



Orientări privind dreptul la portabilitatea datelor

**Adoptate la 13 decembrie 2016
Astfel cum au fost revizuite și adoptate ultima dată la 5 aprilie 2017**

Acest grup de lucru a fost constituit în temeiul articolului 29 din Directiva 95/46/CE. Acesta este un organ european privind protecția datelor și a vieții private cu rol consultativ și statut independent. Atribuțiile sale sunt descrise la articolul 30 din Directiva 95/46/CE și la articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de Direcția C (Drepturi fundamentale și statul de drept) din cadrul Comisiei Europene, Direcția Generală Justiție și Consumatori, B-1049 Bruxelles, Belgia, Nr. birou MO59 05/35

Site: http://ec.europa.eu/justice/data-protection/index_en.htm

CUPRINS

Rezumat 3

I.	Introducere	3
II.	Care sunt principalele elemente ale portabilității datelor?	4
III.	Când se aplică portabilitatea datelor?	9
IV.	Cum se aplică regulile generale care reglementează exercitarea drepturilor persoanei vizate în cazul portabilității datelor?	14
V.	Cum trebuie să fie furnizate datele portabile?	17

Rezumat

Articolul 20 din RGPD creează un nou drept la portabilitatea datelor, care este strâns legat de dreptul de acces, însă diferit de acesta în multe moduri. Acesta permite persoanelor vizate să primească datele cu caracter personal pe care le-au furnizat unui operator într-un format structurat, utilizat în mod curent și prelucrabil automat, și să transmită datele respective unui alt operator. Scopul acestui nou drept este de a capacita persoana vizată și de a-i oferi acesteia mai mult control asupra datelor cu caracter personal care o privesc.

Deoarece permite transmiterea directă a datelor cu caracter personal de la un operator la altul, dreptul la portabilitatea datelor este totodată un instrument important care va susține libera circulație a datelor cu caracter personal în UE și va promova concurența între operatori. Aceasta va facilita schimbarea diferiților furnizori de servicii și, prin urmare, va stimula dezvoltarea de noi servicii în contextul strategiei privind piața unică digitală.

Prezentul aviz oferă îndrumări cu privire la interpretarea și punerea în aplicare a dreptului la portabilitatea datelor, astfel cum a fost introdus de RGPD. Obiectivul acestuia este de a aborda dreptul la portabilitatea datelor și domeniul său de aplicare. Acesta oferă o clarificare cu privire la condițiile în care se aplică acest nou drept ținând seama de temeiul juridic al prelucrării datelor (fie consimțământul persoanei vizate, fie necesitatea de a executa un contract) și de faptul că acest drept este limitat la datele cu caracter personal furnizate de persoana vizată. Avizul prezintă, de asemenea, exemple concrete și criterii pentru a explica împrejurările în care se aplică acest drept. În această privință, GL29 consideră că dreptul la portabilitatea datelor vizează datele furnizate cu bună știință și în mod activ de către persoana vizată, precum și datele cu caracter personal generate de activitatea acesteia. Acest nou drept nu poate fi subminat și limitat la informații cu caracter personal comunicate în mod direct de către persoana vizată, de exemplu, într-un formular on-line.

Ca exemplu de bună practică, operatorii ar trebui să înceapă să dezvolte mijloacele care vor contribui la soluționarea solicitărilor privind portabilitatea datelor, cum ar fi instrumente de descărcare și interfețe de programare a aplicațiilor. Aceștia ar trebui să garanteze transmiterea datelor cu caracter personal într-un format structurat, utilizat în mod curent și prelucrabil automat și ar trebui să fie încurajați să asigure interoperabilitatea formatului datelor pus la dispoziție în cadrul unei solicitări privind portabilitatea datelor.

Avizul îi ajută, de asemenea, pe operatori să înțeleagă în mod clar obligațiile ce le revin și recomandă cele mai bune practici și instrumente care susțin respectarea dreptului la portabilitatea datelor. În sfârșit, avizul recomandă părților interesate din industrie și organismelor profesionale să lucreze împreună pentru a elabora un set comun de standarde și formate interoperabile pentru a îndeplini cerințele asociate dreptului la portabilitatea datelor.

I. Introducere

Articolul 20 din Regulamentul general privind protecția datelor (RGPD) introduce un nou drept la portabilitatea datelor. Acest drept permite persoanelor vizate să primească datele cu

caracter personal pe care le-au furnizat unui operator într-un format structurat, utilizat în mod curent și prelucrabil automat, și să transmită datele respective unui alt operator fără obstacole. Acest drept, care supune persoana vizată anumitor condiții, sprijină alegerea pentru utilizatori, controlul de către utilizatori și capacitatea utilizatorilor.

Persoanele care își exercită dreptul de acces în temeiul Directivei 95/46/CE privind protecția datelor au fost limitați de formatul ales de operator la furnizarea informațiilor solicitate. **Noul drept la portabilitatea datelor are obiectivul de a capacita persoanele vizate în privința propriilor lor date cu caracter personal, întrucât facilitează capacitatea acestora de a muta, a copia sau a transmite cu ușurință date cu caracter personal dintr-un mediu informatic în altul** (în sistemele proprii, în sistemele unor terți de încredere sau în cele ale unor operatori noi).

Prin afirmarea drepturilor personale ale persoanelor și exercitarea controlului asupra datelor cu caracter personal care le privesc, portabilitatea datelor reprezintă, de asemenea, oportunitatea de a „reechilibra” relația dintre persoanele vizate și operatori¹.

Chiar dacă dreptul la portabilitatea datelor cu caracter personal ar putea conduce la creșterea concurenței între servicii (prin facilitarea schimbării furnizorului de servicii), RGPD reglementează datele cu caracter personal, nu concurența. În mod specific, articolul 20 nu limitează datele portabile la acelea care sunt necesare sau utile pentru schimbarea furnizorului de servicii².

Cu toate că portabilitatea datelor este un nou drept, există deja sau sunt în curs de a fi discutate și alte tipuri de portabilitate în alte domenii ale legislației (de exemplu, în contextul rezilierii contractului, al serviciilor de comunicații în roaming și al accesului transfrontalier la servicii³). Este posibil să apară unele sinergii, și chiar beneficii, pentru persoane între diferitele tipuri de portabilitate dacă acestea sunt asigurate în cadrul unei abordări combinate, chiar dacă analogiile ar trebui tratate cu precauție.

Prezentul aviz oferă orientări pentru operatori, astfel încât aceștia să poată să își actualizeze practicile, procesele și politicile, și clarifică sensul portabilității datelor pentru a permite persoanelor vizate să beneficieze în mod eficient de noul lor drept.

II. Care sunt principalele elemente ale portabilității datelor?

RGPD definește dreptul la portabilitatea datelor la articolul 20 alineatul (1), după cum urmează:

Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără

¹ Obiectivul principal al portabilității datelor este sporirea controlului persoanelor asupra datelor lor cu caracter personal și asigurarea faptului că acestea au un rol activ în ecosistemul de date.

² De exemplu, acest drept ar putea permite băncilor să ofere servicii suplimentare, sub controlul utilizatorului, folosind date cu caracter personal colectate inițial în cadrul unui serviciu de furnizare de energie.

³ A se vedea agenda Comisiei Europene pentru o piață unică digitală: <https://ec.europa.eu/digital-agenda/en/digital-single-market>, în special, primul pilon de politică intitulat „Ameliorarea accesului online la bunuri și servicii”.

obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal [...]

- **Dreptul de a primi date cu caracter personal**

În primul rând, portabilitatea datelor constituie **un drept al persoanei vizate de a primi un subset de date cu caracter personal** prelucrate de către un operator cu privire la aceasta și de a stoca datele respective pentru uz personal în viitor. În acest context, stocarea poate fi realizată pe un dispozitiv privat sau un sistem cloud privat, fără a transmite neapărat datele unui alt operator.

În această privință, portabilitatea datelor completează dreptul de acces. Una dintre particularitățile portabilității datelor constă în faptul că aceasta oferă persoanelor vizate o modalitate simplă de gestionare și reutilizare a propriilor date cu caracter personal. Aceste date ar trebui să fie primite „*într-un format structurat, utilizat în mod curent și prelucrabil automat*”. De exemplu, o persoană vizată ar putea fi interesată să obțină lista curentă de piese ascultate (sau istoricul pieselor ascultate) de la un serviciu de redare de muzică în flux continuu, pentru a afla de câte ori a ascultat anumite melodii sau a verifica ce muzică dorește să cumpere sau să asculte pe o altă platformă. În mod similar, aceasta ar putea dori, de asemenea, să obțină lista de contacte de pe aplicația de webmail, de exemplu, pentru a întocmi o listă de invitați la o nuntă sau pentru a obține informații despre achiziții realizate cu diferite carduri de fidelitate sau pentru a-și evalua amprenta de carbon⁴.

- **Dreptul de transmitere a datelor cu caracter personal de la un operator la alt operator**

În al doilea rând, articolul 20 alineatul (1) acordă persoanelor vizate **dreptul de a transmite date cu caracter personal de la un operator la alt operator** „fără obstacole”. De asemenea, datele pot să fie transmise direct de la un operator la altul la cererea persoanei vizate și în cazul în care acest lucru este fezabil din punct de vedere tehnic [articolul 20 alineatul (2)]. În acest sens, considerentul 68 încurajează operatorii să dezvolte formate interoperabile care să permită portabilitatea datelor⁵, însă fără a crea o obligație pentru operatori de a adopta sau de a întreține sisteme de prelucrare care să fie compatibile din punct de vedere tehnic⁶. Însă RGPD interzice operatorilor să introducă obstacole în calea transmiterii.

În esență, acest element al portabilității datelor oferă persoanelor vizate posibilitatea nu doar de a obține și a reutiliza, ci și de a transmite datele pe care acestea le-au pus la dispoziția unui alt prestator de servicii (fie în același domeniu de activitate, fie într-un domeniu diferit). În plus față de capacitatea consumatorilor prin prevenirea riscului de blocaj, dreptul la portabilitatea datelor este prevăzut a promova oportunități de inovare și schimbul de date cu

⁴ În aceste cazuri, prelucrarea efectuată pe baza datelor de către persoana vizată poate intra în domeniul de aplicare al activităților casnice, atunci când întregul proces de prelucrare are loc sub controlul exclusiv al persoanei vizate, sau poate fi gestionată de o altă parte, în numele persoanei vizate. În acest din urmă caz, cealaltă parte ar trebui să fie considerată drept operator, chiar și numai în scopul de stocare a datelor cu caracter personal, și să respecte principiile și obligațiile prevăzute în RGPD.

⁵ A se vedea, de asemenea, secțiunea V.

⁶ În consecință, ar trebui să se acorde o atenție deosebită formatului datelor transmise, astfel încât să se garanteze reutilizarea datelor, cu puține eforturi, de către persoana vizată sau un alt operator. A se vedea, de asemenea, secțiunea V.

caracter personal între operatori în condiții de siguranță și securitate, sub controlul persoanei vizate⁷. Portabilitatea datelor poate să promoveze schimbul controlat și limitat de către utilizatori de date cu caracter personal între organizații și, astfel, să îmbogățească serviciile și experiența clienților⁸. Portabilitatea datelor poate facilita transmiterea și reutilizarea datelor cu caracter personal privind utilizatorii în rândul diferitelor servicii care îi interesează.

⁷ A se vedea mai multe aplicații experimentale din Europa, spre exemplu [MiData](#) în Regatul Unit, [MesInfos / SelfData](#) de către FING în Franța.

⁸ Așa-numita industrie „quantified self” și cea a internetului obiectelor au demonstrat beneficiile (și riscurile) asociate conectării datelor personale din diferite aspecte ale vieții unei persoane, precum fitnessul, activitatea și aportul caloric pentru a oferi o imagine mai completă din viața unei persoane într-un singur dosar.

- Activitatea operatorului

Portabilitatea datelor garantează dreptul de a primi date cu caracter personal și de a le prelucra conform intențiilor persoanei vizate⁹.

Operatorii răspund solicitărilor de portabilitate a datelor în condițiile prevăzute la articolul 20, nu poartă răspunderea pentru prelucrarea gestionată de către persoana vizată sau de către o altă societate care primește date cu caracter personal. Aceștia acționează în numele persoanei vizate, inclusiv în cazul în care datele cu caracter personal sunt transmise direct unui alt operator. În acest sens, operatorul nu poartă răspunderea pentru conformitatea operatorului beneficiar cu legislația în materie de protecție a datelor, având în vedere că nu operatorul trimițător este cel care alege beneficiarul. În același timp, operatorul ar trebui să stabilească garanții pentru a se asigura că acționează cu adevărat în numele persoanei vizate. Spre exemplu, acesta poate să instituie proceduri pentru a se asigura că tipul de date cu caracter personal transmise sunt într-adevăr cele pe care persoana vizată dorește să le transmită. Acest lucru ar putea fi realizat prin obținerea confirmării din partea persoanei vizate, fie înainte de transmitere, fie mai devreme cu privire la momentul în care este acordat consimțământul inițial pentru prelucrare sau în care este încheiat contractul.

Operatorii care răspund unei solicitări de portabilitate a datelor nu au obligația specifică de a verifica și controla calitatea datelor înainte de transmiterea acestora. Desigur, aceste date ar trebui să fie deja corecte și actualizate în conformitate cu principiile enunțate în articolul 5 alineatul (1) din RGPD. În plus, portabilitatea datelor nu impune operatorului obligația de a păstra date cu caracter personal mai mult decât este necesar sau în afara oricărei perioade de păstrare specificate¹⁰. Este important faptul că nu există nicio cerință suplimentară de păstrare a datelor în afara perioadelor de păstrare aplicabile în alte condiții doar pentru a servi oricărei posibile solicitări viitoare de portabilitate a datelor.

În cazul în care datele cu caracter personal sunt prelucrate de o persoană împuternicită de către operator, contractul încheiat în conformitate cu articolul 28 din RGPD trebuie să includă obligația de a oferi asistență „operatorului prin măsuri tehnice și organizatorice adecvate (...) de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute”. Operatorul ar trebui, prin urmare, să pună în aplicare proceduri specifice în cooperare cu persoanele sale împuternicite pentru a răspunde cererilor de portabilitate a datelor. În cazul exercitării controlului comun, ar trebui să existe un contract care să repartizeze în mod clar responsabilitățile între fiecare operator în ceea ce privește prelucrarea cererilor de portabilitate a datelor.

În plus, un operator beneficiar¹¹ are responsabilitatea de a se asigura că datele portabile furnizate sunt relevante și nu excesive în ceea ce privește noua acțiune de prelucrare a datelor. De exemplu, în cazul unei cereri de portabilitate a datelor adresate unui serviciu de webmail, atunci când cererea este utilizată de persoana vizată pentru a obține mesaje prin poșta electronică și a le trimite pe o platformă de arhivare securizată, nu este nevoia ca noul operator să prelucreze datele de contact ale corespondenților persoanei vizate. Dacă aceste

⁹ Dreptul la portabilitatea datelor nu se limitează la datele cu caracter personal care sunt utile și relevante pentru servicii similare furnizate de concurenții operatorului.

¹⁰ În exemplul de mai sus, în cazul în care operatorul nu păstrează o evidență a cântecele redade de către un utilizator, aceste date cu caracter personal nu pot fi incluse într-o cerere de portabilitate a datelor.

¹¹ și anume, cel care primește date cu caracter personal în urma unei cereri de portabilitate a datelor adresate de către persoana vizată unui alt operator.

informații nu sunt relevante sub aspectul scopului noii acțiuni de prelucrare, acestea nu ar trebui să fie păstrate și prelucrate. În orice caz, operatorii beneficiari nu sunt obligați să accepte și să prelucreze date cu caracter personal transmise în urma unei cereri de portabilitate a datelor. În mod similar, în cazul în care o persoană vizată solicită transmiterea unor detalii privind tranzacțiile sale bancare unui serviciu care îi oferă acesteia asistență în gestionarea bugetului său, nu este nevoie ca operatorul beneficiar să accepte toate datele sau să rețină toate detaliile tranzacțiilor odată ce acestea au fost etichetate în scopul noului serviciu. Cu alte cuvinte, ar trebui să fie acceptate și păstrate doar datele care sunt necesare și relevante pentru serviciul care este prestat de operatorul beneficiar,

O organizație „beneficiară” devine un nou operator cu privire la aceste date cu caracter personal și trebuie să respecte principiile enunțate în articolul 5 din RGPD. Prin urmare, „noul” operator beneficiar trebuie să precizeze în mod clar și direct scopul noii prelucrări înaintea oricărei cereri de transmitere a datelor portabile, în conformitate cu cerințele de transparență prevăzute la articolul 14¹². Ca și în cazul oricăror alte acțiuni de prelucrare a datelor desfășurate sub responsabilitatea sa, operatorul ar trebui să aplice principiile prevăzute la articolul 5, cum ar fi legalitatea, corectitudinea și transparența, limitarea scopului, reducerea la minimum a datelor, precizia, integritatea și confidențialitatea, limita de stocare și responsabilitatea¹³.

Operatorii care dețin date cu caracter personal ar trebui să fie pregătiți să faciliteze dreptul la portabilitatea datelor al persoanei lor vizate. De asemenea, operatorii pot să aleagă să accepte date de la o persoană vizată, însă nu au această obligație.

- **Portabilitatea datelor comparativ cu alte drepturi ale persoanelor vizate**

Atunci când o persoană își exercită dreptul la portabilitatea datelor această exercitare nu aduce atingere vreunui alt drept (așa cum este cazul oricărui alt drept din RGPD). O persoană vizată poate utiliza și beneficia în continuare de serviciile operatorului, chiar și după încheierea unei operațiuni de portabilitate a datelor. Portabilitatea datelor nu atrage după sine în mod automat ștergerea datelor¹⁴ provenite din sistemele operatorului și nu afectează perioada inițială de păstrare valabilă pentru datele care au fost transmise. Persoana vizată își poate exercita drepturile atâta timp cât operatorul se află încă în curs de prelucrare a datelor,

De asemenea, dacă persoana vizată dorește să își exercite dreptul la ștergerea datelor („dreptul de a fi uitat”, în temeiul articolului 17), un operator nu se poate prevala de portabilitatea datelor pentru a întârzia sau a refuza o astfel de ștergere.

În cazul în care o persoană vizată descoperă că datele cu caracter personal solicitate în temeiul dreptului la portabilitatea datelor nu îi satisfac pe deplin cererea, ar trebui să se respecte pe

¹² În plus, noul operator nu ar trebui să prelucreze date cu caracter personal care nu sunt relevante, iar prelucrarea trebuie să fie limitată la ceea ce este necesar pentru noile scopuri, chiar și în cazul în care datele cu caracter personal fac parte dintr-un set de date transmise la un nivel mai global printr-un proces de portabilitate. Datele cu caracter personal care nu sunt necesare pentru atingerea scopului noii acțiuni de prelucrare ar trebui să fie eliminate cât mai curând posibil.

¹³ Odată primite de către operator, datele cu caracter personal transmise în cadrul dreptului la portabilitatea datelor pot fi considerate ca fiind „furnizate de” persoana vizată și retransmise în conformitate cu dreptul la portabilitatea datelor, în măsura în care sunt îndeplinite celelalte condiții care se aplică acestui drept (și anume, temeiul juridic al prelucrării ...).

¹⁴ astfel cum se menționează la articolul 17 din RGPD.

deplin orice nouă cerere de date cu caracter personal în temeiul unui drept de acces, în conformitate cu articolul 15 din RGPD.

În plus, în cazul în care legislația unui anumit stat european sau stat membru dintr-un alt domeniu prevede, de asemenea, o formă de portabilitate a datelor în cauză, condițiile prevăzute în aceste legi specifice trebuie să fie, de asemenea, luate în considerare atunci când se soluționează o cerere de portabilitate a datelor în temeiul RGPD. În primul rând, dacă reiese în mod clar din cererea depusă de persoana vizată că intenția sa nu este de a exercita drepturi în temeiul RGPD, ci, mai degrabă, de a exercita drepturi doar în conformitate cu legislația sectorială, dispozițiile RGPD privind portabilitatea datelor nu se vor aplica în cazul acestei cereri¹⁵. Dacă, pe de altă parte, cererea vizează portabilitatea în temeiul RGPD, existența unei astfel de legislații specifice nu anulează aplicarea generală a principiului portabilității datelor în cazul tuturor operatorilor, astfel cum este prevăzut în RGPD. În schimb, trebuie să se verifice, de la caz la caz, cum ar putea o astfel de legislație specifică să afecteze dreptul la portabilitatea datelor, dacă este cazul.

III. Când se aplică portabilitatea datelor?

- Ce operațiuni de prelucrare sunt vizate de dreptul la portabilitatea datelor?

Conformitatea cu RGPD impune operatorilor să aibă un temei juridic clar pentru prelucrarea datelor cu caracter personal.

În conformitate cu articolul 20 alineatul (1) litera (a) din RGPD, **pentru a se încadra în domeniul de aplicare al portabilității datelor**, operațiunile de prelucrare trebuie să se bazeze:

- fie pe consimțământul persoanei vizate [în temeiul articolului 6 alineatul (1) litera (a) sau al articolului 9 alineatul (2) litera (a) în cazul în care este vorba de categorii speciale de date cu caracter personal];
- fie pe un contract la care persoana vizată este parte în conformitate cu articolul 6 alineatul (1) litera (b).

De pildă, titlurile de cărți cumpărate de către o persoană dintr-o librărie online sau melodiile ascultate prin intermediul unui serviciu de redare de muzică online sunt exemple de date cu caracter personal care intră, în general, în domeniul de aplicare al portabilității datelor, deoarece sunt prelucrate în cadrul executării unui contract la care persoana vizată este parte.

RGPD nu stabilește un drept general la portabilitatea datelor în cazurile în care prelucrarea datelor cu caracter personal nu este întemeiată pe consimțământ sau efectuată în baza unui contract¹⁶. De exemplu, instituțiile financiare nu au nicio obligație de a răspunde unei cereri

¹⁵ De exemplu, dacă cererea persoanei vizate este prevăzută în mod specific să ofere acces la istoricul contului său bancar unui prestator de servicii de informare despre conturi, în scopurile menționate în Directiva privind serviciile de plată 2 (DSP 2), un astfel de acces ar trebui acordat în conformitate cu dispozițiile acestei directive.

¹⁶ A se vedea considerentul 68 și articolul 20 alineatul (3) din RGPD. Articolul 20 alineatul (3) și considerentul 68 prevăd că portabilitatea datelor nu se aplică atunci când prelucrarea datelor este necesară pentru îndeplinirea unei sarcini executate în interesul public sau în exercitarea unei autorități oficiale cu care este investit operatorul, sau atunci când un operator își exercită atribuțiile publice sau respectă o obligație juridică. Prin urmare,

de portabilitate a datelor care vizează datele cu caracter personal prelucrate ca parte a obligației lor de a preveni și a depista spălarea de bani și alte infracțiuni financiare; de asemenea, portabilitatea datelor nu include datele de contact profesionale prelucrate în relațiile business-to-business în cazurile în care prelucrarea nu este nici întemeiată pe consimțământul persoanei vizate, nici efectuată în baza unui contract la care aceasta este parte.

Când este vorba despre datele angajaților, dreptul la portabilitatea datelor se aplică, de regulă, doar în cazul în care prelucrarea este efectuată în baza unui contract la care persoana vizată este parte. În multe cazuri, consimțământul nu va fi considerat a fi dat în mod liber în acest context, având în vedere dezechilibrul de la nivelul puterii între angajator și angajat¹⁷. În schimb, unele acțiuni de prelucrare în domeniul resurselor umane se întemeiază pe criteriul juridic al unui interes legitim sau sunt necesare pentru asigurarea conformității cu obligațiile legale specifice în domeniul ocupării forței de muncă. În practică, dreptul la portabilitatea datelor într-un context al resurselor umane va viza, fără îndoială, anumite operațiuni de prelucrare (precum servicii de plată și compensare, recrutare internă), dar în multe alte situații, va fi necesară o abordare de la caz la caz pentru a verifica dacă sunt îndeplinite toate condițiile aplicabile dreptului la portabilitatea datelor.

În cele din urmă, dreptul la portabilitatea datelor se aplică doar dacă prelucrarea datelor este „efectuată prin mijloace automate” și, prin urmare, nu vizează majoritatea dosarelor pe suport de hârtie.

- Ce date cu caracter personal trebuie să fie incluse?

În conformitate cu articolul 20 alineatul (1), ca să fie incluse în domeniul de aplicare al dreptului la portabilitatea datelor, datele trebuie să fie:

- date cu caracter personal care privesc persoana vizată și
- pe care aceasta le-a *furnizat* unui operator.

Articolul 20 alineatul (4) prevede, de asemenea, că respectarea acestui drept nu aduce atingere drepturilor și libertăților altor persoane.

Prima condiție: date cu caracter personal referitoare la persoana vizată

Doar datele cu caracter personal intră în domeniul de aplicare al unei cereri de portabilitate a datelor. Prin urmare, orice date care sunt anonime¹⁸ 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.

operatorii de date nu au nicio obligație de a asigura portabilitatea în aceste cazuri. Cu toate acestea, este o bună practică să se dezvolte procese prin care să se răspundă automat cererilor de portabilitate, cu respectarea principiilor care reglementează dreptul la portabilitatea datelor. Un exemplu în acest sens ar fi un serviciu public care asigură descărcarea ușoară a declarațiilor de venit personale depuse în trecut. Pentru portabilitatea datelor ca o bună practică în cazul prelucrării bazate pe criteriul juridic al necesității unui interes legitim și pentru schemele voluntare existente, a se vedea paginile 47 și 48 din Avizul nr. 6/2014 al GL29 privind interesele legitime (GL217).

¹⁷ Astfel cum a subliniat GL29 în Avizul nr. 8/2001 din 13 septembrie 2001 (GL48).

¹⁸ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

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).

A doua condiție datele furnizate de persoana vizată

A doua condiție limitează domeniul de aplicare la date „furnizate de” persoana vizată.

Există numeroase exemple de date cu caracter personal care vor fi „furnizate de” persoana vizată cu bună știință și în mod activ, cum ar fi datele despre cont (de exemplu, adresa poștală, numele utilizatorului, vârstă) transmise prin formulare online. Cu toate acestea, datele „furnizate de” persoana vizată rezultă și ca urmare a activității acesteia. În consecință, GL29 consideră că, pentru a conferi pe deplin valoare acestui nou drept, sintagma „furnizat de” ar trebui să includă și datele cu caracter personal care sunt observate din activitățile utilizatorilor, cum ar fi date brute prelucrate de un contor inteligent sau alte tipuri de obiecte conectate¹⁹, jurnale de activități, istoricul de utilizare sau de căutare în site.

Această ultimă categorie de date nu include date care sunt create de către operator (utilizând datele observate sau furnizate direct ca date de intrare), cum ar fi un profil de utilizator creat în urma analizei datelor brute colectate prin sistemul de contorizare inteligentă.

Se poate face o distincție între diferitele categorii de date, în funcție de originea lor, pentru a determina dacă acestea intră în domeniul de aplicare al dreptului la portabilitatea datelor. Următoarele categorii pot fi calificate drept date „furnizate de către persoana vizată”:

- **Date furnizate în mod activ și cu bună știință de persoana vizată** (de exemplu, adresa poștală, numele de utilizator, vârsta etc.)
- **Date observate furnizate de către persoana vizată prin virtutea utilizării serviciului sau a dispozitivului.** Acestea pot include, de exemplu, istoricul de căutare al unei persoane, datele privind traficul și datele de localizare. Acestea pot include și alte date brute precum bătăile inimii detectate cu ajutorul unui dispozitiv portabil.

În schimb, datele deduse și datele derivate sunt create de către operator pe baza datelor „furnizate de persoana vizată”. De exemplu, rezultatul unei evaluări privind sănătatea unui utilizator sau profilul creat în contextul normelor financiare și de gestionare a riscurilor (de exemplu, atribuirea unui punctaj de bonitate sau respectarea normelor de combatere a spălării banilor) nu pot fi considerate în sine ca fiind „furnizate de” persoana vizată. Chiar dacă astfel de date pot face parte dintr-un profil păstrat de un operator și sunt deduse sau derivate ca

¹⁹ Datorită faptului că poate să obțină datele rezultate ca urmare a observării activității sale, persoana vizată va putea totodată să aibă o imagine mai bună a opțiunilor de implementare adoptate de către operator în ceea ce privește domeniul de aplicare al datelor observate și se va afla pe o poziție mai bună să aleagă datele pe care este dispus să le ofere pentru a obține un serviciu similar, precum și să cunoască măsura în care va fi respectat dreptul său la viața privată.

urmare a analizei datelor furnizate de persoana vizată (de exemplu, prin acțiunile sale), aceste date nu vor fi considerate, în mod normal, ca fiind „furnizate de persoana vizată” și, prin urmare, nu vor fi incluse în domeniul de aplicare al acestui drept nou²⁰.

În general, având în vedere obiectivele de politică ale dreptului la portabilitatea datelor, sintagma „furnizate de persoana vizată” trebuie să fie interpretată în sens larg și ar trebui să excludă „datele deduse” și „datele derivate”, care includ date cu caracter personal create de către un prestator de servicii (de exemplu, rezultate algoritmice). Un operator poate exclude aceste date deduse, însă ar trebui să includă, de asemenea, toate celelalte date cu caracter personal furnizate de persoana vizată prin mijloace tehnice puse la dispoziție de către operator²¹.

Astfel, sintagma „furnizate de” include date cu caracter personal referitoare la activitatea persoanei vizate sau date generate în urma observării comportamentului unei persoane, însă nu include datele rezultate în urma analizei ulterioare a comportamentului respectiv. În schimb, orice date cu caracter personal care au fost create de către operator în cadrul activității de prelucrare a datelor, de exemplu, printr-un proces de personalizare sau recomandare, prin clasificarea utilizatorilor sau crearea de profiluri sunt date derivate sau deduse din datele cu caracter personal furnizate de persoana vizată, și nu sunt vizate de dreptul la portabilitatea datelor.

A treia condiție: dreptul la portabilitatea datelor nu aduce atingere drepturilor și libertăților altora

Referitor la datele cu caracter personal privind alte persoane vizate:

Cea de a treia condiție este menită să evite obținerea și transmiterea de date care conțin date cu caracter personal ale altor persoane vizate (care nu și-au exprimat consimțământul) unui nou operator în cazurile în care aceste date sunt susceptibile de a fi prelucrate într-un mod care ar aduce atingere drepturilor și libertăților celorlalte persoane vizate [articolul 20 alineatul (4) din RGPD]²².

Un astfel de efect negativ s-ar produce, de exemplu, în cazul în care transmiterea datelor de la un operator la altul ar împiedica părțile terțe să își exercite drepturile în calitate de persoane vizate în temeiul RGPD (cum ar fi drepturile de informare, de acces etc.).

²⁰ Cu toate acestea, persoana vizată se poate prevala în continuare de „dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective”, precum și de informații despre „existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la articolul 22 alineatele (1) și (4), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată”, în conformitate cu articolul 15 din RGPD (care se referă la dreptul de acces).

²¹ Acestea includ toate datele observate despre persoana vizată în cursul activităților în scopul cărora au fost colectate datele, precum istoricul unor tranzacții sau jurnalul de accesări. Datele colectate în urma urmării și înregistrării persoanei vizate (cum ar fi o aplicație care înregistrează bătăile inimii sau tehnologia utilizată pentru a urmări comportamentul de navigare) ar trebui să fie considerate, de asemenea, ca fiind „furnizate de” persoana vizată, chiar dacă datele nu sunt transmise în mod activ sau conștient.

²² Considerentul 68 prevede că „În cazul în care, într-un anumit set de date cu caracter personal, sunt implicate mai multe persoane vizate, dreptul de a primi datele cu caracter personal nu ar trebui să aducă atingere drepturilor și libertăților altor persoane vizate, în conformitate cu prezentul regulament.”

Persoana vizată care inițiază transmisiunea datelor sale către un alt operator, fie își dă consimțământul noului operator pentru prelucrare, fie încheie un contract cu respectivul operator. În cazul în care în setul de date sunt incluse datele cu caracter personal ale unor părți terțe, trebuie să fie identificat un alt temei juridic pentru prelucrare. De exemplu, ar putea fi urmărit un interes legitim de către operator în temeiul articolului 6 alineatul (1) litera (f), în special atunci când scopul operatorului este de a furniza un serviciu persoanei vizate, care să îi permită acesteia din urmă să prelucreze date cu caracter personal pentru o activitate exclusiv personală sau domestică. Operațiunile de prelucrare inițiate de către persoana vizată în contextul activității personale, care privesc și, eventual, au un impact asupra unor părți terțe, rămân sub responsabilitatea sa, în măsura în care o astfel de prelucrare nu este decisă, în niciun fel, de către operator.

De exemplu, un serviciu de webmail poate permite crearea unui anuar al contactelor, prietenilor, rudelor, familiei și mediului mai larg al unei persoane vizate. Întrucât aceste date se referă la (și sunt create de) persoana identificabilă care dorește să își exercite dreptul la portabilitatea datelor, operatorii ar trebui să transmită persoanei vizate în cauză întregul anuar de mesaje electronice primite și trimise.

În mod similar, contul bancar al unei persoane vizate poate conține date cu caracter personal referitoare la tranzacții nu doar ale titularului de cont, ci și ale altor persoane fizice (de exemplu, în cazul în care acestea au transferat bani în contul titularului de cont). Este puțin probabil ca drepturile și libertățile părților terțe respective să fie afectate negativ de transmiterea informațiilor referitoare la contul bancar către titularul de cont după emiterea unei cereri de portabilitate - cu condiția ca, în ambele exemple, datele să fie utilizate în același scop (și anume, o adresă de contact folosită numai de către persoana vizată sau istoricul contului bancar al persoanei vizate).

Dimpotrivă, drepturile și libertățile părților terțe nu vor fi respectate în cazul în care noul operator utilizează datele cu caracter personal în alte scopuri, de exemplu, dacă operatorul beneficiar utilizează datele cu caracter personal ale altor persoane din anuarul persoanelor de contact ale persoanei vizate în scopuri comerciale.

Prin urmare, pentru a preveni efectele negative asupra părților terțe implicate, prelucrarea acestor date cu caracter personal de către un alt operator este permisă numai în măsura în care datele sunt păstrate sub controlul unic al utilizatorului solicitant și sunt gestionate exclusiv pentru nevoile personale sau domestice. Un operator beneficiar „nou” (căruia îi pot fi transmise datele la cererea utilizatorului) nu poate utiliza datele transmise despre părțile terțe în scopuri proprii, de exemplu, pentru a propune comercializarea de produse și servicii acestor alte persoane vizate ca părți terțe. De exemplu, aceste informații nu ar trebui să fie utilizate pentru a îmbogăți profilul persoanei vizate ca parte terță și a reconstitui mediul social al acesteia, fără ca aceasta să aibă cunoștința despre aceasta și fără aprobarea sa²³. Acestea nu pot fi utilizate nici pentru a obține informații cu privire la astfel de părți terțe și a crea profiluri specifice, chiar dacă datele lor cu caracter personal sunt deja deținute de operator. În caz contrar, o astfel de prelucrare este susceptibilă de a fi ilegală și inechitabilă, în special în cazul

²³ Un serviciu de socializare nu ar trebui să îmbogățească profilul membrilor săi prin utilizarea datelor cu caracter personal transmise de o persoană vizată în cadrul dreptului său la portabilitatea datelor, fără a respecta principiul transparenței și a se asigura, de asemenea, că se bazează pe un temei juridic adecvat în ceea ce privește această prelucrare specifică.

în care părțile terțe în cauză nu sunt informate în acest sens și nu își pot exercita drepturile în calitate de persoane vizate.

În plus, una dintre practicile principale ale tuturor operatorilor (părțile „transmițătoare” și, respectiv, „beneficiare”) este să pună în aplicare instrumente care să permită persoanelor vizate să selecteze datele relevante pe care doresc să le primească și să le transmită și să excludă, dacă este cazul, datele altor persoane. Aceasta va contribui în continuare la reducerea riscurilor pentru părțile terțe ale căror date cu caracter personal pot fi portate.

În plus, operatorii ar trebui să pună în aplicare mecanisme de obținere a consimțământului pentru alte persoane vizate implicate, pentru a facilita transmiterea datelor în acele cazuri în care astfel de părți sunt dispuse să își exprime consimțământul, de exemplu, în cazul în care aceștia doresc, de asemenea, să își transfere datele către un alt operator. O astfel de situație ar putea să apară, de exemplu, în cazul rețelelor de socializare, însă operatorii sunt cei care trebuie să decidă cu privire la care practica principală de urmat.

Referitor la datele care intră sub incidența drepturilor de proprietate intelectuală și a secretelor comerciale:

Drepturile și libertățile altor persoane sunt menționate la articolul 20 alineatul (4). Deși nu sunt legate direct de portabilitate, acestea pot fi interpretate ca fiind asociate „inclusiv secretului comercial sau proprietății intelectuale și, în special, drepturilor de autor care asigură protecția programelor software. Cu toate acestea, chiar dacă aceste drepturi ar trebui să fie examinate înainte de a răspunde unei cereri de portabilitate a datelor, „considerațiile de mai sus nu ar trebui să aibă drept rezultat refuzul de a furniza toate informațiile persoanei vizate”. În plus, operatorul nu ar trebui să respingă o cerere de portabilitate a datelor pe baza faptului că a fost încălcat un alt drept contractual (de exemplu, există o datorie restantă sau un conflict comercial cu persoana vizată).

Dreptul la portabilitatea datelor nu conferă unei persoane dreptul de a folosi în mod abuziv informațiile într-un mod care ar putea fi calificat drept practică neloială sau care constituie o încălcare a drepturilor de proprietate intelectuală.

Însă un posibil risc comercial nu poate servi în sine drept temei pentru refuzul de a răspunde cererii de portabilitate, iar operatorii pot transmite datele cu caracter personal furnizate de persoanele vizate sub o formă care să nu divulge informații care fac obiectul secretului comercial sau al drepturilor de proprietate intelectuală.

IV. Cum se aplică regulile generale care reglementează exercitarea drepturilor persoanei vizate în cazul portabilității datelor?

- Ce informații prelabile ar trebui furnizate persoanei vizate?

Pentru a respecta noul drept la portabilitatea datelor, operatorii trebuie să informeze persoanele vizate în legătură cu existența noului drept la portabilitate. În cazul în care datele cu caracter personal sunt colectate direct de la persoana vizată, acest lucru trebuie să realizeze „în momentul obținerii acestor date cu caracter personal”. În cazul în care nu au fost obținute datele cu caracter personal de la persoana vizată, operatorul trebuie să furnizeze informațiile prevăzute la articolele 13 alineatul (2) litera (b) și 14 alineatul (2) litera (c).

„În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată”, articolul 14 alineatul (3) impune furnizarea informațiilor într-un termen rezonabil care să nu

depășească o lună de la obținerea datelor, în timpul primei comunicări cu persoana vizată sau atunci când informațiile sunt transmise unor părți terțe²⁴.

Atunci când furnizează informațiile solicitate, operatorii trebuie să se asigure că fac o distincție între dreptul la portabilitatea datelor și alte drepturi. Prin urmare, GL29 recomandă, în mod specific, operatorilor să explice în mod clar diferența între tipurile de date pe care le poate primi o persoană vizată prin drepturile sale de acces și la portabilitatea datelor.

În plus, grupul de lucru recomandă operatorilor să includă întotdeauna informații despre dreptul la portabilitatea datelor înainte ca persoanele vizate să închidă orice cont pe care l-ar avea. Aceasta le permite utilizatorilor să își verifice datele cu caracter personal și să transmită cu ușurință datele la propriul lor dispozitiv sau unui alt furnizor înainte de data rezilierii unui contract.

În cele din urmă, ca practică principală pentru operatorii „beneficiari”, GL29 recomandă ca persoanele vizate să primească informații complete cu privire la natura datelor cu caracter personal care sunt relevante pentru prestarea serviciilor lor. Pe lângă faptul că stă la baza prelucrării echitabile, aceasta le permite utilizatorilor să limiteze riscurile pentru părți terțe și, de asemenea, orice duplicare inutilă a datelor cu caracter personal, chiar și atunci când nu sunt implicate alte persoane vizate.

- Cum poate identifica operatorul persoana vizată înainte de a răspunde la cererea sa?

RGPD nu prevede cerințe privind modul de autentificare a persoanei vizate. Cu toate acestea, articolul 12 alineatul (2) din RGPD prevede că operatorul nu refuză să dea curs cererii unei persoane vizate de a-și exercita drepturile (inclusiv dreptul la portabilitatea datelor), cu excepția cazului în care acesta prelucrează date cu caracter personal într-un scop care nu prevede identificarea unei persoane vizate și poate demonstra că nu este în măsură să identifice persoana vizată. Cu toate acestea, în conformitate cu articolul 11 alineatul (2), în astfel de împrejurări, persoana vizată poate furniza mai multe informații care să permită identificarea sa. În plus, articolul 12 alineatul (6) prevede că, în cazul în care un operator are îndoieli întemeiate cu privire la identitatea unei persoane fizice, acesta poate solicita informații suplimentare pentru a confirma identitatea persoanei vizate. În cazul în care o persoană vizată oferă informații suplimentare care permit identificarea sa, operatorul nu refuză să dea curs cererii. În cazul în care informațiile și datele colectate online sunt legate de pseudonime sau identificatori unici, operatorii pot pune în aplicare proceduri adecvate care să permită unei persoane să emită o cerere de portabilitate a datelor și să primească datele care o privesc. În orice caz, operatorii trebuie să pună în aplicare o procedură de autentificare pentru a stabili cu certitudine identitatea persoanei vizate care își solicită datele cu caracter personal sau, mai general, care își exercită drepturile conferite prin RGPD.

Aceste proceduri deseori există deja. Persoanele vizate sunt deseori deja autentificate de către operator înainte de a încheia un contract sau a obține consimțământul acestora pentru prelucrare. Drept urmare, datele cu caracter personal utilizate pentru a înregistra persoana

²⁴ Articolul 12 impune operatorilor să asigure „orice comunicări [...] într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil.”

vizată de procesul de prelucrare pot fi utilizate și ca probe pentru autentificarea persoanei vizate în scopurile portabilității²⁵.

Deși în aceste cazuri, identificarea prealabilă a persoanelor vizate ar putea presupune adresarea unei cereri privind o dovadă a identității lor juridice, este posibil ca o astfel de verificare să nu fie relevantă pentru evaluarea legăturii dintre datele și persoana în cauză, întrucât o astfel de legătură nu este asociată cu identitatea oficială sau juridică. În esență, capacitatea operatorului de a solicita informații suplimentare pentru a evalua identitatea unei persoane nu poate conduce la emiterea de solicitări în exces și la colectarea datelor cu caracter personal care nu sunt relevante sau necesare pentru a consolida legătura dintre persoana în cauză și datele cu caracter personal solicitate.

În multe cazuri, astfel de proceduri de autentificare sunt instituite deja. De exemplu, numele de utilizator și parolele sunt adesea utilizate pentru a permite persoanelor să aibă acces la datele lor din conturile lor electronice, din conturile de pe rețelele de socializare și din conturile utilizate pentru diverse alte servicii, dintre care unele persoane au ales să folosească o parte fără a-și dezvălui numele complet și identitatea.

Dacă dimensiunea datelor solicitate de persoana vizată produce probleme la transmiterea pe internet, în loc să acorde eventual o perioadă de timp extinsă de maximum trei luni pentru soluționarea cererii²⁶, eventual operatorul ar trebui să aibă în vedere mijloace alternative de furnizare a datelor, cum ar fi prin streaming sau cu salvare pe un CD, DVD sau pe un alt suport fizic, ori permițând ca datele cu caracter personal să fie transmise direct unui alt operator [în conformitate cu articolul 20 alineatul (2) din RGPD, în cazul în care acest lucru este fezabil din punct de vedere tehnic].

- Care este termenul-limită impus pentru a răspunde unei cereri de portabilitate?

Articolul 12 alineatul (3) prevede că operatorul furnizează „informații privind acțiunile întreprinse” persoanei vizate „fără întârzieri nejustificate” și, în orice caz, „în cel mult o lună de la primirea cererii”. Această perioadă de o lună poate fi prelungită până la maxim trei luni în cazuri complexe, cu condiția ca persoana vizată să fie informată cu privire la motivele acestei întârzieri în termen de o lună de la cererea inițială.

Este posibil ca operatorii care prestează servicii ale societății informaționale să fie mai bine pregătiți pentru a fi în măsură să soluționeze cererile într-un interval de timp foarte scurt. Pentru a răspunde așteptărilor utilizatorilor, o bună practică este de a defini intervalul de timp în care poate fi soluționată, de regulă, o cerere de portabilitate a datelor și de a comunica acest lucru persoanelor vizate.

Operatorii care refuză să răspundă unei cereri de portabilitate informează persoana vizată, în temeiul articolului 12 alineatul (4), „cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară” în termen de cel mult o lună de la primirea cererii.

²⁵ De exemplu, atunci când prelucrarea datelor este legat de un cont de utilizator, furnizarea numelui de autentificare și a parolei corespunzătoare ar putea fi suficientă pentru a identifica persoana vizată.

²⁶ Articolul 12 alineatul (3): „Operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri”.

Operatorii trebuie să respecte obligația de a răspunde în condițiile date, chiar dacă este vorba despre un refuz. Cu alte cuvinte, operatorul nu poate păstra tăcerea atunci când i se solicită să dea curs unei cereri de portabilitate a datelor.

- **În ce cazuri poate fi o cerere de portabilitate a datelor respinsă sau o taxă percepută?**

Articolul 12 interzice operatorului să perceapă o taxă pentru furnizarea datelor cu caracter personal, cu excepția cazului în care operatorul poate demonstra că cererile sunt în mod vădit nefondate sau excesive, „în special din cauza caracterului lor repetitiv”. Pentru servicii ale societății informaționale care sunt specializate în prelucrarea automată a datelor cu caracter personal, implementarea de sisteme automatizate precum interfețele de programare a aplicațiilor (API)²⁷ poate să faciliteze schimbul cu persoana vizată și, prin urmare, să reducă o eventuală povară asociată cererilor cu caracter repetitiv. Prin urmare, ar trebui să existe foarte puține cazuri în care operatorul să poată justifica refuzul de a furniza informațiile solicitate, chiar și în ceea ce privește cererile multiple de portabilitate a datelor.

În plus, costul total al proceselor create pentru a răspunde cererilor de portabilitate a datelor nu ar trebui să fie luat în considerare în vederea stabilirii caracterului excesiv al unei cereri. De fapt, articolul 12 din RGPD vizează cererile formulate de o singură persoană vizată, nu numărul total de cereri primite de un operator. Prin urmare, costurile generale de punere în aplicare a sistemului nu ar trebui nici să fie percepute de la persoanele vizate, nici să fie folosite pentru a justifica un refuz de a răspunde cererilor de portabilitate.

V. Cum trebuie să fie furnizate datele portabile?

- **Care sunt măsurile preconizate pe care operatorul ar trebui să le pună în aplicare pentru furnizarea datelor?**

Articolul 20 alineatul (1) din RGPD prevede că persoanele vizate au dreptul de a transmite datele unui alt operator fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal.

Astfel de obstacole pot fi caracterizate ca fiind orice obstacole juridice, tehnice sau financiare din partea operatorului cu scopul de a împiedica sau a încetini accesul, transmiterea sau reutilizarea datelor de către persoana vizată sau de către un alt operator. De exemplu, astfel de obstacole ar putea fi: taxe solicitate pentru transmiterea datelor, lipsa de interoperabilitate sau de acces la un format de date sau la API ori la formatul furnizat, întâzieri excesive sau complexitatea de a obține setul complet de date, ambiguitatea intenționată a setului de date sau impunerea de cerințe specifice și nejustificate sau excesive de standardizare sau de acreditare la nivel de sector²⁸.

²⁷ Interfața de programare a aplicației (API) înseamnă interfețele aplicațiilor sau serviciilor pe web puse la dispoziție de operatori, astfel încât alte sisteme sau aplicații să poată face legătura și să funcționeze cu sistemele lor.

²⁸ Ar putea să apară unele obstacole legitime precum cele care sunt legate de drepturile și libertățile altor persoane menționate la articolul 20 alineatul (4) sau cele care se referă la securitatea sistemelor proprii ale operatorilor. Operatorul este cel care are responsabilitatea de a justifica motivul pentru care aceste obstacole ar fi legitime și de ce acestea nu constituie un obstacol în sensul articolului 20 alineatul (1).

Articolul 20 alineatul (2) introduce obligații și pentru operatori în cazul transmiterii datelor portabile direct altor operatori „atunci când acest lucru este fezabil din punct de vedere tehnic”.

Fezabilitatea tehnică a transmiterii de la un operator la alt operator, sub controlul persoanei vizate, ar trebui evaluată de la caz la caz. Considerentul 68 clarifică, în plus, limitele a ceea ce înseamnă „fezabil din punct de vedere tehnic”, indicând faptul că „nu ar trebui să creeze pentru operatori obligația de a adopta sau de a menține sisteme de prelucrare care să fie compatibile din punct de vedere tehnic.

Operatorii sunt prevăzuți a transmite date cu caracter personal într-un format interoperabil, deși acest lucru nu impune obligații asupra altor operatori de a susține aceste formate. Așadar, transmiterea directă de la un operator la altul ar putea apărea atunci când este posibilă comunicarea între două sisteme, într-un mod securizat²⁹ și când sistemul beneficiar este din punct de vedere tehnic în măsură să primească datelor intrate. Dacă există impedimente de ordin tehnic care interzic transmiterea directă, operatorul trebuie să explice aceste obstacole persoanelor vizate, întrucât, dacă nu face acest lucru, decizia sa va fi similară ca efect unui refuz de a lua măsuri cu privire la cererea unei persoane vizate [articolul 12 alineatul (4)].

La nivel tehnic, operatorii ar trebui să analizeze și să evalueze două căi diferite și complementare de a pune date portabile la dispoziția persoanelor vizate sau a altor operatori:

- transmiterea directă a întregului set de date portabile (sau mai multe părți extrase din setul de date global);
- un instrument automat care permite obținerea datelor relevante.

Cea de a doua metodă ar putea fi preferată de către operatori în cazurile care implică seturi de date mari și complexe, deoarece aceasta permite obținerea oricărei părți a setului de date care este relevantă pentru persoana vizată în contextul cererii sale, poate contribui la reducerea la minimum a riscurilor și, eventual, permite utilizarea mecanismelor de sincronizare a datelor³⁰ (de exemplu, în contextul unei comunicări periodice între operatori). Aceasta ar putea fi o modalitate mai bună de a asigura conformitatea în cazul „noului” operator și ar constitui o bună practică pentru reducerea riscurilor legate de viața privată din partea operatorului inițial.

Aceste două modalități diferite și eventual complementare de furnizare a datelor portabile ar putea fi puse în aplicare prin punerea la dispoziție a datelor prin diverse mijloace precum, spre exemplu, mesageria securizată, un server SFTP, un WebAPI sau WebPortal securizat. Persoanele vizate ar trebui să aibă posibilitatea de a utiliza un depozit de date cu caracter personal, sistemul de gestionare a informațiilor cu caracter personal³¹ sau alte tipuri de părți terțe de încredere, să păstreze și să stocheze date cu caracter personal, precum și să acorde permisiunea operatorilor de a accesa și a prelucra date cu caracter personal, după caz.

- **Care este formatul preconizat al datelor?**

²⁹ Printr-o comunicare autentificată cu nivelul necesar de criptare a datelor.

³⁰ Mecanismul de sincronizare poate contribui la îndeplinirea obligațiilor generale de la articolul 5 din RGPD, care prevede că „datele cu caracter personal sunt (...) exacte și, în cazul în care este necesar, să fie actualizate”.

³¹ Cu privire la sistemele de gestionare a informațiilor cu caracter personal (PIMS), a se vedea, spre exemplu, Avizul nr. 9/2016 al AEPD, disponibil la https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

RGPD impune operatorilor cerințe privind furnizarea datelor cu caracter personal solicitate de o persoană într-un format care să favorizeze reutilizarea. Mai exact, articolul 20 alineatul (1) din RGPD prevede că datele cu caracter personal trebuie să fie furnizate „într-un format structurat, utilizat în mod curent și care poate fi citit automat”. Considerentul 68 oferă o clarificare suplimentară privind faptul că acest format ar trebui să fie interoperabil, un termen care este definit³² în UE ca fiind:

capacitatea unor organizații distincte și diverse de a interacționa în scopul realizării unor obiective care aduc beneficii reciproce și sunt convenite mutual, care implică partajarea de informații și cunoștințe între organizații prin intermediul proceselor profesionale pe care acestea le sprijină, utilizând schimbul de date între respectivele sisteme TIC deținute de acestea.

Termenii „structurat”, „utilizat” și „care poate fi citit automat” constituie un set de cerințe minime care ar trebui să faciliteze interoperabilitatea formatului datelor furnizate de operator. În acest mod, „structurat, utilizat în mod curent și care poate fi citit automat” înseamnă specificații pentru mijloace, în timp ce interoperabilitatea reprezintă rezultatul dorit.

Considerentul 21 din Directiva 2013/37/UE^{33,34} definește „prelucrabil automat” ca fiind:

un format de fișier structurat astfel încât să permită aplicațiilor software să identifice, să recunoască și să obțină cu ușurință date specifice, inclusiv declarații individuale de fapt, și structura internă a acestora. Datele codificate în fișiere care sunt structurate într-un format prelucrabil automat sunt date prelucrabile automat. Formatele prelucrabile automat pot fi deschise sau protejate prin drepturi exclusive; și pot fi standarde formale sau nu. Documentele codificate într-un format de fișier care limitează această prelucrare automată, deoarece datele nu pot fi extrase sau nu pot fi extrase cu ușurință din aceste documente, nu ar trebui considerate documente în format prelucrabil automat. Statele membre ar trebui, după caz, să încurajeze utilizarea de formate deschise, prelucrabile automat.

Având în vedere gama largă de posibile tipuri de date care ar putea fi prelucrate de un operator, RGPD nu impune recomandări specifice privind formatul datelor cu caracter personal care trebuie furnizate. Formatul cel mai adecvat va diferi de la un sector la altul și este posibil să existe deja formate adecvate și ar trebui ca acestea să fie întotdeauna alese în vederea îndeplinirii scopului ca datele să fie interpretabile și să permită persoanei vizate să asigure un grad ridicat de portabilitate a datelor. Ca atare, formatele care fac obiectul unor constrângeri costisitoare privind obținerea licențelor nu ar fi considerate a fi o abordare adecvată.

Considerentul 68 clarifică faptul că „Dreptul persoanei vizate de a transmite sau de a primi date cu caracter personal care o privesc nu ar trebui să creeze pentru operatori obligația de a adopta sau de a menține sisteme de prelucrare care să fie compatibile din punct de vedere

³² Articolul 2 din Decizia 922/2009/CE a Parlamentului European și a Consiliului din 16 septembrie 2009 privind soluțiile de interoperabilitate pentru administrațiile publice europene (ISA) (JO L 260, 03.10.2009, p. 20)

³³ De modificare a Directivei 2003/98/CE privind reutilizarea informațiilor din sectorul public.

³⁴ Glosarul UE (<http://eur-lex.europa.eu/eli-register/glossary.html>) oferă clarificări suplimentare privind așteptările legate de conceptele utilizate în prezentul ghid, precum *prelucrabil automat*, *interoperabilitate*, *format deschis*, *standard*, *metadata*.

*tehnic.” Astfel, obiectivul portabilității este de a produce sisteme interoperabile, nu sisteme compatibile*³⁵.

Datele cu caracter personal sunt prevăzute a fi furnizate în formate care au un nivel ridicat de obținere din orice format intern sau protejat. Ca atare, portabilitatea datelor presupune un nivel suplimentar de prelucrare a datelor de către operatori pentru a obține date de pe platformă și a filtra pentru a exclude datele cu caracter personal care nu intră în sfera de aplicare a portabilității, cum ar fi datele deduse sau datele legate de securitatea sistemelor. Astfel, operatorii sunt încurajați să identifice în prealabil datele care sunt incluse în domeniul de aplicare al portabilității în cadrul propriilor lor sisteme. Această prelucrare suplimentară a datelor va fi considerată drept una auxiliară activității principale de prelucrare a datelor, întrucât nu este efectuată în vederea îndeplinirii unui nou scop stabilit de către operator.

În cazul în care nu există formate utilizate în mod frecvent pentru o anumită industrie sau un context dat, **operatorii ar trebui să furnizeze date cu caracter personal folosind formate deschise utilizate în mod frecvent (de exemplu, XML, JSON, CSV ...), alături de metadata utile la cel mai bun nivel posibil de granularitate**, în același timp menținându-se un nivel ridicat de extracție. Ca atare, ar trebui să se utilizeze metadata adecvate pentru a descrie cu precizie sensul informațiilor schimbate. Aceste metadata ar trebui să fie suficiente pentru a asigura funcția și posibilitatea de reutilizare a datelor, însă, desigur, fără divulgarea secretelor comerciale. Prin urmare, este puțin probabil ca versiunile PDF ale căsuței de primire din poșta electronică, ce sunt furnizate unei persoane, să fie suficient de structurate sau descriptive pentru a permite datelor din căsuța de primire să poată fi reutilizate cu ușurință. În schimb, datele din poșta electronică ar trebui să fie furnizate într-un format care păstrează toate metadatale pentru a permite reutilizarea eficientă a datelor. Ca atare, atunci când se selectează un format al datelor în care să se furnizeze date cu caracter personal, operatorul ar trebui să aibă în vedere modul în care acest format ar afecta sau împiedica exercitarea dreptului persoanei de a reutiliza datele. În cazul în care un operator are posibilitatea de a oferi persoanei vizate opțiuni privind formatul preferat al datelor cu caracter personal, ar trebui să se ofere o explicație clară a impactului alegerii făcute. Cu toate acestea, prelucrarea metadatelor suplimentar doar pentru că acestea ar putea fi necesare sau dorite pentru a răspunde unei cereri de portabilitate a datelor nu constituie un motiv legitim pentru o astfel de prelucrare.

GL29 încurajează ferm cooperarea dintre părțile interesate din industrie și organismele profesionale pentru a conlucra în vederea elaborării unui set comun de standarde și formate interoperabile pentru a îndeplini cerințele asociate dreptului la portabilitatea datelor. Această problemă a fost abordată, de asemenea, în Cadrul european de interoperabilitate (EIF), care a creat o abordare comună a interoperabilității pentru organizațiile care doresc să furnizeze în comun servicii publice. În domeniul său de aplicare, cadrul specifică un set de elemente comune cum ar fi vocabularul, conceptele, principiile, politicile, orientările, recomandările, standardele, specificațiile și practicile³⁶.

- **Cum se procedează în cazul unei colecții mari și complexe de date cu caracter personal?**

³⁵ ISO/IEC 2382-01 definește interoperabilitatea după cum urmează: „Capacitatea de a comunica, de a executa programe sau de a transfera date între diverse unități funcționale într-un mod care impune utilizatorului să dețină puține cunoștințe sau deloc despre caracteristicile unice ale acestor unități.”

³⁶ Sursa: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

RGPD nu explică modul în care să se abordeze problema acordării unui răspuns în cazul în care există o colecție amplă de date, o structură complexă de date sau alte probleme tehnice care ar putea da naștere unor dificultăți pentru operatori sau persoanele vizate.

Cu toate acestea, în toate cazurile, este esențial ca persoana în cauză să fie în măsură să înțeleagă pe deplin definiția, schema și structura datelor cu caracter personal care ar putea fi furnizate de către operator. De exemplu, datele ar putea fi transmise mai întâi într-o formă sintetică prin intermediul unor tablouri de bord care să permită persoanei vizate să poarte subseturi de date cu caracter personal, nu toate datele. Operatorul ar trebui să ofere o prezentare „într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu” [a se vedea articolul 12 alineatul (1) din RGPD], în așa fel încât persoana vizată să dispună întotdeauna de informații clare despre datele care să fie descărcate sau transmise unui alt operator în legătură cu un anumit scop. De exemplu, persoanele vizate ar trebui să fie în măsură să utilizeze aplicații software pentru a identifica, a recunoaște și a prelucra cu ușurință date specifice din acestea.

Astfel cum este menționat mai sus, una dintre modalitățile practice prin care un operator poate răspunde cererilor de portabilitate a datelor poate fi asigurarea unei API securizate și documentate în mod corespunzător. Astfel, se poate permite persoanelor să formuleze cereri la adresa operatorului pentru datele lor cu caracter personal prin intermediul software-ului propriu sau al terților sau acestea pot acorda permisiunea altor persoane să facă acest lucru în numele lor (inclusiv unui alt operator), astfel cum este prevăzut la articolul 20 alineatul (2) din RGPD. Prin acordarea accesului la date prin intermediul unei API accesibile la nivel extern, ar putea fi posibil, de asemenea, să se ofere un sistem de acces mai sofisticat care să permită persoanelor să formuleze cereri ulterioare de date, fie cu descărcare integrală, fie ca funcție delta care conține doar modificări de la ultima descărcare, fără ca aceste cereri suplimentare să fie solicitante pentru operator.

- Cum pot fi securizate datele portabile?

În general, operatorii ar trebui să garanteze „securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare” în conformitate cu articolul 5 alineatul (1) litera (f) din RGPD.

Cu toate acestea, transmiterea datelor cu caracter personal persoanei vizate poate ridica, de asemenea, unele probleme de securitate:

Cum se pot asigura operatorii că datele cu caracter personal sunt livrate persoanei potrivite în condiții de siguranță?

Întrucât scopul portabilității datelor este de a obține date cu caracter personal din sistemul informatic al operatorului, transmiterea poate deveni o posibilă sursă de risc cu privire la aceste date (în special de cazuri de încălcare a securității datelor în timpul transmisiei). Operatorul are responsabilitatea de a lua toate măsurile de securitate necesare pentru a asigura nu doar faptul că datele cu caracter personal sunt transmise în condiții de siguranță (prin criptare de la un capăt la altul sau criptarea datelor) la destinația corectă (aplicând măsuri stricte de autentificare), și pentru a proteja în continuare datele cu caracter personal care rămân în sistemele lor, precum și de a institui proceduri transparente pentru soluționarea unor

posibile cazuri de încălcare a securității datelor³⁷. Ca atare, operatorii ar trebui să evalueze riscurile specifice legate de portabilitatea datelor și să ia măsuri adecvate de atenuare a riscurilor.

Astfel de măsuri de atenuare a riscurilor ar putea include: în cazul în care persoana vizată trebuie să fie deja autentificată, utilizând informații suplimentare de autentificare, precum un secret împărtășit sau un alt factor de autentificare, cum ar fi o parolă pentru prima dată; suspendarea sau oprirea transiterii în cazul în care se suspectează că a fost compromis contul; în cazul transiterii directe de la un operator unui alt operator, ar trebui să se recurgă la autentificarea prin mandat, cum ar fi autentificările bazate pe token.

Astfel de măsuri de securitate nu trebuie să aibă un caracter obstructiv și nu trebuie să împiedice utilizatorii să își exercite drepturile, de exemplu, prin impunerea unor costuri suplimentare.

Cum se ajută utilizatorii să își stocheze datele cu caracter personal în propriile sisteme?

Atunci când obțin datele lor cu caracter personal de la un serviciu online, există întotdeauna riscul ca utilizatorii să le păstreze în sisteme mai puțin securizate decât cel prevăzut de serviciu. Persoana vizată care solicită date este responsabilă pentru identificarea măsurilor adecvate în vederea asigurării protecției datelor cu caracter personal în propriul sistem. Însă aceasta ar trebui să fie informată cu privire la acest lucru pentru a lua măsurile necesare de protejare a informațiilor pe care le-a primit. Ca un exemplu de practică principală, operatorii pot, de asemenea, să recomande un format (formate) adecvat(e), instrumentele de criptare și alte măsuri de securitate pentru a ajuta persoana vizată în atingerea acestui obiectiv.

* * *

Adoptate la Bruxelles, 13 decembrie 2016

*Pentru grupul de lucru,
Președinte
Isabelle FALQUE-PIERROTIN*

Astfel cum au fost revizuite și adoptate ultima dată la 5 aprilie 2017

*Pentru grupul de lucru
Președinte
Isabelle FALQUE-PIERROTIN*

³⁷ În conformitate cu Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune