulile împotriva spălării banilor, rezultate algoritmice, rezultatele unei evaluări de sănătate sau a unui proces de personalizare sau recomandare)[59];
- Date pseudonimizate, spre deosebire de datele anonimizate (a se vedea, de asemenea, secțiunea 3 a prezentului ghid).

Exemplul 16: Elementele care au fost utilizate pentru a lua o decizie cu privire, de exemplu, la promovarea angajatului, creșterea salariului sau atribuirea unui nou loc de muncă (de exemplu, analize anuale de performanță, cereri de formare, dosare disciplinare, clasament, potențial de carieră) sunt date cu caracter personal care privesc acel angajat. Astfel, asemenea elemente pot fi accesate de către persoana vizată la cerere și cu respectarea art. 15(4) din RGPD, în cazul în care datele cu caracter personal, de exemplu, se referă și la o altă persoană fizică [de exemplu, identitatea sau elementele care dezvăluie identitatea unui alt angajat a cărui mărturie despre performanța profesională este inclusă într-o evaluare anuală a performanței pot face obiectul limitărilor în temeiul art. 15(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 naționale ale legislației muncii se pot aplica, de exemplu, cu privire la accesul angajaților la dosarele de personal sau alte prevederi naționale precum cele referitoare la secretul profesional. În toate circumstanțele, astfel de restricții privind exercitarea dreptului de acces al persoanei vizate (sau a altor drepturi) prevăzute într-o lege națională trebuie să respecte condițiile art. 23 din RGPD (a se vedea secțiunea 6.4).

[56] Orientările WP29 privind dreptul la portabilitatea datelor – aprobate de CEPD, p. 9.

[57] Avizul WP29 4/2007 privind conceptul de date cu caracter personal, p. 8

[58]Orientările WP29 privind dreptul la portabilitatea datelor – aprobate de CEPD, p. 10 – 11

[59] Orientările WP29 privind dreptul la portabilitatea datelor – aprobate de CEPD, p. 10 – 11; , Orientările Grupului de lucru Art. 29, WP 251 rev.01, 6 februarie 2018 privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului 2016/679 – aprobate de CEPD (în continuare „Orientările WP29 privind procesul decizional individual individualizat și crearea de profiluri – aprobate de CEPD"), p. 9 – 10.

98. Din lista neexhaustivă de mai sus de date cu caracter personal care pot fi furnizate persoanei vizate pot fi extrase mai multe considerații în contextul unei cereri de acces. Din cele de mai sus reiese că operatorul nu poate face distincție atunci când oferă acces la date cu caracter personal între datele conținute în fișiere pe suport de hârtie și cele stocate electronic, atât timp cât acestea intră în sfera de aplicare a RGPD. Cu alte cuvinte, datele cu caracter personal care sunt conținute în fișiere pe suport de hârtie ca parte a unui sistem de arhivare sau care sunt destinate să facă parte dintr-un sistem de arhivare sunt acoperite de dreptul de acces în același mod ca datele cu caracter personal stocate într-o memorie de computer prin intermediul, de exemplu, al codului binar sau al casetei video.

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 doar 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 face o analiză sau o evaluare ulterioară a acestor date, ci și rezultatul oricărei astfel de analize sau evaluări ulterioare.

100. De asemenea, este important de reamintit că există informații, cum ar fi datele anonime[61], care sunt date care nu privesc direct sau indirect o persoană identificabilă și care sunt, prin urmare, excluse din sfera de aplicare a RGPD. De exemplu, locația serverului pe care datele cu caracter personal ale persoanei vizate sunt prelucrate nu sunt date cu caracter personal. Distincția poate fi o provocare, iar operatorii se pot întreba cum să tragă o linie clară între datele cu caracter personal și cele cu caracter nepersonal, în special în cazul seturilor de date mixte. În acest caz, poate fi util să se facă diferența între seturile de date mixte în care datele cu caracter personal și cele cu caracter nepersonal sunt indisolubil legate și cele în care nu este cazul. Datele cu caracter personal și cele cu caracter nepersonal pot fi indisolubil legate în seturi de date mixte și pot intra în întregime sub sfera dreptului de acces al persoanei vizate la care se referă datele cu caracter personal[62]. În alte cazuri, datele cu caracter personal și cele cu caracter nepersonal din seturi de date mixte nu pot fi legate indisolubil făcând accesibile persoanei vizate doar datele cu caracter personal din set. De exemplu, o companie ar putea avea nevoie să furnizeze persoanei vizate rapoartele individuale ale incidentelor IT pe care le-a declanșat, dar nu și baza de cunoștințe a companiei despre problemele IT. Cu toate acestea, măsurile de securitate pe care operatorul le-a pus în aplicare nu trebuie în general înțelese ca fiind date cu caracter personal, cu condiția ca acestea să nu fie indisolubil legate 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 prevederilor RGPD, și în cele din urmă încalcă art. 8 din Carta drepturilor fundamentale. Aplicarea unui regim diferit de exercitare a unui drept în legătură cu unele tipuri de date cu caracter personal, care nu a fost prevăzut de RGPD poate fi introdusă exclusiv prin lege, în conformitate cu art. 23 din RGPD (după cum este explicat în

[60] După cum s-a menționat anterior în Orientările WP29 privind dreptul la portabilitatea datelor – aprobate de CEPD, p. 10 și reiterat în Orientările WP29 privind procesul decizional individual individualizat și crearea de profiluri – aprobate de CEPD, p. 17.

[61] Explicații suplimentare cu privire la conceptul de anonimizare pot fi găsite în Avizul 05/2014 al Grupului de lucru Art. 29 privind tehnicile de anonimizare, WP216, 10 aprilie 2014, p. 5 – 19.

[62] Comunicarea Comisiei către Parlamentul European și Consiliu, Orientări referitoare la Regulamentul privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea European, 29.05.2019, COM/2019/250 final.

secțiunea 6.4). Astfel, operatorii nu pot limita exercitarea dreptului de acces prin restrângerea nejustificată a sferei de aplicare a datelor cu caracter personal.

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

102. Conform art. 15(1) din RGPD, *„persoana vizată are dreptul să obțină de la operator confirmarea dacă sunt sau nu prelucrate datele cu caracter personal care îl sau o privesc și, dacă este cazul, să obțină acces la datele cu caracter personal și la următoarele informații”* (sublinierea noastră).

103. Câteva elemente reies din alineatul (1) al art. 15 din RGPD. Alineatul se referă expresis verbis la *„date cu caracter personal care îl sau o privesc”* (4.2.1), care *„sunt în curs de prelucrare”*(4.2.2) de către operator:

4.2.1 „date cu caracter personal care îl sau o privesc”

104. Dreptul de acces poate fi exercitat exclusiv cu privire la datele cu caracter personal ce privesc persoana vizată care solicită accesul sau, după caz, de către o persoană autorizată sau un mandatar autorizat (a se vedea secțiunea 3.4). Există și situații în care datele nu au o legătură cu persoana care exercită dreptul de acces ci cu o altă persoană fizică. Cu toate acestea, persoana vizată are dreptul la date cu caracter personal care se referă la el însuși, cu excepția datelor care privesc exclusiv pe altcineva[63].

105. Clasificarea datelor ca date cu caracter personal ce privesc persoana vizată nu depinde de faptul că aceste date cu caracter personal se referă și la altcineva[64]. Astfel, este posibil ca datele cu caracter personal să se refere la mai multe persoane fizice în același timp. Acest lucru nu înseamnă în mod automat că ar trebui acordat accesul la datele cu caracter personal și referitoare la altcineva, deoarece operatorul trebuie să se conformeze art. 15(4) din RGPD.

106. Cuvintele *„date cu caracter personal care îl sau o privesc”* nu trebuie interpretate într-un mod *„excesiv de restrictiv”* de către operatori, după cum a menționat deja Grupul de lucru Art. 29 cu privire la dreptul la portabilitatea datelor[65]. Aplicând dreptul de acces, CEPD consideră, de exemplu, că înregistrările convorbirilor telefonice (și transcrierea acestora) între solicitant și operator, pot intra sub incidența

[63] Orientările WP29 privind dreptul la portabilitatea datelor - aprobate de CEPD, p. 9: *„Doar 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 se referă la persoana vizată, nu vor fi incluse în respectivul domeniu de aplicare. Cu toate acestea, datele sub pseudonim care pot fi legate în mod clar de o persoană vizată [de exemplu, prin faptul că aceasta furnizează identificatorul respectiv în conformitate cu articolul 11 alineatul (2)] se încadrează în domeniul de aplicare.*

[64] CJUE, hotărârea în cauza C-434/16 Peter Nowak v Comisarul pentru protecția datelor, 2017, alin. 44.

[65] Orientările WP29 privind dreptul la portabilitatea datelor – aprobate de CEPD, p. 9: *În multe cazuri, operatorii vor prelucra informații care conțin date cu caracter personal ale mai multor persoane vizate. În acest caz, operatorii ar trebui să nu adopte o interpretare prea restrictivă a tezei „date cu caracter personal referitoare la persoana vizată”. Spre exemplu, telefonul, sistemul de mesagerie interpersonală sau înregistrările VoIP ar putea include (în istoricul din contul abonatului) detalii privind părți terțe implicate în apelurile primite și cele efectuate. Deși evidențele vor conține, așadar, date cu caracter personal referitoare la mai multe persoane, abonații ar trebui să aibă posibilitatea de a procura aceste înregistrări ca răspuns la cererile de portabilitate a datelor, deoarece acestea se referă (de asemenea) la persoana vizată. Cu toate acestea, în cazul în care aceste date sunt apoi transmise unui nou operator, acest nou operator nu ar trebui să le prelucreze în niciun scop care ar afecta în mod negativ drepturile și libertățile părților terțe (a se vedea mai jos: a treia condiție).”*

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 fie acoperită de scutirea gospodăriei conform art. 2(2)(c) din RGPD, în cazul în care persoana vizată utilizează înregistrarea obținută care include datele cu caracter personal ale interlocutorului în alte scopuri, de exemplu, publicând înregistrarea, persoana vizată va deveni operator pentru această prelucrare a datelor cu caracter personal ce privesc cealaltă persoană a cărei voce a fost înregistrată. Deși acest lucru nu va scuti operatorul de obligațiile sale de protecție a datelor atunci când analizează în mod corespunzător dacă se poate acorda acces la înregistrarea completă, operatorul este încurajat să informeze persoana vizată despre faptul că acesta poate deveni operator în acest caz. Acest lucru nu aduce atingere oricărei evaluări ulterioare conform art. 15(4) din RGPD detaliat în secțiunea 6. În același sens, mesajele pe care persoanele vizate le-au trimis altora sub formă de mesaje interpersonale și s-au șters de pe dispozitivul lor, care sunt încă disponibile furnizorului de servicii, pot fi vizate de dreptul de acces.

107. Iarăși, există situații în care legătura dintre date și mai multe persoane fizice poate părea neclară pentru operator, cum ar fi în cazul furtului de identitate. În caz de furt de identitate, o persoană acționează în mod fraudulos în numele altei persoane. În acest context, este important să reamintim că victima ar trebui să primească 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 infractorului. Cu alte cuvinte, chiar și după ce operatorul a aflat despre 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 fizică folosește în mod fraudulos identitatea altei persoane pentru a juca poker online. Infractorul plătește cazinoul online folosind cardul de credit pe care l-a furat de la victimă. Atunci când victima află despre furtul de identitate, aceasta solicită furnizorului cazinoului online să-i ofere acces la datele sale cu caracter personal și, mai precis, la jocurile online jucate și la informațiile despre cardul de credit utilizat de către infractor.

Există o legătură între datele colectate și victimă, deoarece identitatea acesteia din urmă a fost folosită. După detectarea fraudei, datele cu caracter personal menționate mai sus au încă o legătură din cauza conținutului lor (cardul de credit al victimei este în mod clar despre victimă), scop și efect (informațiile despre jocurile online jucate de infractor pot, de exemplu, să fie utilizate pentru a emite facturi către victimă). Prin urmare, cazinoul online va acorda victimei acces la datele cu caracter personal menționate mai sus.

108. Dacă este cazul, pot fi utilizate jurnalele de conectare interne pentru a păstra înregistrări despre accesările unui fișier și pentru a urmări ce acțiuni au fost efectuate în legătură cu accesările unei înregistrări, cum ar fi imprimarea, copierea sau ștergerea datelor cu caracter personal. Aceste jurnale pot include momentul înregistrării, motivul accesului la fișier, precum și informații care identifică persoana care a avut acces. Întrebări legate de acest subiect sunt în discuție într-o cauză aflată în prezent pe rolul CJUE (C-579/21). Realizarea și supravegherea și revizuirea jurnalelor de conectare intră în responsabilitatea operatorului și pot fi verificate de autoritățile de supraveghere. Operatorul ar trebui astfel să se asigure că persoanele care acționează sub autoritatea sa și care au acces la date cu caracter personal nu prelucrează date cu caracter personal decât la instrucțiunile operatorului, conform art. 29 din RGPD. În cazul în care, totuși, persoana prelucrează datele cu caracter personal în alte scopuri decât îndeplinirea instrucțiunilor operatorului, aceasta poate deveni operator pentru respectiva

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

prelucrare și poate face obiectul unor proceduri disciplinare sau penale sau sancțiuni administrative emise de autoritățile de supraveghere. CEPD observă că intră în atribuțiile angajatorului în temeiul art. 24 din RGPD să utilizeze măsuri corespunzătoare, extinzându-se de la instruire la proceduri disciplinare, pentru a se asigura că prelucrarea este în conformitate cu RGPD și că nu are loc nicio încălcare.

4.2.2 Datele cu caracter personal care „sunt în curs de prelucrare”

109. Alineatul (1) al art. 15 din RGPD se referă, de asemenea, la datele cu caracter personal, care „sunt în curs de prelucrare”. Momentul de referință pentru determinarea seriei de date cu caracter personal care se încadrează în cererea de acces a fost deja dezvoltat în secțiunea 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 companie a prelucrat date cu caracter personal ce privesc o persoană vizată pentru a procesa comanda sa de cumpărare și a aranja 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 legale referitoare la păstrarea evidențelor.

Persoana vizată solicită accesul la datele cu caracter personal care îl privesc. Pentru a se conforma obligației care îi revine în temeiul articolului 15(1) din RGPD, operatorul trebuie să furnizeze persoanei vizate datele cu caracter personal solicitate care sunt stocate pentru a se conforma obligațiilor 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 restabilirii datelor în cazul unui eveniment de pierdere a datelor. Trebuie subliniat că, în ceea ce privește principiile protecției datelor din momentul conceperii și minimizării datelor, datele de rezervă sunt, în principiu, similare cu datele din sistemul activ. Acolo unde există mici diferențe între datele cu caracter personal din sistemul de rezervă și cel de producție live, acestea sunt în general legate de colectarea de date suplimentare de la ultima copie de rezervă. O reducere a datelor din sistemul live (de exemplu, ștergerea 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 numai în momentul copierii ulterioare. În cazul în care există o cerere de acces în momentul în care există mai multe date cu caracter personal ce privesc persoana vizată în backup și nu în sistemul live sau date cu caracter personal diferite (observabile, de exemplu, prin jurnalul de ștergere în sistemul de producție live implementat în deplină conformitate cu principiul minimizării datelor), operatorul trebuie să fie transparent cu privire la această situație și, acolo unde este fezabil din punct de vedere tehnic, să ofere acces la solicitarea persoanei vizate, inclusiv la datele cu caracter personal stocate în sistemul de rezervă. De exemplu, pentru a fi transparent pentru persoanele vizate care își exercită dreptul, un jurnal al ștergerilor din sistemul de producție live poate permite operatorului să vadă că există date în backup care nu mai sunt în sistemul live, deoarece acestea au fost șterse recent și nu au fost încă suprascrise în back-up.

4.2.3 Sfera de aplicare a unei noi cereri de acces

111. Ceea ce rămâne de menționat este că persoanele vizate au dreptul să acceseze toate datele sau părți ale datelor prelucrate ce le privesc, în funcție de sfera de aplicare a cererii (a se vedea, de asemenea, 2.3.1 privind caracterul complet al informațiilor și 3.1. 1 pentru analiza conținutului cererii). În consecință, în cazul în care un operator s-a conformat deja unei cereri de acces în trecut și cu condiția ca cererea să nu fie excesivă, operatorul nu poate restrânge sfera de aplicare a acestei noi cereri. Aceasta înseamnă

că, în legătură cu orice altă cerere de acces a aceleiași persoane vizate, operatorul nu ar trebui să informeze persoana vizată doar despre simplele modificări ale datelor cu caracter personal prelucrate sau despre prelucrarea în sine de la ultima cerere, cu excepția cazului în care persoana vizată este de acord în mod expres. 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 privind informațiile lor ce țin de prelucrarea și drepturile persoanelor vizate.

4.3 Informații privind prelucrarea și drepturile persoanelor vizate

112. Pe lângă accesul la datele cu caracter personal în sine, operatorul trebuie să furnizeze informații privind prelucrarea și drepturile persoanelor vizate conform art. 15(1)(a)-(h) și 15(2) din RGPD. Majoritatea informațiilor referitoare la acele puncte specifice sunt deja compilate, cel puțin în formă generală, în evidența activităților de prelucrare a operatorului menționată la art. 30 din RGPD și/sau în notificarea sa de confidențialitate elaborată în conformitate cu art. 12 până la 14 din RGPD. Prin urmare, ar putea fi util ca în primul rând să se consultate „Orientările Grupului de lucru Art. 29 privind transparența conform Regulamentului 2016/679”[67] privind conținutul informațiilor care urmează să fie furnizate în temeiul art. 13 și 14 din RGPD.

113. Pentru a se conforma art. 15(1)(a)-(h) și 15(2), operatorii pot folosi cu atenție modulele de text ale notificării lor de confidențialitate, atât timp cât se asigură că sunt actualizate și precise în ceea ce privește cererea persoanei vizate. Înainte de prelucrarea datelor sau la începutul procesului, unele informații, cum ar fi identificarea anumitor destinatari sau durata specifică a prelucrării datelor, de multe ori încă nu pot fi furnizate. Unele informații, cum ar fi, de exemplu, dreptul de a depune o plângere la o autoritate de supraveghere [a se vedea art. 15(1)(f)], nu se modifică în funcție de persoana care depune cererea de acces. Prin urmare, poate fi comunicat în termeni generali, deoarece se face și în notificarea de confidențialitate. Alte tipuri de informații, cum ar fi informațiile despre destinatari, despre categorii și despre sursa datelor pot varia în funcție de cine depune cererea și care este sfera de aplicare a cererii. În contextul unei cereri de acces în temeiul art. 15, orice informație privind prelucrarea disponibilă operatorului poate, prin urmare, să fie actualizată și adaptată pentru operațiunile de prelucrare desfășurate efectiv în ceea ce privește persoana vizată care depune cererea. Astfel, referirea la formularea politicii sale de confidențialitate nu ar fi o modalitate suficientă pentru ca operatorul să ofere informațiile cerute de art. 15(1)(a)-(h) și (2), cu excepția cazului în care informațiile „adaptate și actualizate” sunt aceleași cu informațiile furnizate la începutul prelucrării. În explicarea informațiilor care se referă la solicitant, operatorul ar putea, după caz, să facă referire la anumite activități (cum ar fi „dacă ați folosit acest serviciu…”, „dacă ați plătit prin factură”), atât timp cât este evident pentru persoanele vizate, dacă sunt vizate. În cele ce urmează, gradul de specificare cerut este explicat în raport cu tipurile individuale de informații.

114. Informațiile privind scopurile conform art. 15(1)(a) trebuie să fie specifice cu privire la scopul (scopurile) precis(e) în cazul efectiv al persoanei vizate care solicită datele. Nu ar fi suficient să se enumere scopurile generale ale operatorului fără a clarifica ce scop (scopuri) urmărește operatorul în cazul de față al persoanei vizate care solicită datele. În cazul în care prelucrarea este efectuată în mai multe scopuri, operatorul trebuie să clarifice care date sau categorii de date sunt prelucrate în ce scop (scopuri). Spre deosebire de art. 13(1)(c) și art. 14(1)(c) din RGPD, informațiile privind prelucrarea menționată la art. 15(1)(a) nu conține informații cu privire la temeiul juridic al prelucrării. Cu toate

[67] Orientările Grupului de lucru 29, WP260 rev.01, 11 aprilie 2018 privind transparența în temeiul Regulamentului 2016/679 - aprobate de CEPD (denumite în continuare „Orientările WP29 privind transparența - aprobate de CEPD”).

acestea, întrucât drepturile unor persoane vizate depind de temeiul legal aplicabil, aceste informații sunt importante pentru persoanele vizate pentru a verifica legalitatea prelucrării datelor și pentru a determina drepturile persoanelor vizate care sunt aplicabile în situația dată. Prin urmare, pentru a facilita exercitarea drepturilor persoanelor vizate în conformitate cu art. 12(2) din RGPD, operatorului i se recomandă, de asemenea, să informeze persoana vizată cu privire la temeiul legal aplicabil pentru fiecare operațiune de prelucrare sau să indice unde poate găsi 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 notificare de confidențialitate).

115. Informațiile privind categoriile de date [articolul 15(1)(b)] pot fi, de asemenea, adaptate la situația persoanei vizate, astfel încât categoriile care s-au dovedit a fi irelevante în cazul solicitantului ar trebui eliminate.

Exemplul 19: În contextul informațiilor prevăzute la art. 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 numărul cardului de credit, etc.). În cazul în care în baza art. 15 se depune o cerere de acces, persoana vizată care depune cererea trebuie, pe lângă accesul la datele efective în curs de prelucrare (componenta 2), în conformitate cu art. 15(1)(b), să fie informat și cu privire la categoriile specifice de date care sunt prelucrate în cazul specific (de exemplu, neincluzând datele bancare sau datele cardului de credit în cazul în care plata a fost efectuată în numerar).

116. Informațiile privind „destinatarii sau categoriile de destinatari" [art. 15(1)(c)] trebuie să țină cont în primul rând de definiția destinatarilor dată la art. 4(9) din RGPD. Definiția destinatarilor se bazează pe dezvăluirea datelor cu caracter personal către o persoană fizică sau juridică, autoritate publică, agenție sau alt organ[68]. Din art. 4(9) din RGPD rezultă că autoritățile publice care acționează în cadrul unei anumite anchete care fac obiectul unor dispoziții naționale specifice nu trebuie să fie considerați destinatari.

117. În ceea ce privește întrebarea, dacă operatorul este liber să aleagă între informații despre destinatari sau despre categorii de destinatari, trebuie menționat că „spre deosebire de art. 13 și 14 din RGPD, care stabilesc o obligație din partea operatorului (…), articolul 15 din RGPD stabilește un drept de acces autentic pentru persoana vizată, astfel încât persoana vizată trebuie să aibă opțiunea de a obține fie informații despre destinatarii specifici cărora le-au fost sau vor fi dezvăluite datele, dacă este posibil, fie informații despre categoriile de destinatari."[69] De asemenea, trebuie reamintit că, așa cum se precizează în orientările menționate mai sus privind transparența[70] deja în temeiul art. 13 și 14 din RGPD informațiile despre destinatari sau categoriile de destinatari ar trebui să fie cât mai concrete posibil, cu respectarea principiilor transparenței și echității. Conform articolului 15, dacă 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 operatorul demonstrează că cererile de acces ale persoanei vizate sunt vădit nefondate sau excesive în sensul articolului 12(5) din RGPD. [71][72]

[68] Trebuie menționat că în aceeași companie pot exista diferiți operatori, în modul prevăzut la art. 4(7) din RGPD. Respectiv, este posibilă divulgarea datelor între mai mulți destinatari din cadrul aceleiași companii.

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

[70] Orientările Grupului de lucru 29, WP260 rev.01, 11 aprilie 2018 privind transparența în temeiul Regulamentului 2016/679 - aprobate de CEPD (denumite în continuare „Orientările WP29 privind transparența - aprobate de CEPD"), p. 37 (Anexă)

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

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

CEPD reamintește, în această privință, că stocarea informațiilor referitoare la destinatarii efectivi este necesară, printre altele, pentru a se putea conforma obligațiilor operatorului în temeiul art. 5(2) și 19 din RGPD.

Exemplul 20: În notificarea sa de confidențialitate, un angajator oferă informații despre categoriile de date care sunt transmise „agențiilor de turism" sau „hotelurilor" în cazul călătoriilor de afaceri, în conformitate cu art. 13(1)(e) și 14(1)(e) din RGPD. În cazul în care un angajat depune o cerere de acces la datele cu caracter personal după ce au avut loc călătorii de afaceri, angajatorul ar trebui atunci, în ceea ce privește destinatarii datelor cu caracter personal, în conformitate cu art. 15(1)(c), să indice în răspunsul său agenția (agențiile) de turism și hotelul (hotelurile) care au primit datele. În timp ce angajatorul s-a referit în mod legitim la categorii de destinatari în notificarea sa de confidențialitate în temeiul art. 13 și 14, deoarece la această etapă, nu a fost încă posibilă numirea destinatarilor, acesta ar trebui, dacă angajatul nu a ales altfel, să furnizeze informații cu privire la destinatarii specifici (denumirea agențiilor de turism, hotelurilor etc.) atunci când angajatul depune o cerere de acces.

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

118. Conform art. 15(1)(d), trebuie furnizate informații cu privire la perioada preconizată pentru care datele cu caracter personal vor fi stocate, acolo unde este posibil. În caz contrar, trebuie furnizate criteriile utilizate pentru a determina perioada respectivă. Informațiile furnizate de operator trebuie să fie suficient de precise pentru ca persoana vizată să știe cât timp vor continua să fie stocate datele ce privesc persoana vizată. Dacă nu este posibil să se precizeze momentul ștergerii, se va specifica durata perioadelor 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 perioadelor legale de stocare" nu este suficientă. Indicațiile privind perioadele de stocare a datelor vor trebui să se concentreze pe datele specifice ce privesc persoana vizată. În cazul în care datele cu caracter personal ale persoanei vizate fac obiectul unor perioade de ștergere diferite (de exemplu, deoarece nu toate datele sunt supuse obligațiilor legale de stocare), perioadele de ștergere vor fi precizate în raport 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 [art. 15(1)(f)] nu depind de circumstanțele specifice, drepturile persoanelor vizate menționate la art. 15(1)(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 art. 12(2) din RGPD, răspunsul operatorului cu privire la aceste drepturi va fi adaptat 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. Potrivit art. 15(1)(g), „orice informații disponibile" cu privire la sursa datelor trebuie furnizate, în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată. Gradul de informații disponibile se poate modifica în timp.

Exemplul 21: Politica de confidențialitate a unei companii mari prevede:

[73] Orientările WP29 privind transparența - aprobate de CEPD, p. 37 (Anexă)

„Verificările de credit ne ajută să prevenim problemele în tranzacțiile de plată. Acestea garantează protecția companiei noastre împotriva riscurilor financiare, care pot afecta și prețurile de vânzare pe termen mediu și lung. O verificare a creditului este efectuată în mod necesar atunci când vom expedia mărfuri fără a primi în același timp prețul de achiziție respectiv, de ex. în cazul unei achiziții cu plata facturii. Fără efectuarea verificării creditului, este posibilă doar o opțiune de plată în avans (transfer bancar imediat, furnizor de plăți online, card de credit).

În scopul verificării creditului, vă vom trimite numele, adresa și data nașterii 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 limitele a ceea ce este permis legal și numai în scopul analizei comportamentului dumneavoastră de plată din trecut, precum și pentru evaluarea riscului de neplată pe baza unor criterii matematice – proceduri statistice folosind datele de adresă precum și pentru verificarea adresei dumneavoastră (examinarea livrării). În funcție de rezultatul verificării creditului, este posibil să nu vă mai putem oferi metode de plată individuale, cum ar fi achiziționarea de facturi."

Notificarea de confidențialitate conține astfel informații generale cu privire la posibilitatea obținerii de informații de la Birourile de Informare Economică enumerate în conformitate cu art. 13 și 14 din RGPD. Dacă nu este clar ex ante care dintre companii se va implica în prelucrare, este suficient să se menționeze denumirea companiilor eligibile în politica de confidențialitate. În contextul unei cereri întemeiate pe art. 15, pe lângă informațiile că s-a obținut o informație de bonitate, ar fi necesar (ex post) să se dezvăluie care dintre companiile menționate a fost implicată exact. Este clar exprimat în art. 15(1)(g), că informațiile privind prelucrarea datelor cuprind „orice informații disponibile cu privire la sursa lor" în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată.

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

122. Informațiile despre transferurile de date intenționate către o țară terță sau o organizație internațională, inclusiv existența unei decizii a Comisiei privind caracterul adecvat sau a unor garanții corespunzătoare, trebuie furnizate în temeiul art. 13(1)(f) și 14(1)(f) din RGPD. În contextul unei cereri de acces în temeiul art. 15, art. 15(2) sunt necesare informații cu privire la garanțiile corespunzătoare în temeiul art. 46 din RGPD numai în cazurile în care transferul într-o țară terță sau într-o organizație internațională are loc efectiv.

5 CUM POATE UN OPERATOR SĂ OFERE ACCES?

[74] A se vedea în acest sens Orientările(WP260) privind transparența în temeiul Regulamentului 2016/679 alin. 41, cu referire la Orientările privind procesul decizional individual automatizat și crearea de profiluri în scopurile stabilite de Regulamentul 2016/679 (WP 251).

123. RGPD nu este foarte prescriptiv cu privire la 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 despre un persoană vizată. În alte situații, dreptul de acces este mai complicat deoarece prelucrarea datelor este mai complexă; în ceea ce privește numărul persoanelor vizate, categoriile de date prelucrate, precum și fluxul de date în cadrul și între diferite organizații.

124. Această secțiune își propune să ofere câteva îndrumări și exemple practice privind diferitele modalități prin care operatorii pot satisface o cerere de acces, precum și semnificația art. 12(1) din RGPD în legătură cu dreptul de acces. Această secțiune va oferi, de asemenea, câteva îndrumări cu privire la ceea ce este considerat a fi un format electronic utilizat în mod curent, precum și termenul pentru furnizarea accesului în conformitate cu art. 12(3) din RGPD.

5.1 Cum poate operatorul să recupereze datele solicitate?

125. Persoanele vizate ar trebui să aibă acces la toate informațiile ce le privesc pe care operatorul le prelucrează. Aceasta înseamnă, de exemplu, că operatorul este obligat să caute date cu caracter personal în sistemele sale IT și non-IT de evidență. Atunci când efectuează o astfel de căutare, operatorul ar trebui să utilizeze informațiile disponibile în organizație cu privire la persoana vizată, care probabil va duce la potriviri în sisteme, în funcție de modul în care sunt structurate informațiile.[75] De exemplu, dacă informațiile sunt sortate în fișiere în funcție de nume sau un număr de referință, căutarea ar putea fi limitată la acești factori. Dar dacă structura datelor depinde de alți factori, cum ar fi relațiile de familie sau titlurile profesionale sau orice fel de identificatori direcți sau indirecți (de exemplu, numărul clientului, numele utilizatorului sau adresele IP), căutarea trebuie extinsă pentru a include acestea, cu condiția ca operatorul să dețină și aceste informații ce privesc persoana vizată sau să i se furnizeze respectivele informații de către persoana vizată. Același lucru se aplică și atunci când înregistrările referitoare la terțe părți sunt susceptibile să conțină date cu caracter personal privind persoana vizată. Operatorul poate, totuși, să nu ceară persoanei vizate să furnizeze mai multe informații decât este necesar pentru a identifica persoana vizată. Dacă un operator folosește o persoană împuternicită de către operator pentru activitățile sale de prelucrare a datelor, căutarea trebuie să fie extinsă pentru a include și datele cu caracter personal prelucrate de către persoana împuternicită de către operator.

În conformitate cu art. 25 din RGPD privind protecția datelor începând cu momentul conceperii și în mod implicit, operatorul (și orice persoană împuternicită de către operator pe care o folosește) ar trebui să aibă deja implementate funcții care să permită conformarea cu drepturile persoanelor vizate. Aceasta înseamnă, în acest context, că ar trebui să existe modalități corespunzătoare de a găsi și de a prelua informațiile ce privesc o persoană vizată atunci când se gestionează o cerere. Cu toate acestea, trebuie remarcat faptul că o interpretare excesivă în acest sens ar putea conduce la funcții de identificare și recuperare a informațiilor care în sine prezintă un risc pentru confidențialitatea persoanelor vizate. Prin urmare, este important de reținut că procesul de recuperare a datelor ar trebui, de asemenea, conceput într-un mod prietenos de protecție a datelor, astfel încât să nu compromită confidențialitatea altora, de exemplu a angajaților operatorului.

[75] O astfel de căutare ar trebui, desigur, să includă și informații care sunt deținute de o persoană împuternicită de către operator, a se vedea articolul 28(3)(e) din RGPD.

5.2 Măsurile corespunzătoare pentru asigurarea accesului

5.2.1 Luarea „măsurilor corespunzătoare”

127. Articolul 12 din RGPD stabilește cerințele pentru furnizarea accesului, de ex. pentru furnizarea confirmării, a datelor cu caracter personal și a informațiilor suplimentare conform art. 15, și precizează, de asemenea, forma, modalitatea și termenul în raport cu dreptul de acces. „Orientările Grupului de lucru Art. 29[76] privind transparența în temeiul Regulamentului 2016/679” oferă îndrumări suplimentare cu privire la art. 12, mai ales în legătură cu art. 13 și 14 din RGPD dar și în legătură cu art. 15 și despre transparență în general. Astfel, ceea ce este definit în aceste orientări se poate aplica adesea în mod egal în ceea ce privește furnizarea accesului în temeiul articolului 15.

128. Articolul 12(1) din RGPD prevede că operatorul va lua măsurile corespunzătoare pentru a furniza orice comunicare conform art. 15 referitoare la prelucrare către persoana vizată într-o formă concisă, transparentă, inteligibilă și ușor accesibilă folosind un limbaj clar și simplu. Articolul 12(2) prevede că operatorul va facilita exercitarea dreptului de acces de către persoana vizată. Cerințele mai precise în acest sens vor trebui evaluate de la caz la caz. Atunci când decid ce măsuri sunt corespunzătoare, operatorii trebuie să ia în considerare toate circumstanțele relevante, inclusiv, dar fără a se limita la, cantitatea de date care sunt prelucrate, complexitatea prelucrării lor și cunoștințele pe care le au despre persoanele 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 orice nevoi speciale ale persoanei vizate care face solicitarea, de exemplu prin informații suplimentare din solicitarea făcută, operatorul trebuie să ia în considerare aceste circumstanțe. Ca urmare, măsurile corespunzătoare vor varia.

129. Este important de reținut atunci când se face evaluarea că termenul „corespunzător” nu trebuie niciodată înțeles ca o modalitate de limitare a sferei de aplicare a datelor acoperite de dreptul de acces. Termenul „corespunzător” nu înseamnă că eforturile de furnizare a informațiilor pot fi echilibrate cu, de exemplu, orice interes pe care persoana vizată îl poate avea în obținerea datelor cu caracter personal. În schimb, evaluarea ar trebui să urmărească alegerea celei mai adecvate metode de furnizare a tuturor informațiilor acoperite de acest drept, în funcție de circumstanțele specifice din fiecare caz. În consecință, un operator care prelucrează o cantitate mare de date la scară largă trebuie să accepte să depună eforturi mari pentru a asigura dreptul de acces al persoanelor vizate într-o formă concisă, transparentă, inteligibilă și ușor accesibilă folosind limbaj simplu și clar.

130. Trebuie evitată direcționarea persoanei vizate către diferite surse ca răspuns la o cerere de acces la date. După cum s-a afirmat anterior în Orientările WP29 privind transparența (în ceea ce privește noțiunea de „a furniza” din art. 13 și 14 din RGPD), noțiunea de „furnizare” presupune că *„persoana vizată nu trebuie să caute în mod activ informații acoperite de aceste articole, printre alte informații, cum ar fi termenii și condițiile de utilizare a unui site web sau a unei aplicații”.* [77] Prin urmare, și cu respectarea principiului transparenței, persoanele vizate trebuie să obțină de la operator informațiile și datele cu caracter personal prevăzute la art. 15(1), 15(2) și 15(3) într-un mod care să permită accesul complet la informațiile solicitate. În circumstanțe speciale, ar fi inadecvat sau chiar ofensator de a partaja informațiile în cadrul operatorului, de exemplu din cauza naturii sensibile a informațiilor (cum ar fi informațiile referitoare la denunțare). În aceste cazuri, s-ar considera adecvată împărțirea

[76] Orientările Grupului de lucru Art. 29, WP260 rev.01, 11 aprilie 2018 privind transparența în temeiul Regulamentului 2016/679 - aprobate de CEPD (denumite în continuare „Orientările WP29 privind transparența - aprobate de CEPD”).

[77] Orientările WP29 privind transparența – aprobate de CEPD, alin. 33.

informațiilor în mai multe răspunsuri ca răspuns la cererea de acces a persoanelor vizate. Metoda aleasă de operator trebuie să furnizeze de fapt persoanei vizate datele și informațiile solicitate, prin urmare nu ar fi potrivit să se adreseze persoanei vizate doar să verifice datele solicitate stocate pe propriul dispozitiv, inclusiv, de exemplu, să verifice istoricul fluxului de clicuri și adresele IP de pe telefonul lor mobil.

131. În conformitate cu principiul responsabilității, un operator trebuie să documenteze abordarea sa pentru a putea demonstra modul în care mijloacele alese pentru a furniza informațiile necesare în temeiul art. 15 sunt adecvate în circumstanțele în cauză.

5.2.2 Diferite mijloace de a oferi acces

132. După cum s-a explicat deja în secțiunea 2.2.2 de mai sus, atunci când depun o cerere de acces, persoanele vizate au dreptul să primească o copie a datelor lor în curs de prelucrare în temeiul art. 15(3) împreună cu informațiile suplimentare, care sunt considerate ca modalitate principală de asigurare a accesului la datele cu caracter personal.

133. Cu toate acestea, în anumite circumstanțe, ar putea fi oportun ca operatorul să ofere acces prin alte modalități decât furnizarea unei copii. Astfel de modalități nepermanente de acces la date ar putea fi, de exemplu: informarea orală, inspecția fișierelor, accesul la fața locului sau la distanță fără posibilitatea de descărcare. Aceste modalități pot fi modalități adecvate de acordare a accesului, de exemplu în cazurile în care este în interesul persoanei vizate sau 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 o cantitate mare de date nedigitalizate pentru a permite persoanei vizate să cunoască ce date cu caracter personal sunt în curs de prelucrare și să poată lua o decizie în cunoștință de cauză cu privire la ce date cu caracter personal dorește să i se furnizeze printr-o copie. Căile nepermanente de acces pot fi suficiente și adecvate în anumite situații; de exemplu, pot satisface nevoia persoanelor vizate de a verifica dacă datele prelucrate de operator sunt corecte oferindu-le persoanelor vizate șansa de a vizualiza datele originale. Un operator nu este obligat să furnizeze informațiile prin alte moduri decât furnizarea unei copii, dar ar trebui să adopte o abordare rezonabilă atunci când ia în considerare o astfel de cerere. Acordarea accesului prin alte căi decât furnizarea unei copii nu exclude persoanele vizate de dreptul de a avea și o copie, cu excepția cazului în care aleg să nu o facă.

134. Operatorul poate alege, în funcție de situația în cauză, să furnizeze copia datelor în curs de prelucrare, împreună cu informațiile suplimentare, în diferite moduri, de ex. prin e-mail, poștă fizică sau prin utilizarea unui instrument de autoservire. În cazul în care persoana vizată depune cererea prin mijloace electronice și cu excepția cazului în care persoana vizată solicită altfel, informațiile vor fi furnizate într-o formă electronică utilizată în mod curent, conform prevederilor art. 15(3). În orice caz, operatorul trebuie să ia în considerare măsurile tehnice și organizatorice corespunzătoare, inclusiv criptarea adecvată atunci când furnizează informații prin e-mail sau instrumente de autoservire online.

135. În situația în care operatorul prelucrează date cu caracter personal ce privesc solicitantul doar la scară mică, copia datelor cu caracter personal și informațiile suplimentare pot și trebuie furnizate printr-o procedură simplă.

Exemplul 22: O librărie locală păstrează o evidență a numelor și adreselor clienților care au comandat livrarea la domiciliu. Un client vizitează librăria și face o cerere de acces. În această situație ar fi suficientă tipărirea datelor cu caracter personal ce privesc clientul direct din sistemul de afaceri furnizând totodată și informațiile suplimentare prevăzute la art. 15(1) și (2).

Exemplul 23: Un donator lunar al unei organizații de caritate depune o cerere de acces prin e-mail. Organizația de caritate deține informații despre donațiile făcute 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 la e-mail, cu condiția să se aplice toate măsurile de protecție necesare luând în considerare, de exemplu, natura datelor.

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

Exemplul 24: Un administrator este desemnat de operator pentru a gestiona problemele practice privind cererile de acces. Atunci când primește o cerere, administratorul trimite o anchetă prin e-mail către diferitele departamente ale organizației solicitându-le să colecteze date cu caracter personal cu privire la persoana vizată. Reprezentanții fiecărui departament îi oferă administratorului datele cu caracter personal prelucrate de departamentul lor. Administratorul trimite apoi toate datele cu caracter personal persoanei vizate împreună cu informațiile suplimentare necesare, de exemplu și atunci când este cazul, prin e-mail.

137. Deși procesele manuale pentru gestionarea cererilor de acces ar putea fi considerate adecvate, unii operatori pot beneficia de utilizarea unor procese automatizate pentru a gestiona cererile persoanelor vizate. Acesta ar putea fi, de exemplu, cazul operatorilor care primesc un număr mare de cereri. O modalitate de a furniza informațiile conform art. 15 este prin furnizarea persoanei vizate de instrumente de autoservire. Acest lucru ar putea facilita o gestionare eficientă și în timp util a cererilor de acces ale persoanelor vizate și ar permite, de asemenea, operatorului să includă mecanismul de verificare în instrumentul de autoservire.

Exemplul 25: Un serviciu de social media are un proces automat pentru gestionarea cererilor de acces care permite persoanei vizate să își acceseze datele cu caracter personal din contul de utilizator. Pentru a prelua datele cu caracter personal, utilizatorii rețelelor de socializare pot alege opțiunea „Descărcați datele cu caracter personal" atunci când sunt conectați la contul lor de utilizator. Această opțiune de autoservire permite utilizatorilor să descarce un fișier care conține datele lor cu caracter personal direct din contul de utilizator pe propriul computer.

138. Utilizarea instrumentelor de autoservire nu ar trebui să limiteze niciodată sfera datelor cu caracter personal primite. Dacă nu este posibilă furnizarea tuturor informațiilor prevăzute la art. 15 prin intermediul instrumentului de autoservire, informațiile rămase trebuie furnizate într-un mod diferit. Operatorul poate, într-adevăr, să încurajeze persoana vizată să utilizeze un instrument de autoservire pe care operatorul l-a stabilit pentru gestionarea cererilor de acces. Cu toate acestea, trebuie remarcat faptul că operatorul trebuie să gestioneze și cererile de acces care nu sunt trimise prin canalul de comunicare stabilit. Asigurarea accesului într-o formă „concisă, transparentă, inteligentă și ușor accesibilă folosind limbaj clar și simplu".[78]

139. Potrivit art. 12(1) din RGPD, operatorul va lua măsurile corespunzătoare pentru a oferi accesul conform art. 15 într-o formă concisă, transparentă, inteligibilă și ușor accesibilă folosind un limbaj clar și simplu.

140. Cerința ca acordarea accesului persoanei vizate să se facă într-o formă concisă și transparentă înseamnă că operatorii trebuie să prezinte informațiile în mod eficient și succint pentru a fi ușor de înțeles de

[78] A se vedea secțiunea 3.1.2.

persoana vizată, mai ales dacă este un copil. Operatorul trebuie să țină cont de cantitatea și complexitatea datelor atunci când alege mijloacele de asigurare a accesului conform art. 15.

Exemplul 26: Un furnizor de rețele sociale prelucrează o cantitate mare de informații despre o persoană vizată. O mare parte a acestor date cu caracter personal sunt informații conținute în sute de pagini de fișiere-jurnal în care sunt înregistrate activitățile persoanei vizate pe site-ul web. Dacă persoanele vizate cer acces la datele lor cu caracter personal, datele cu caracter personal din aceste fișiere-jurnal sunt într-adevăr acoperite de dreptul de acces. Dreptul de acces poate fi, prin urmare, îndeplinit în mod oficial dacă aceste sute de pagini de fișiere-jurnal ar fi furnizate persoanei vizate. Cu toate acestea, fără măsurile luate pentru a facilita înțelegerea informațiilor din fișierele-jurnal, dreptul de acces al persoanei vizate s-ar putea să nu fie îndeplinit în practică, deoarece nicio informație nu poate fi extrasă cu ușurință din fișierele-jurnal, în consecință, neîndeplinind cerința art. 12(1) din RGPD. Prin urmare, operatorul trebuie să fie atent și minuțios 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 stratificate, similare abordării stratificate susținute în Orientările privind transparența în ceea ce privește notificările privind confidențialitatea, [79] ar putea fi o măsură corespunzătoare pentru a îndeplini ambele cerințe din art. 15 și 12(1) din RGPD. Acest lucru va fi detaliat în continuare în secțiunea 5.2.4. de mai jos. Cerința ca informația să fie „inteligibilă" înseamnă că trebuie înțeleasă de publicul vizat,[80] ținând cont de orice nevoi speciale pe care persoana vizată le-ar putea avea faptul fiind cunoscut de operator. [81] Întrucât dreptul de acces permite adesea exercitarea altor drepturi ale persoanelor vizate, este esențial ca informațiile furnizate să fie înțelese și clare. Acest lucru se datorează faptului că persoanele vizate vor putea decide dacă își vor invoca dreptul, de exemplu, la rectificare conform art. 16 din RGPD odată ce cunosc ce date cu caracter personal sunt prelucrate, în ce scopuri etc. Ca urmare, operatorul ar putea avea nevoie să furnizeze persoanei vizate informații suplimentare care explică datele furnizate. Trebuie subliniat faptul că complexitatea prelucrării datelor obligă operatorul să furnizeze mijloacele pentru a face datele inteligibile și nu ar putea fi folosită ca argument pentru limitarea accesului la toate datele. În mod similar, obligația operatorului de a furniza datele într-o manieră concisă nu poate fi folosită ca argument pentru limitarea accesului la toate datele.

Exemplul 27: Un site web de comerț electronic colectează date despre articolele vizualizate sau achiziționate pe site-ul său web în scopuri de marketing. O parte din aceste date va consta în date într-un format brut, [82] care nu a fost analizat și poate să nu aibă sens direct pentru cititor (coduri, istoricul activităților 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 într-un format brut, este important ca operatorul să ia măsurile necesare pentru a se asigura că persoana vizată înțelege datele, de exemplu, furnizând un document explicativ care traduce formatul brut într-o formă ușor de utilizat. De asemenea, un astfel de document

[79] Orientările WP29 privind transparența – aprobate de CEPD, alin. 35.

[80] Inteligibilitatea este strâns legată de cerința de a folosi un limbaj simplu și clar (Orientările WP29 privind transparența – aprobate de CEPD, alin. 9). Ceea ce se spune despre un limbaj simplu și clar la alin. 12-16 în ceea ce privește informațiile menționate la articolele 13 și 14 din RGPD, se aplică în mod egal comunicării în temeiul articolului 15.

[81] A se vedea alin. 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 prelucrabile numai automat (cum ar fi „biți").

ar putea explica că abrevierile și alte acronime, de exemplu „A” înseamnă că achiziția a fost întreruptă, iar „B” înseamnă că achiziția a fost finalizată.

142. Elementul „ușor accesibil” înseamnă că informațiile prevăzute la art. 15 ar trebui să fie prezentate într-un mod ușor de accesat pentru persoana vizată. Acest lucru se aplică, de exemplu, aspectului, titlurilor și paragrafelor corespunzătoare. Informațiile trebuie întotdeauna furnizate într-un limbaj simplu și clar. Un operator care oferă un serviciu într-o țară ar trebui să ofere și răspunsuri în limba pe care o înțeleg persoanele vizate din acea țară. Utilizarea pictogramelor standardizate este, de asemenea, încurajată atunci când facilitează inteligibilitatea și accesibilitatea informațiilor. Atunci când cererea de informații se referă la persoane vizate cu deficiențe de vedere sau alte persoane vizate care pot avea dificultăți în accesarea sau înțelegerea informațiilor, operatorul trebuie să ia măsuri care să faciliteze înțelegerea informațiilor furnizate, inclusiv a informațiilor orale, atunci când este cazul.[83] Operatorul ar trebui să aibă o grijă 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, oferind în mod proactiv elemente ușor accesibile pentru a facilita exercitarea acestor drepturi.

5.2.3 O cantitate mare de informații necesită cerințe specifice privind modul în care sunt furnizate informațiile

143. Indiferent de mijloacele folosite pentru a asigura accesul, poate exista o tensiune între cantitatea de informații pe care operatorul trebuie să le furnizeze persoanelor vizate și cerința ca acestea să fie concise. O modalitate de a le realiza pe ambele și un exemplu de măsură corespunzătoare pentru anumiți operatori, atunci când urmează să fie furnizată o cantitate mare de date, este utilizarea unei abordări stratificate. Această abordare poate facilita înțelegerea datelor de către persoanele vizate. Cu toate acestea, trebuie subliniat că această abordare poate fi utilizată numai în anumite circumstanțe și trebuie realizată într-un mod care să nu limiteze dreptul de acces, așa cum se explică mai jos. În plus, utilizarea unei abordări stratificate nu ar trebui să creeze o povară suplimentară pentru persoana vizată. Prin urmare, ar fi cea mai potrivită atunci când accesul este oferit într-un context online. O abordare stratificată este pur și simplu o modalitate de a prezenta informațiile conform art. 15 într-o manieră care să fie, de asemenea, conformă cerințelor art. 12(1) din RGPD și nu trebuie confundată cu posibilitatea operatorilor de a solicita ca persoana vizată să specifice informațiile sau activitățile de prelucrare la care se referă cererea, așa cum este prevăzut în considerentul 63 din RGPD.[84]

144. O abordare stratificată în legătură cu dreptul de acces înseamnă că un operator, în anumite circumstanțe, poate furniza datele cu caracter personal și informațiile suplimentare cerute de art. 15 în straturi diferite. Primul strat ar trebui să includă informații despre prelucrare și drepturile persoanei vizate conform art. 15(1)(a)-(h) și 15(2), precum și o primă parte a datelor cu caracter personal prelucrate. Într-un al doilea strat, ar trebui furnizate mai multe date cu caracter personal.

145. Atunci când decide ce informații ar trebui furnizate în diferitele straturi, operatorul ar trebui să ia în calcul informațiile pe care persoana vizată le-ar considera în general ca fiind cele mai relevante. În conformitate cu principiul echității, primul strat ar trebui să conțină și informații despre prelucrarea care are cel mai mare impact asupra persoanei vizate. [85] [86] Operatorii trebuie să fie capabili să demonstreze responsabilitate în ceea ce privește raționamentul de mai sus.

[83] A se vedea Orientările WP29 privind transparența – aprobate de CEPD, alin. 21.
[84] A se vedea secțiunea 2.3.1.
[85] A se vedea Orientările WP29 privind transparența – aprobate de CEPD, alin. 36
[86] A se vedea nota de subsol 82.

Exemplul 28: Un operator analizează seturi mari de date pentru a plasa clienții în diferite segmente, în funcție de comportamentul lor online. În această situație, se poate presupune că informația care este cea mai importantă pentru ca persoanele vizate să le obțină este informația despre segmentul în care au fost introduse. Ca rezultat, aceste informații ar trebui incluse în primul strat. Datele într-un format brut care nu au fost încă analizate sau prelucrate suplimentar, cum ar fi activitatea utilizatorului pe un site web, sunt, de asemenea, date cu caracter personal acoperite de dreptul de acces, totuși, în unele cazuri, ar putea fi suficientă furnizarea acestor informații într-un alt strat.

146. Pentru ca utilizarea abordării stratificate să fie considerată o măsură corespunzătoare, este necesar ca persoana vizată să fie informată de la început despre faptul că informațiile prevăzute la art. 15 sunt structurate în diferite straturi și sunt prevăzute cu o descriere a datelor și informațiilor cu caracter personal care vor fi conținute în diferitele straturi. În acest fel, va fi mai ușor pentru persoana vizată să decidă ce straturi dorește să acceseze. Descrierea ar trebui să reflecte în mod obiectiv toate categoriile de date cu caracter personal care sunt efectiv prelucrate de operator. De asemenea, trebuie să fie clar modul în care persoana vizată poate avea acces la diferitele straturi. Accesul la diferitele straturi nu implică niciun efort disproporționat pentru persoana vizată și nu va fi condiționat de formularea unei noi cereri a persoanei vizate. Aceasta înseamnă că persoanele vizate trebuie să aibă posibilitatea de a alege să acceseze toate straturile simultan sau să acceseze unul sau două dintre straturi, dacă sunt satisfăcute de acest lucru.

Exemplul 29: O persoană vizată depune o cerere de acces la un serviciu de difuzare video. Cererea se depune printr-o opțiune care este disponibilă atunci când persoanele vizate s-au autentificat în contul lor. Persoanei vizate i se prezintă două opțiuni care apar ca butoane pe pagina web. Opțiunea 1 este descărcarea părții 1 a datelor cu caracter personal și a informațiilor suplimentare. Aceasta conține, de exemplu, istoricul de difuzare recent, informații despre cont și informații despre plată. Opțiunea 2 este descărcarea părții 2 a datelor cu caracter personal care conține fișiere-jurnal tehnice despre activitățile persoanelor vizate și informații istorice despre cont. În acest caz, operatorul a făcut posibil ca persoanele vizate să-și exercite dreptul într-un mod care să nu creeze o povară suplimentară pentru persoana vizată.

Variația 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.

Variația 2: În cazurile în care persoana vizată alege butoanele atât pentru partea 1, cât și pentru partea 2 a datelor, operatorul nu poate comunica doar partea 1 a datelor și nu poate cere o nouă confirmare înainte de comunicarea părții 2 a datelor. În schimb, ambele părți ale datelor trebuie furnizate persoanei vizate, după cum rezultă din cererea depusă.

Utilizarea unei abordări stratificate nu va fi considerată adecvată pentru toți operatorii sau în toate situațiile. Ar trebui să fie utilizată numai atunci când ar fi dificil pentru persoana vizată să înțeleagă informațiile dacă sunt furnizate în întregime. Cu alte cuvinte, operatorul trebuie să fie capabil să demonstreze că utilizarea abordării stratificate adaugă valoare persoanei vizate ajutând-o să înțeleagă informațiile furnizate. Prin urmare, o abordare stratificată ar fi considerată adecvată numai atunci când un operator prelucrează o cantitate mare de date cu caracter personal despre persoana vizată care face o solicitare și în cazul în care ar exista dificultăți aparente pentru persoana vizată de a sesiza sau înțelege informațiile dacă ar fi furnizate în întregime. Faptul că ar fi nevoie de un mare efort și resurse din partea operatorului pentru a furniza informațiile prevăzute la art. 15 nu este în sine un argument pentru utilizarea unei abordări stratificate.

5.2.4 Formatul

148. Potrivit art. 12(1) din RGPD, informațiile prevăzute la art. 15 vor fi furnizate în scris sau prin alte mijloace, inclusiv, după caz, prin mijloace electronice. În ceea ce privește accesul la datele cu caracter personal în curs de prelucrare, art. 15(3) prevede că, în cazul în care persoana vizată depune cererea prin mijloace electronice, și dacă nu este solicitat altfel de către persoana vizată, informațiile vor fi furnizate într-o formă electronică utilizată în mod curent. RGPD nu specifică ce este un format electronic utilizat în mod obișnuit. Astfel, există mai multe formate imaginabile care pot fi utilizate. Ceea ce este considerat 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 determina ce format trebuie considerat un format utilizat în mod curent în situația în cauză, operatorul va trebui să evalueze dacă există formate specifice utilizate în general în zona de operare a operatorului sau în contextul dat. Atunci când 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 fie considerate a fi 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 cât de ușor poate accesa persoana fizică informațiile furnizate în formatul actual. În acest sens, trebuie menționat ce informații a furnizat operatorul persoanei vizate cu privire la modul de accesare a unui fișier care a fost furnizat într-un anumit format, cum ar fi ce programe sau software-uri 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 software-ul pentru a avea acces la informații.

150. Atunci când se decide asupra formatului în care copia datelor cu caracter personal și informațiilor prevăzute la art. 15 ar trebui furnizate, operatorul trebuie să țină cont de faptul că formatul trebuie să permită prezentarea informațiilor într-un mod inteligibil și ușor accesibil. Este important ca persoana vizată să primească informațiile în formă încorporată, permanentă (text, electronic). Deoarece informațiile ar trebui să persiste în timp, informațiile în scris, inclusiv prin mijloace electronice, sunt, în principiu, de preferat față de alte forme. Copia datelor cu caracter personal ar putea fi stocată, atunci când este cazul, pe un dispozitiv de stocare electronic, cum ar fi un CD sau USB.

151. Trebuie menționat 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 le 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-o formă electronică utilizată în mod curent.

152. Este responsabilitatea operatorului să decidă asupra formei corespunzătoare 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 despre persoanele vizate care fac solicitarea, în forma lor originală. Operatorul ar putea, de exemplu, de la caz la caz, să ofere acces la o copie a suportului ca atare, având în vedere necesitatea de transparență (de exemplu, pentru a verifica acuratețea datelor deținute de operator în cazul unei cereri de acces la dosarul medical sau a unei înregistrări audio a cărei transcriere este contestată). Cu toate acestea, CJUE, în interpretarea sa a dreptului de acces în temeiul Directivei 95/46/CE, a afirmat că „pentru ca *[dreptul de acces]* să fie respectat, este suficient ca solicitantului să i se furnizeze un rezumat complet al acestor date într-o formă inteligibilă, adică într-o formă care îi permite să ia cunoștință de aceste date și să verifice dacă sunt exacte și prelucrate în

conformitate cu directiva menționată, astfel încât să își poată exercita, după caz, drepturile conferite”.[87] Spre deosebire de directivă, RGPD conține în mod expres obligația de a furniza persoanei vizate o copie a datelor cu caracter personal în curs de prelucrare. Aceasta, însă, 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 care sunt prelucrate în aceste documente.[88] O astfel de copie a datelor cu caracter personal ar putea fi furnizată printr-o compilație care să conțină toate datele cu caracter personal acoperite de dreptul de acces, atât timp cât compilarea face posibil ca persoana vizată să cunoască și să verifice legalitatea prelucrării. Prin urmare, nu există nicio contradicție între formularea RGPD și hotărârea CJUE cu privire la această chestiune. Cuvântul „rezumat” din hotărâre nu ar trebui interpretat greșit în sensul că compilarea nu ar cuprinde toate datele acoperite de dreptul de acces, ci este pur și simplu o modalitate de a prezenta toate aceste date fără a oferi acces la documentele subiacente care conțin datele cu caracter personal. Deoarece compilarea trebuie să conțină o copie a datelor cu caracter personal, trebuie subliniat că aceasta nu poate fi făcută într-un mod care să modifice sau să schimbe cumva conținutul informațiilor.

Exemplul 30: O persoană vizată este asigurată de mulți ani la o companie de asigurări. Au avut loc mai multe incidente asigurate. În fiecare caz, a existat o corespondență scrisă prin e-mail între persoana vizată și compania de asigurări. Întrucât persoana vizată trebuia să furnizeze informații cu privire la circumstanțele specifice ale fiecărui incident, corespondența presupune o mulțime de informații personale despre persoana vizată (hobby-uri, colegi de apartament, obiceiuri zilnice etc.). În unele cazuri, a apărut un dezacord cu privire la obligația companiei de asigurări de a despăgubi persoana vizată, ceea ce a provocat multe discuții contradictorii. Toată această corespondență este stocată de compania de asigurări. Persoana vizată depune o cerere de acces. În această situație, operatorul nu trebuie neapărat să furnizeze e-mailurile în forma lor originală prin transmiterea acestora către persoana vizată. În schimb, operatorul ar putea alege să compileze corespondența prin e-mail ce conține datele cu caracter personal ale persoanei vizate într-un fișier care este furnizat persoanei vizate.

153. Fără a aduce atingere formei în care operatorul furnizează datele cu caracter personal, de ex. prin furnizarea documentelor efective care conțin datele cu caracter personal sau o compilare a datelor cu caracter personal, informațiile vor respecta cerințele de transparență prevăzute la art. 12 din RGPD. Efectuarea unui fel de compilări și/sau extrageri a datelor într-un mod care să facă informațiile ușor de înțeles ar putea, în unele cazuri, să fie o modalitate de a se conforma cu 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, care formă este cea mai potrivită trebuie decis de la caz la caz.

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

155. În unele cazuri, datele cu caracter personal în sine stabilesc cerințele în ce format ar trebui furnizate datele cu caracter personal. De exemplu, atunci când datele cu caracter personal constituie informații

[87] CJUE, Cauzele conexe C-141/12 și 372/12, YS și Alții, alin. 60.

[88] Întrebări legate de acest subiect sunt în discuție în cauzele aflate în prezent pe rolul CJUE (C-487/21 și C307/21).

scrise de mână de către persoana vizată, este posibil ca persoana vizată să aibă nevoie de o fotocopie a respectivei informații scrise de mână, deoarece scrisul de mână în sine constituie date cu caracter personal. Acesta ar putea fi mai ales cazul când scrisul de mână este ceva care contează pentru prelucrare, de ex. analiza scripturii. Același lucru este valabil în general pentru înregistrările audio, deoarece vocea persoanei vizate în sine constituie date cu caracter personal. În unele cazuri, totuși, accesul poate fi oferit prin furnizarea unei transcrieri a conversației, de exemplu, dacă este convenit între persoana vizată și operator.

156. Trebuie menționat că dispozițiile privind cerințele de format sunt diferite în ceea ce privește dreptul de acces și dreptul la portabilitatea datelor. În timp ce dreptul la portabilitatea datelor în temeiul art. 20 din RGPD impune ca informațiile să fie furnizate într-un format care poate fi citit automat, dreptul la informații în temeiul art. 15 nu impun acest lucru. Prin urmare, formatele care sunt considerate a fi neadecvate atunci când se conformează cu o cerere de portabilitate a datelor, de exemplu fișierele pdf, ar putea fi în continuare adecvate atunci când se conformează unei cereri de acces.

5.3 Termenul pentru furnizarea accesului

157. Articolul 12(3) din RGPD impune ca operatorul să furnizeze informații persoanei vizate cu privire la acțiunile întreprinse în legătură cu o cerere conform art. 15 fără întârzieri nejustificate și, în orice caz, în termen de o lună de la primirea cererii. Acest termen poate fi prelungit cu maximum două luni, ținând cont de complexitatea și numărul de cereri, 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 întârziere și motivele acesteia nu trebuie confundată cu informațiile care trebuie furnizate fără întârziere și cel târziu în termen de o lună, când operatorul nu ia măsuri în legătură cu cererea, conform art. 12(4) din RGPD.

158. Operatorul reacționează și, ca regulă generală, furnizează informațiile prevăzute la art. 15 fără întârzieri nejustificate, ceea ce înseamnă că informația trebuie furnizată cât mai curând posibil. Aceasta înseamnă că, dacă este posibil să furnizeze informațiile solicitate în mai puțin de o lună, operatorul ar trebui să facă acest lucru. CEPD consideră, de asemenea, că momentul de răspuns la cerere în unele situații trebuie adaptat la perioada de stocare pentru a se putea oferi acces[89]

159. Termenul limită începe în momentul în care operatorul a primit o cerere conform art. 15, adică atunci când cererea ajunge la operator prin unul dintre canalele sale oficiale.[90] Nu este necesar ca operatorul să cunoască, de fapt, cererea. Cu toate acestea, atunci când operatorul trebuie să comunice cu persoana vizată din motiv că nu este sigur de identitatea solicitantului, cererea poate fi suspendată până când operatorul va 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 unui persoane vizate să specifice operațiunile de prelucrare la care se referă cererea, atunci când sunt îndeplinite condițiile prevăzute la considerentul 63[91] .

Exemplul 31: În urma recepționării cererii, un operator reacționează imediat și cere informațiile de care are nevoie pentru a confirma identitatea solicitantului. Acesta din urmă răspunde doar câteva zile mai târziu, iar informațiile pe care persoana vizată le transmite pentru verificarea identității nu par

[89] A se vedea secțiunea 2.3.3

[90] În unele state membre există o legislație națională care stabilește când un mesaj trebuie considerat ca fiind primit, ținând cont de weekenduri și sărbători naționale.

[91] A se vedea secțiunea 2.3.1.

suficiente, ceea ce impune operatorului să ceară clarificări. În această situație va exista o suspendare în timp până când operatorul va obține suficiente informații pentru a verifica identitatea persoanei vizate.

160. Perioada de timp pentru a răspunde la o cerere de acces trebuie calculată în conformitate cu Regulamentul nr. 1182/71.[92]

Exemplul 32: O organizație primește o cerere pe 5 martie. Termenul limită începe în aceeași zi. Acest lucru îi acordă organizației timp până la 5 aprilie inclusiv, cel târziu, pentru a satisface cererea.

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

161. În cazul în care ultima zi a acestui termen cade într-un weekend sau într-o sărbătoare oficială, 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 cont de complexitatea și numărul cererilor. Trebuie subliniat faptul că această posibilitate este o exceptare de la regula generală și nu trebuie suprautilizată. Dacă operatorii sunt adesea nevoiți să prelungească termenul, ar putea fi un indiciu al necesității de a-și dezvolta în continuare procedurile generale de gestionare 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:

- cantitatea de date prelucrată de operator,
- modul în care sunt stocate informațiile, în special atunci când este dificil să se preia informațiile, de exemplu atunci când datele sunt prelucrate de diferite unități ale organizației,
- necesitatea de a redacta informații atunci când se aplică o exceptare, de exemplu informații referitoare la alte subiecte de date sau care constituie secrete comerciale și
- când informația necesită eforturi suplimentare pentru a fi inteligibilă.

164. Simplul fapt că satisfacerea cererii ar necesita un efort mare nu face o cerere complexă. În mod similar, faptul că o companie mare primește un număr mare de cereri nu ar declanșa automat o prelungire a termenului. Totuși, atunci când un operator primește temporar un număr mare de cereri, de exemplu datorită unei reclame extraordinare cu privire la activitățile sale, aceasta poate fi considerată un motiv legitim pentru prelungirea termenului de răspuns. Cu toate acestea, un operator, în special unul care operează cu o cantitate mare de date, ar trebui să aibă proceduri și mecanisme în vigoare pentru a putea gestiona cererile în termenul-limită în circumstanțe normale.

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

6 LIMITELE ȘI RESTRICȚIILE DREPTULUI DE ACCES

6.1 Observații generale

165. Dreptul de acces este supus limitelor care rezultă din art. 15(4) din RGPD (drepturile și libertățile altora) și art. 12 (5) din RGPD (cereri vădit nefondate sau excesive). În plus, legislația Uniunii sau statelor membre poate restrânge dreptul de acces în conformitate cu art. 23 din RGPD. Derogările privind prelucrarea datelor cu caracter personal în scopuri științifice, de cercetare istorică sau statistică sau în scopuri de arhivare în interes public se pot baza pe art. 89(2) și art. 89(3) din RGPD în consecință și derogările pentru prelucrarea efectuată în scopuri jurnalistice sau în scop de exprimare academică, artistică sau literară se pot baza pe art. 85(2) din RGPD.

166. Este important de menționat că, în afară de limitele, derogările și eventualele 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 la proporționalitate în ceea ce privește eforturile pe care operatorul trebuie să le depună pentru a se conforma cu cererea persoanelor vizate în temeiul art. 15 din RGPD.[93] În plus, nu este permisă limitarea sau restricționarea dreptului de acces într-un contract între operator și persoana vizată.

167. Potrivit considerentului 63, dreptul de acces este acordat persoanelor vizate pentru a fi conștienți de legalitatea prelucrării și a o verifica. Dreptul de acces permite persoanei vizate, printre altele, să obțină, în funcție de circumstanțe, rectificarea, ștergerea sau blocarea datelor cu caracter personal. [94] Cu toate acestea, persoanele vizate nu sunt obligate să motiveze sau să își justifice cererea. Atât timp cât cerințele art. 15 din RGPD sunt îndeplinite, scopurile cererii ar trebui considerate irelevante.[95]

6.2 Articolul 15 (4) din RGPD

168. Potrivit art. 15(4) din RGPD, dreptul de a obține o copie nu va afecta în mod negativ drepturile și libertățile altora. Explicațiile cu privire la această limitare sunt oferite în propozițiile a cincea și a șasea din considerentul 63. Acest drept nu ar trebui să afecteze în mod negativ drepturile sau libertățile altora, inclusiv secretele comerciale sau proprietatea intelectuală și în special drepturile de autor care protejează software-ul. Totuși, rezultatul acestor considerații nu ar trebui să fie un refuz de a furniza toate informațiile persoanei vizate. La interpretarea art. 15(4) din RGPD trebuie acordată atenție specială pentru a nu extinde în mod nejustificat restricțiile prevăzute la art. 23 din RGPD, care sunt permise numai în condiții stricte.

169. Articolul 15(4) din RGPD se aplică dreptului de a obține o copie a datelor, care este modalitatea principală de acordare a accesului la datele prelucrate (a doua componentă a dreptului de acces). Este, de asemenea, aplicabil, iar drepturile și libertățile celorlalți vor fi luate în considerare, dacă 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 prin furnizarea unei copii sau prin acordarea accesului persoanei vizate la fața locului. Articolul 15(4) din RGPD nu se

[93] În cazul în care operatorul prelucrează o cantitate mare de informații ce privesc persoana vizată, așa cum se menționează în considerentul 63 din RGPD, operatorul poate solicita persoanei vizate să specifice informațiile sau activitățile de prelucrare la care se referă cererea. A se vedea și secțiunea 2.3.1.

[94] CJEU, Cauzele conexe C-141/12 și C-372/12, YS și Alții.

[95] Acest lucru nu aduce atingere oricărei legi naționale aplicabile care respectă cerințele prevăzute de art. 23 din RGPD, a se vedea capitolul 6.4.

aplică informațiilor suplimentare cu privire la prelucrare, după cum este prevăzut la art. 15(1) lit. a)-h) din RGPD.

170. Potrivit considerentului 63, drepturile și libertățile conflictuale includ secretele comerciale sau proprietatea intelectuală și în special drepturile de autor care protejează software-ul. Aceste drepturi și libertăți menționate în mod explicit ar trebui privite doar ca exemple, deoarece, în principiu, orice drept sau libertate bazată pe dreptul Uniunii sau al statului membru poate fi considerată că invocă limitarea art. 15(4) din RGPD. [96] Astfel, dreptul la protecția datelor cu caracter personal (art. 8 din Carta europeană a drepturilor fundamentale) poate fi considerat și drept afectat în sensul art. 15(4) din RGPD

În ceea ce privește dreptul de a obține o copie, dreptul la protecția datelor altora este un caz tipic în care limitarea trebuie evaluată. În plus, trebuie luat în considerare dreptul la confidențialitatea corespondenței, de exemplu în ceea ce privește corespondența privată prin e-mail în contextul angajării. [97]Este important de menționat că nu orice interes echivalează cu „drepturi și libertăți" în temeiul art. 15(4) din RGPD. De exemplu, interesele economice ale unei companii de a nu dezvălui date cu caracter personal nu ating pragul pentru recurgerea la excepția prevăzută la art. 15(4) atât timp cât nu sunt afectate secrete comerciale, proprietate intelectuală sau alte drepturi protejate.

171. „Alții" înseamnă orice altă persoană sau entitate, în afară de persoana vizată, care își exercită dreptul de acces. Prin urmare, ar putea fi luate în considerare drepturile și libertățile operatorului sau persoanei împuternicite de către operator (de exemplu, la păstrarea confidențialității secretelor comerciale și a proprietății intelectuale). Dacă legiuitorul UE ar fi dorit să excludă drepturile și libertățile operatorilor sau persoanelor împuternicite de către operatori, ar fi folosit termenul „terță parte", care este definit la art. 4(10) din RGPD.

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

Exemplul 34: O persoană care este acum adult a fost îngrijită de biroul de asistență pentru tineri timp de mai mulți ani în trecut. Fișierele corespunzătoare pot conține informații sensibile despre 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, cu referire la art. 15(4) din RGPD. Mai degrabă, drepturile și libertățile celorlalți trebuie să fie examinate în detaliu și demonstrate de către biroul de asistență pentru tineri 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 ștergerea numelor).

173. În ceea ce privește considerentul 4 din RGPD și raționamentul art. 52(1) din Carta europeană a drepturilor fundamentale, dreptul la protecția datelor cu caracter personal nu este un drept absolut.[98] Prin urmare, exercitarea dreptului de acces trebuie să fie echilibrată cu alte drepturi fundamentale, în conformitate cu principiul proporționalității. Când evaluarea art. 15(4) din RGPD demonstrează că

[96] Ponderea sau prioritatea drepturilor și libertăților conflictuale nu este o chestiune de definire a termenilor „drepturi și libertăți". Cu toate acestea, echilibrarea unor astfel de interese face parte dintr-o a doua etapă a evaluării, dacă art. 15(4) este aplicabil. A se vedea alin. 173 mai jos.

[97] CEDO, Bărbulescu v. Romania, nr. 61496/08, alin. 80, 5 septembrie 2017.

[98] A se vedea, de exemplu, și CJUE, Cauzele conexe C-92/09 și C-93/09, Volker und Markus Schecke GbR și Hartmut Eifert v. Land Hessen [GC], 9 noiembrie 2010, alin. 48.

satisfacerea cererii are efecte adverse (negative) asupra drepturilor și libertăților altor participanți (pasul 1), interesele tuturor participanților trebuie cântărite luând în considerare circumstanțele specifice ale cazului și în special probabilitatea și gravitatea riscurilor prezente în comunicarea datelor. Operatorul ar trebui să încerce să reconcilieze drepturile aflate în conflict (pasul 2), de exemplu prin punerea în aplicare a măsurilor corespunzătoare care atenuează riscul pentru drepturile și libertățile altora. După cum se subliniază în considerentul 63, protejarea drepturilor și libertăților altora în virtutea art. 15(4) din RGPD nu ar trebui să aibă ca rezultat refuzul de a furniza toate informațiile persoanei vizate. Aceasta înseamnă, de exemplu, în cazul în care se aplică limitarea, că informațiile ce privesc 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 de găsit o soluție de reconciliere a drepturilor relevante, operatorul trebuie să decidă într-o etapă următoare care dintre drepturile și libertățile aflate în conflict prevalează (pasul 3).

Exemplul 35: Un comerciant cu amănuntul oferă clienților săi posibilitatea de a comanda produse printr-o linie telefonică operată de serviciul său pentru clienți. În scopul dovedirii tranzacțiilor comerciale, comerciantul cu amănuntul stochează o înregistrare a apelurilor, în conformitate cu cerințele stricte ale legislației în vigoare. Un client dorește să primească o copie a conversației pe care a avut-o cu un reprezentant relații clienți. Într-o primă etapă, comerciantul cu amănuntul analizează cererea și realizează că înregistrarea conține date cu caracter personal referitoare și la o altă persoană, și anume reprezentantul relații clienți. Într-o a doua etapă, pentru a evalua dacă furnizarea copiei ar afecta drepturile și libertățile altora, comerciantul cu amănuntul trebuie să echilibreze interesele conflictuale, în special ținând cont de probabilitatea și gravitatea posibilelor riscuri la adresa drepturilor și libertăților reprezentantului relații clienți, care sunt prezente în comunicarea înregistrării către client. Comerciantul cu amănuntul concluzionează că în dosar există date cu caracter personal foarte limitate ce privesc reprezentantul relații clienți, doar vocea acestuia. Comerciantul cu amănuntul/operatorul constată că reprezentantul nu este ușor de identificat. Mai mult, 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 afectează în mod negativ drepturile și libertățile reprezentatului relații clienți și, prin urmare, operatorul poate furniza persoanei vizate înregistrarea completă, inclusiv părțile înregistrării vocale ce privesc reprezentatul relații clienți.

Exemplul 36: O clientă a unui magazin de produse medicale dorește să aibă acces la rezultatele măsurării privind picioarele sale în baza art. 15 din RGPD. Magazinul de materiale medicale măsurase picioarele persoanei vizate pentru a crea ciorapi compresivi medicali individuali. Aparent, magazinul de materiale medicale avea multă experiență și stabilise o tehnică specială pentru măsurarea exactă. După măsurarea în magazinul de produse medicale, clienta dorește să folosească rezultatele măsurării pentru a cumpăra șosete mai ieftine în altă parte (comandându-le într-un magazin online). Magazinul de produse medicale refuză parțial accesul la date în baza art. 15(4) din RGPD susținând că, datorită tehnicilor lor speciale și precise de măsurare, rezultatele au fost protejate ca secrete comerciale. Dacă și în măsura în care operatorul poate dovedi că:

- furnizarea persoanei vizate informații despre rezultatele măsurării nu este posibilă fără a dezvălui modul în care au fost efectuate măsurările și
- informațiile despre modul în care au fost efectuate măsurările, inclusiv, dacă este cazul, determinarea exactă a punctelor de măsurare sunt secrete comerciale

acesta poate aplica art. 15(4) din RGPD.

Operatorul ar trebui să furnizeze în continuare cât mai multe informații despre rezultatele măsurărilor care nu ar dezvălui secretul său comercial, chiar dacă aceasta ar implica efortul de a revizui și edita rezultatele.

Exemplul 37: JUCĂTORUL X este înregistrat ca utilizator pe platforma de jocuri PLATFORMA Y. Într-o zi, JUCĂTORUL X este notificat că contul său online a fost restricționat. Întrucât nu se mai poate autentifica, JUCĂTORUL X solicită operatorului accesul la toate datele cu caracter personal care îl privesc. În plus, JUCĂTORUL X cere acces la motivele restricționării contului. PLATFORMA Y, operatorul platformei de jocuri online la care a fost depusă cererea, informează utilizatorii în termenii și condițiile generale disponibile pe site-ul său, că orice fel de înșelăciune (în principal prin utilizarea de software de terță parte) va atrage după sine interzicerea temporară sau permanentă a platformei sale. PLATFORMA Y informează, de asemenea, utilizatorii în politica sa de confidențialitate cu privire la prelucrarea datelor cu caracter personal în scopul detectării trucurilor de jocuri, în conformitate cu cerințele prevăzute la art. 13 din RGPD.

La recepționarea cererii de acces a JUCĂTORULUI X, PLATFORMA Y ar trebui să furnizeze JUCĂTORULUI X o copie a datelor cu caracter personal prelucrate despre JUCĂTORUL X. În ceea ce privește motivul restricției contului, PLATFORMA Y ar trebui să confirme JUCĂTORULUI X că a decis să restricționeze accesul JUCĂTORULUI X la jocuri online din cauza utilizării unuia sau a unor trucuri de jocuri repetate care încalcă condițiile generale de utilizare. Pe lângă informațiile furnizate despre prelucrare în scopul detectării trucurilor de jocuri, PLATFORMA Y ar trebui să acorde JUCĂTORULUI X acces la informațiile pe care le-a stocat despre trucurile de jocuri ale JUCĂTORULUI X care au condus la impunerea restricției. În special, PLATFORMA Y ar trebui să furnizeze JUCĂTORULUI X informațiile care au condus la restricționarea contului (de exemplu, prezentarea generală a jurnalului, data și ora înșelăciunii, detectarea software-ului terțelor părți,...) pentru ca persoana vizată (adică JUCĂTORUL X) să verifice dacă prelucrarea datelor a fost corectă.

Cu toate acestea, conform art. 15(4) din RGPD și considerentului 63 din RGPD, PLATFORMA Y nu este obligată să dezvăluie nicio parte a funcționării tehnice a softului anti-cheat, chiar dacă aceste informații se referă la JUCĂTORUL X, atât timp cât acestea pot fi considerate secrete comerciale. Echilibrarea necesară a intereselor în temeiul art. 15(4) din RGPD va avea ca rezultat că secretele comerciale ale PLATFORMEI Y să împiedice dezvăluirea acestor date cu caracter personal, deoarece

cunoașterea funcționării tehnice a softului anti-cheat ar putea permite, de asemenea, utilizatorului să evite detectarea viitoare a trucurilor sau fraudelor. [99]

174. În cazul în care operatorii refuză să acționeze la o cerere de drept de acces în totalitate sau în parte conform art. 15(4) din RGPD, aceștia trebuie să informeze persoana vizată cu privire la motive fără întârziere și cel târziu în termen de o lună [art. 12(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. Acesta trebuie să includă informații despre posibilitatea de a depune o plângere la o autoritate de supraveghere (art. 77 din RGPD) și de a solicita căi de atac judiciare (art. 79 din RGPD).

6.3 Articolul 12(5) din RGPD

175. Articolul 12(5) din RGPD permite operatorilor să anuleze cererile de drept de acces care sunt vădit nefondate sau excesive. Aceste concepte trebuie interpretate în mod restrâns, deoarece principiile transparenței și drepturile persoanelor vizate la acces gratuit nu trebuie să fie subminate.

176. Operatorii trebuie să fie capabili să demonstreze persoanei fizice de ce consideră că cererea este vădit nefondată sau excesivă și, dacă li se solicită, să explice motivele autorității de supraveghere competente. Fiecare cerere ar trebui analizată de la caz la caz, în contextul în care este făcută, pentru a decide dacă este vădit nefondată sau excesivă.

6.3.1 Ce înseamnă vădit nefondată?

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

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

179. Alte cazuri în care aplicabilitatea art. 12(5) din RGPD este îndoielnică sunt cererile legate de informații sau activități de prelucrare care în mod clar și evident nu fac obiectul activităților de prelucrare ale operatorului.

Exemplul 38: O persoană vizată adresează o cerere către o autoritate municipală cu privire la datele care sunt prelucrate de o autoritate de stat. În loc să argumenteze că cererea este vădit nefondată, ar fi mai potrivit și mai ușor pentru autoritatea vizată să confirme că aceste date nu sunt prelucrate de

[99] Amploarea informațiilor furnizate persoanelor fizice va depinde în mare măsură de context, ținând cont de natura operatorului și de natura încălcării condițiilor de serviciu. În unele cazuri, este posibil ca operatorul să furnizeze informații de bază doar ca răspuns la o cerere de acces la care art. 15(4) se aplică.

către autoritate (prima componentă a art. 15 din RGPD: „dacă” datele cu caracter personal sunt în curs de prelucrare). [100]

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 impropriu.

6.3.2 Ce înseamnă excesivă?

181. Nu există o definiție a termenului „excesivă” în RGPD. Pe de o parte, formularea „în special din cauza caracterului lor repetitiv” din art. 12(5) din RGPD permite concluzia că principalul scenariu de aplicare a acestui membru în ceea ce privește art. 15 din RGPD este legat de numărul de cereri al 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 provoca caracterul excesiv.

182. Cu siguranță, conform art. 15(3) din RGPD cu privire la dreptul de a obține o copie, o persoană vizată poate depune mai multe cereri unui operator.[101] În cazul unor cereri care ar putea fi considerate excesive, evaluarea „caracterului excesiv” depinde de analiza efectuată de operator și de specificul sectorului în care își desfășoară activitatea.

183. În cazul cererilor ulterioare, trebuie să se evalueze dacă pragul de intervale rezonabile (a se vedea considerentul 63) a fost depășit sau nu. Operatorii trebuie să ia în considerare cu atenție circumstanțele particulare ale fiecărui caz.

184. De exemplu, în cazul rețelelor sociale, se va aștepta o modificare a setului de date la intervale mai scurte decât în cazul cadastrului sau al registrelor centrale de companii. În cazul asociaților de afaceri, trebuie luată în considerare frecvența contactelor cu clientul. Prin urmare, „intervalele rezonabile” în care persoanele vizate își pot exercita din nou dreptul de acces sunt, de asemenea, diferite. Cu cât apar mai des modificări în baza de date a operatorului, cu atât mai des li se poate permite persoanelor vizate să solicite acces la datele lor cu caracter personal, fără a fi excesiv. De altfel, o a doua cerere a 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, în lumina așteptărilor rezonabile ale persoanelor vizate:

- cât de des sunt modificate datele – este puțin probabil ca informațiile să se fi modificat între cereri? Dacă un grup de date nu este în mod evident supus unei alte prelucrări decât stocarea și persoana vizată este conștientă de acest lucru, de ex. din cauza unei cereri anterioare de drept de acces, aceasta ar putea fi un indiciu pentru o cerere excesivă;
- natura datelor – aceasta ar putea include dacă sunt deosebit de sensibile;
- scopurile prelucrării – acestea ar putea include dacă prelucrarea este susceptibilă de a fi în detrimentul (de a cauza prejudicii) solicitantului dacă este dezvăluită;

[100] O altă întrebare este dacă autoritatea căreia i-a fost adresată cererea de acces este îndreptățită să transmită cererea autorității de stat competente

[101] Conform propoziției a doua din art. 15(3), operatorul poate percepe o taxă rezonabilă pentru mai multe copii solicitate.

- dacă cererile ulterioare vizează același tip de informații sau activități de prelucrare sau altele diferite.[102]

Exemplul 39 (tâmplar): O persoană vizată depune cereri de acces la fiecare două luni la tâmplarul care i-a fabricat o masă. Tâmplarul a răspuns complet la prima cerere. Atunci când se decide dacă a trecut un interval rezonabil, ar trebui să se ia în considerare că tâmplarul doar ocazional (primul punct de mai sus) și nu ca parte a activității sale de bază prelucrează și colectează date cu caracter personal și este și mai puțin probabil ca tâmplarul să ofere adesea servicii către aceeași persoană vizată. Într-adevăr, în cazul dat, tâmplarul nu a furnizat mai mult de un serviciu persoanei vizate făcând improbabil ca setul de date ce privește persoana vizată să fi fost modificat. În special, având în vedere natura și cantitatea datelor cu caracter personal prelucrate, riscurile legate de prelucrare pot fi considerate ca fiind reduse (al doilea punct de mai sus), întrucât scopul prelucrării (scopurile de facturare și respectarea obligației de păstrare a evidenței) nu este de natură să provoace prejudicii persoanei vizate (al treilea punct de mai sus). În plus, cererea se referă la aceleași informații ca și ultima cerere (al patrulea punct de mai sus). Astfel de cereri pot fi, în consecință, considerate excesive dat fiind caracterul repetitiv al acestora.

Exemplul 40 (platformă de social media): O platformă de social media a cărei activitate principală este colectarea și/sau prelucrarea datelor cu caracter personal ale persoanei vizate desfășoară activități de prelucrare complexe și continue la scară largă. O persoană vizată care utilizează serviciile platformei depune cereri de acces la fiecare trei luni. În acest caz, sunt foarte probabile modificări frecvente ale datelor cu caracter personal ce privesc persoana vizată (primul punct de mai sus), gama largă de date colectate include date cu caracter personal sensibile deduse (al doilea punct de mai sus) prelucrate în scopul de a afișa conținut relevant și membrii rețelei către persoana vizată (al treilea punct). Solicitările de acces la fiecare trei luni pot – în aceste circumstanțe – în principiu să nu fie considerate excesive din cauza repetitivității.

Exemplul 41 (agenții de credit): La fel ca în cazul rețelelor sociale, nu poate fi exclus ca modificări ale datelor relevante deținute de agențiile de credit să aibă loc la intervale mult mai scurte decât în alte domenii (primul punct de mai sus). Acest lucru rezultă din numeroși factori de care persoana vizată, în calitate de persoană din afară, nu este de obicei la curent din cauza complexității modelului de afaceri. Răspunsul la întrebarea ce tipuri de date au fost colectate pentru un calcul al valorii scorului de către operator și care sunt incluse în prezent în calcul poate fi, prin urmare, furnizat doar de însăși agenția de credit. În plus, prelucrarea datelor prin agenții de credit și valoarea scorului rezultată pot avea consecințe de amploare pentru persoana vizată în ceea ce privește tranzacțiile juridice preconizate, cum ar fi încheierea contractelor de cumpărare, închiriere sau leasing (al treilea punct de mai sus).

Nu este posibil să se determine, în general, un interval specific în care depunerea unei cereri de acces ulterioare ar putea fi considerată excesivă în temeiul art. 12(5) propoziția a doua din RGPD. Este mai degrabă necesară o analiză generală a circumstanțelor cazului individual. Cu 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 gratuit va fi în orice caz prea mare pentru ca cererea să fie considerată excesivă. Dacă o cerere este depusă într-un interval foarte scurt, factorul decisiv ar trebui să fie dacă persoana vizată are motive să presupună că informațiile sau prelucrarea s-au schimbat de la ultima cerere. De exemplu, dacă persoana vizată a efectuat o

[102] Dacă cererea ulterioară se referă la același tip de informații în sfera de aplicare ȘI timp, aceasta nu este o chestiune de excesivitate, ci o chestiune de solicitare a unei copii suplimentare, a se vedea secțiunea 2.2.2.2.

tranzacție financiară, cum ar fi luarea unui împrumut, persoana vizată ar trebui să aibă dreptul de a cere acces la informațiile despre credit, chiar dacă o astfel de solicitare a fost depusă și i s-a răspuns cu puțin timp înainte.

186. Atunci când este posibilă furnizarea cu ușurință a informațiilor prin mijloace electronice sau prin acces de la distanță la un sistem securizat, ceea ce înseamnă că îndeplinirea unor astfel de cereri de fapt nu pune la îndoială operatorul, 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 suprapusă poate fi, în general, considerată excesivă, dacă și în măsura în care acoperă exact aceleași activități de informare sau prelucrare și cererea anterioară nu este încă îndeplinită de operator fără a ajunge la statutul de „întârziere nejustificată" [a se vedea art. 12(3) din RGPD]. În practică, ca rezultat, ambele cereri ar putea fi combinate.

188. Faptul că operatorului i-ar lua timp și efort semnificativ pentru a furniza informațiile sau copia persoanei vizate nu poate, de la sine, face o cerere excesivă. [103] Un număr mare de activități de prelucrare implică de obicei eforturi mai mari atunci când se conformează cu cererile de acces. Cu toate acestea, după cum s-a menționat mai sus, în anumite circumstanțe, cererile pot fi considerate excesive din alte motive decât caracterul lor repetitiv. În opinia CEPD, aceasta include în special cazurile de invocare abuzivă a art. 15 din RGPD, care sunt cazuri în care persoanele vizate folosesc în mod excesiv dreptul de acces cu singura intenție de a provoca daune sau prejudicii operatorului.

189. În acest context, o cerere nu trebuie considerată excesivă pe motiv că:

- persoana vizată nu oferă motivele cererii sau operatorul consideră cererea ca lipsită de sens;
- persoana vizată recurge la limbaj impropriu sau nepoliticos;
- persoana vizată intenționează să folosească datele pentru a depune reclamații suplimentare împotriva operatorului.[104]

190. Pe de altă parte, o cerere poate fi considerată excesivă, de exemplu, dacă:

- o persoană fizică depune o cerere, dar în același timp oferă să o retragă în schimbul unei forme de beneficii din partea operatorului sau
- cererea are intenție malefică și este folosită pentru a hărțui operatorul sau angajații săi fără alte scopuri decât pentru a provoca perturbări, de exemplu pe baza faptului că:

  persoana fizică a declarat în mod explicit, în cererea însăși sau în alte comunicări, că intenționează să provoace perturbări și nimic altceva; sau

[103] Fără test de proporționalitate, a se vedea mai sus alin. 166.

[104] Acest lucru nu aduce atingere oricărei legi naționale aplicabile care respectă cerințele prevăzute de art. 23 din RGPD, a se vedea capitolul 6.4.

persoana fizică trimite sistematic diferite cereri unui operator ca parte a unei campanii, de ex. o dată pe săptămână, cu intenția și efectul de a provoca perturbări.[105][106][107]. .

6.3.3 Consecințe

191. În cazul unei cereri a dreptului de acces vădit nefondate sau excesive operatorii pot, conform art. 12(5) din RGPD, fie percepe o taxă rezonabilă (ținând cont de costurile administrative ale furnizării de informații sau comunicării sau luării măsurii solicitate), fie refuza satisfacerea cererii.

192. CEPD subliniază că operatorii – pe de o parte – nu sunt în general obligați să perceapă o taxă rezonabilă înainte de a refuza să acționeze la o cerere. Pe de altă parte, ei nu sunt complet liberi să aleagă între cele două alternative. De fapt, operatorii trebuie să ia o decizie corespunzătoare în funcție de circumstanțele specifice ale cazului. Întrucât este greu de imaginat că perceperea unei taxe rezonabile este o măsură corespunzătoare în cazul cererilor vădit nefondate, pentru cereri excesive – în conformitate cu principiul transparenței – va fi adesea mai potrivit să se perceapă o taxă pentru compensare pentru costurile administrative pe care cererile repetitive le provoacă.

193. Operatorii trebuie să poată demonstra caracterul vădit nefondat sau excesiv al unei cereri [art. 12(5), propoziția a treia din RGPD]. Prin urmare, se recomandă să se asigure o documentare corespunzătoare a faptelor subiacente. În conformitate cu art. 12(4) din RGPD, în cazul în care operatorii refuză să acționeze la o cerere de acces, în totalitate sau în parte, aceștia trebuie să informeze persoana vizată fără întârziere și în cel mult o lună de la primirea cererii despre

- motivul,
- dreptul de a depune o plângere la o autoritate de supraveghere,
- posibilitatea de a solicita o cale de atac judiciară.

194. Înainte de a percepe o taxă rezonabilă în temeiul art. 12(5) din RGPD, operatorii ar trebui să furnizeze persoanelor vizate o indicație cu privire la planul lor de a face acest lucru. Aceștia din urmă trebuie să poată decide dacă vor să își retragă cererea pentru a evita taxarea.

195. Respingerile nejustificate ale cererilor de drept de acces pot fi considerate încălcări ale drepturilor persoanelor vizate în temeiul art. 12-22 din RGPD și, prin urmare, pot face obiectul exercitării competențelor corective de către autoritățile de supraveghere competente, inclusiv amenzilor administrative în temeiul art. 83(5)(b) din RGPD. În cazul în care persoanele vizate consideră că există o încălcare a drepturilor acestora, acestea au dreptul să depună o plângere în temeiul art. 77 din RGPD.

6.4 Posibile restricții în legislația Uniunii sau a statelor membre în temeiul articolului 23 din RGPD și derogărilor

196. Sfera obligațiilor și drepturilor prevăzute la art. 15 din RGPD poate fi restricționată prin măsuri legislative în legislația Uniunii sau a statelor membre [106].

[105] „Transmiterea sistematică ca parte a unei campanii" înseamnă că solicitările care ar putea fi combinate cu ușurință într-una sunt împărțite artificial nu doar în câteva, ci în multe părți unice de către persoana vizată, cu intenția aparentă de a provoca perturbări.

106

107

197. Operatorii care intenționează să mizeze pe o restricție bazată pe legislația națională trebuie să verifice cu atenție cerințele prevederii legislației naționale respective. În plus, este important de menționat că restricțiile dreptului de acces în dreptul statelor membre (sau al Uniunii) care se bazează pe art. 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 se referă la restricțiile prevăzute la art. 23 din RGPD pot prevedea, de asemenea, că exercitarea unui drept este întârziată în timp, că un drept este exercitat parțial sau circumscris anumitor categorii de date sau că un drept poate fi exercitat indirect printr-o autoritate de supraveghere independentă.

---

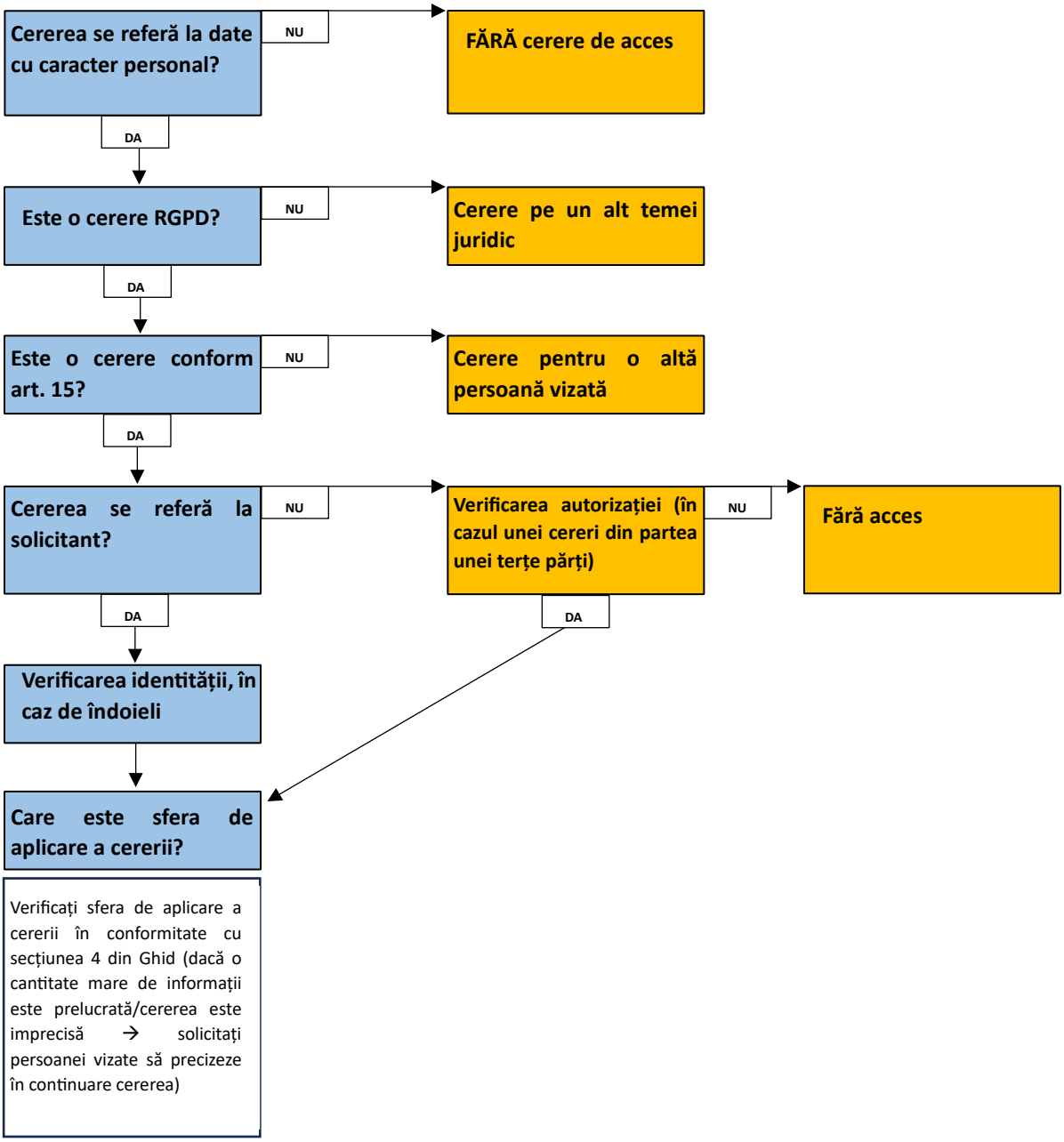
[106] A se vedea, de exemplu, secțiunile 32 până la 37 din Legea federală germană privind protecția datelor (BDSG), secțiunile 16 și 17 din Legea norvegiană privind datele cu caracter personal și capitolul 5 din Legea suedeză privind protecția datelor.

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

[108] Alineatul 12 din Orientările 10/2020 privind restricțiile în temeiul articolului 23 din RGPD, versiunea 2.0, adoptată la 13 octombrie 2021. Secțiunea 34 (3) din Legea federală germană privind protecția datelor, de exemplu, prevede că, dacă o autoritate publică nu furnizează informații unei persoane vizate care respectă o cerere de drept de acces în contextul anumitor restricții, astfel de informații vor fi furnizate autorității federale de supraveghere la cererea persoanei vizate, cu excepția cazului în care autoritatea federală supremă responsabilă (a autorității care a făcut obiectul solicitării) stabilește, în cazul individual, că acest lucru ar pune în pericol securitatea Federației sau a unui Land. Codul DPC italian prevede acces indirect (prin autoritate) în cazul în care accesul ar putea avea consecințe negative asupra unui număr de interese (de exemplu, interes pentru a contrasta spălarea banilor) a se vedea art. 2-L din Codul italian PD.

ANEXĂ – DIAGRAMĂ

Pasul 1: Cum se interpretează și se evaluează cererea?



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

3 componente principale ale dreptului de acces (structura art. 15)		
Confirmare dacă sunt sau nu prelucrate date cu caracter personal	Acces la datele cu caracter personal	Informații suplimentare cu privire la scopuri, destinatari etc. [art. 15(1)(a) – h)]

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

Luați măsurile corespunzătoare

Articolul 12(1): concis, transparent, inteligibil, ușor accesibil

Articolul 12(2): facilitați exercitarea dreptului de acces

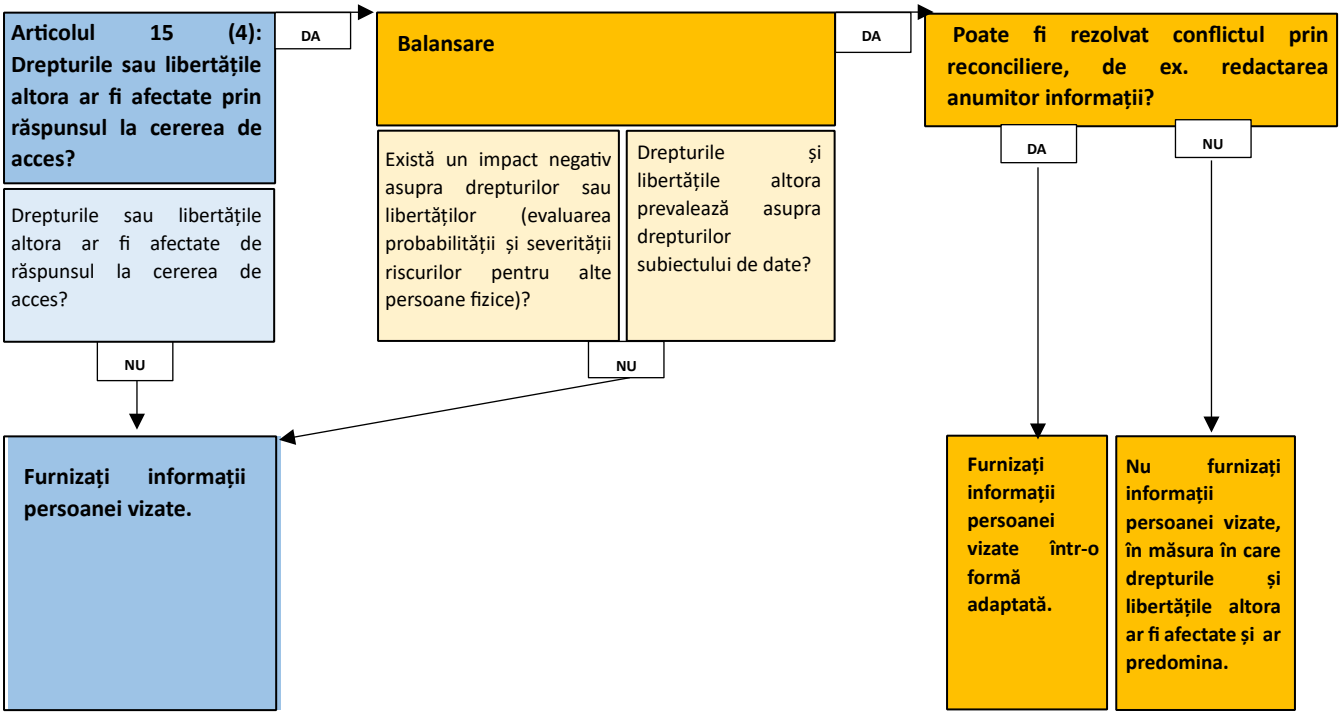
Alegeți între diferite mijloace	Furnizați o copie, dacă nu s-a convenit altfel [art. 15(3)]	Folosiți o abordare stratificată, dacă este cazul (cel mai relevantă în contextul online)	Termenul – fără întârzieri nejustificate, în orice caz în termen de o lună (prelungire cu încă două luni în cazuri excepționale) [art. 12(3)]

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

Cum poate operatorul să preia toate datele despre persoana vizată?

Definiți criteriile de căutare – pe baza a ceea ce persoana vizată a furnizat, alte informații pe care operatorul le deține despre persoana vizată și factorii pe care sunt structurate datele (de exemplu, numărul clientului, adresele IP, titlul profesional, relațiile de familie etc.).	Identificați orice funcții tehnice care pot fi disponibile pentru a prelua date.	Căutați prin toate sistemele de arhivare IT sau non-IT relevante.	Compilați, extrageți sau colectați în alt mod date care se referă la persoana vizată într-un mod care să reflecte pe deplin prelucrarea, adică să includă toate datele cu caracter personal ce privesc persoana vizată și să permită persoanei vizate să cunoască și să verifice legalitatea prelucrării. Preluarea informațiilor se poate face de la caz la caz sau, atunci când este relevant, prin utilizarea unui instrument de confidențialitate prin concepție deja implementat de către operator.

Pasul 3: Verificarea limitelor și restricțiilor (1)



Pasul 3: Verificarea limitelor și restricțiilor (2)