GRUPUL DE LUCRU „ARTICOLUL 29” PENTRU PROTECȚIA DATELOR

16/RO

WP 242 rev.01

Ghid privind dreptul la portabilitatea datelor

Adoptat în data de 13 decembrie 2016

Revizuit și adoptat în data de 5 aprilie 2017

Acest grup de lucru a fost creat în temeiul articolului 29 din Directiva 95/46/CE și este un organ consultativ european independent care se ocupă cu protecția și confidențialitatea datelor. Sarcinile 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 cetățenia Uniunii) din cadrul Comisiei Europene, Direcția Generală Justiție și Consumatori, B- 1049 Bruxelles, Belgia, biroul MO-59 05/35.

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

CUPRINS

Rezumat

Art. 23 din RGPD crează un nou drept la portabilitatea datelor care este strâns legat de dreptul de acces dar diferă în mai multe feluri. Acesta permite persoanelor vizate să primească datele cu caracter personal pe care le-au furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și să transmită respectivele date altui operator. Obiectivul acestui drept este de a responsabiliza persoana vizată și de a-i oferi un control mai mare asupra datelor sale personale.

Din moment ce permite transmiterea directă a datelor cu caracter personal de la un operator la altul, dreptul la portabilitatea datelor este, de asemenea, un instrument important care va sprijini libera circulație a datelor cu caracter personal în UE și va favoriza concurența între operatori. Acesta va facilita comutarea între diferiți furnizori de servicii și, prin urmare, va stimula dezvolarea de noi servicii în contextul strategiei de piață unică digitală.

Prezentul aviz oferă îndrumări cu privire la modul de interpretare și implementare a dreptului la portabilitatea datelor introdus de RGPD. Prezentul document are drept obiectiv analizarea dreptului la portabilitatea datelor și a scopului acestuia. Documentul clarifică condițiile în care acest nou drept se aplică ținând cont de temeiul legal al prelucrării datelor (fie cosimțământul persoanei vizate, fie necesitatea derulării unui contract) și de faptul că acest drept este limitat la datele cu caracter personal furnizate de persoana vizată. De asemenea, avizul oferă exemple și criterii concrete pentru a explica circumstanțele în care se aplică acest drept. În acest sens, WP29 consideră că dreptul la portabilitatea datelor se referă la datele furnizate cu bună știință și în mod activ de persoana vizată, precum și la datele cu caracter personal generate de activitatea sa. Acest nou drept nu poate fi subminat și limitat la datele cu caracter personal comunicate direct de persoana vizată, spre exemplu, prin intermediul unui formular online.

Ca bună practică, operatorii de date ar trebui să înceapă să dezvolte mijloace care îi vor ajuta să răspundă solicitărilor de portabilitate a datelor, cum ar fi instrumente de descărcare și interfețe de programare a aplicațiilor. Trebuie să garanteze că datele cu caracter personal sunt transmise într-un format structurat, utilizat în mod curent și care poate fi citit automat și trebuie să încurajeze asigurarea interoperabilității formatului datelor furnizate în exercitarea unei cereri de portabilitate a datelor.

Prezentul aviz ajută, de asemenea, operatorii de date să înțeleagă în mod clar obligațiile care le revin și recomandă cele mai bune practici și instrumente care să sprijine respectarea dreptului la portabilitatea datelor. În cele din urmă, avizul recomandă ca părțile interesate și asociațiile profesionale să conlucreze pe un set comun de standarde și formate interoperabile pentru a furniza cerințele dreptului la portabilitatea datelor.

I. Introducere

Art. 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 operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și să transmită respectivele date altui operator, fără obstacole. Acest drept, care se aplică sub rezerva unor anumitor condiții, spijină alegerea utilizatorului („user choice"), controlul utilizatorului („user control") și responsabilizarea utilizatorului („user empowerment").

Persoanele fizice care fac uz de dreptul lor de acces în conformitate cu Directiva privind Protecția Datelor 95/46/CE au fost constrânse de formatul ales de operatorul de date atunci când furnizează informațiile solicitate. **Noul drept la portabilitatea datelor are ca scop responsabilizarea persoanelor vizate în ceea ce privește propriile date cu caracter personal întrucât facilitează capacitatea lor de a muta, copia sau transmite datele cu caracter personal cu ușurință de la un mediu IT la altul** (fie la propriile sisteme, fie la sistemele unor părți terțe de încredere sau cele ale noilor operatori de date).

Prin afirmarea drepturilor și controlul persoanelor vizate asupra datelor cu caracter personal care le privesc, portabilitatea datelor reprezintă, de asemenea, o oportunitate de a „re-echilibra" relația dintre persoanele vizate și operatorii de date[1].

În timp ce dreptul la portabilitatea datelor cu caracter personal poate îmbunătăți, de asemenea concurența între servicii (prin facilitarea serviciului de comutare), RGPD reglementează datele cu caracter personal și nu concurența. În special, art. 20 nu limitează datele portabile la cele care sunt necesare sau utile pentru serviciile de comutare[2].

Cu toate că dreptul la portabilitatea datelor este un drept nou, alte tipuri de portabilitate deja există sau sunt discutate în alte domenii ale legislației (de exemplu în contextul rezilierii contractului, servicii de comunicații de roaming și accesul transfrontalier la servicii[3]). Pot apărea unele sinergii și chiar beneficii pentru persoanele fizice între diferitele tipuri de portabilitate, în situația în care sunt prevăzute într-o abordare combinată, chiar dacă analogiile ar trebui să fie tratate cu precauție.

Prezentul aviz oferă îndrumări operatorilor de date astfel încât aceștia să-și actualizeze practicile, procesele și procedurile și clarifică înțelesul portabilitatea datelor pentru a permite persoanelor vizate să utilizeze în mod eficient noul drept.

[1] Scopul principal al portabilității datelor este de a îmbunătăți controlului persoanei fizice asupra datelor personale și de a asigura că acestea joacă un rol activ în ecosistemul de date

[2] De exemplu, acest drept poate permite băncilor să ofere servicii suplimentare, sub controlul utilizatorului, prin folosirea datelor cu character personal colectate inițial ca parte a unui serviciul de furnizare a energiei.

[3] A se vedea agenda Comisie Europene pentru piața unică digitală: https://ec.europa.eu/digital-agenda/en/digital-single-market, în special prima politică de bază „Acces online îmbunătățit la serviciile și bunurile digitale".

II. Care sunt elementele principale ale portabilității datelor?

RGPD definește dreptul la portabilitatea datelor în art. 20 (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 obstacole din partea operatorului căriua i-au fost furnizate datele cu caracter personal[…]*

- **Un drept de a primi datele cu caracter personal**

În primul rând, portabilitatea datelor este **un drept al persoanei vizate de a primi un subset de date cu caracter personal care o privesc** prelucrate de un operator de date și de a stoca respectivele date pentru uz personal ulterior. O astfel de stocare poate fi pe un dispozitiv privat sau într-un mediu de stocare virtual (cloud) privat, fără a transmite neapărat datele unui alt operator.

În acest sent, portabilitatea datelor completează dreptul de acces. O specificitate a portabilității datelor constă în faptul că aceasta oferă o modalitate ușoară pentru persoanele vizate de a gestiona și reutiliza ele însele datele cu caracter personal. Aceste date ar trebui primite „*într-un format structurat, utilizat în mod curent și care poate fi citit automat*". Spre exemplu, o persoană vizată ar putea fi interesată în preluarea listei actuale de melodii (sau un istoric al melodiilor ascultate) de la un serviciu de muzică, pentru a afla de câte ori a ascultat anumite melodii sau pentru a verifica ce muzică dorește să cumpere sau să asculte pe o altă platformă. În mod similar, poate dori să recupereze lista sa de contacte din aplicația webmail, spre exemplu, pentru a construi o listă de nuntă sau pentru a obține informații despre achiziții folosind diferite carduri de loialitate sau pentru a evalua amprenta de carbon[4].

- **Dreptul de a transmite datele cu caracter personal de la un operator la alt operator de date**

În al doilea rând, art. 20 (1) oferă persoanelor vizate **dreptul de a transmite datele cu caracter personal de la un operator de date la altul** „fără obstacole". Datele pot fi transmise, de asemenea, direct de la un operator de date la altul, la solicitarea persoanei vizate și atunci când acest lucru este fezabil din punct de vedere tehnic (art. 20 (2)). În acest sens, Considerentul 68 încurajează operatorii de date să dezvolte formate interoperabile care să permită portabilitatea datelor[5] fără a crea o obligație operatorilor de date de a adopta sau menține sisteme de prelucrare care sunt combatibile[6]. Cu toate acestea, RGPD înterzice operatorilor să stabilească obstacole în calea transmiterii.

[4] În aceste situații, prelucarea efectuată de persoana vizată poate întra sub incidența activităților domestice, atunci când toate prelucrările sunt effectuate numai sub controlul persoanei vizate, sau poate fi efectuată de o altă parte, pe seama persoanei vizate. În acest ultim caz, cealaltă parte ar trebui considerată ca fiind operator, chiar dacă e doar în scop de stocare a datelor, și trebuie să respecte principiile și obligațiile stabilite în RGPD.

[5] A se vedea de asemenea secțiunea V.

[6] Ca o consecință, trebuie acordată o atenție deosebită formatului datelor transmise, astfel încât să se garanteze că datele pot fi reutilizate, cu puțin efort, de către persoana vizată sau de un alt operator. A se vedea, de asemenea, secțiunea V.

În esență, acest element de portabilitate a datelor prevede posibilitatea pentru persoanele vizate nu doar de a obține și reutiliza datele, ci și de a transmite datele pe care le-au furnizat către un alt furnizor de servicii (fie în cadrul aceluiași sector de activitate, fie într-unul diferit). În plus față de furnizarea responsabilizării consumatorilor prin prevenirea „blocării", dreptul la portabilitatea datelor este de așteptat să stimuleze oportunitățile de inovare și schimbul de date cu caracter personal între operatorii de date într-un mod sigur și securizat, sub controlul persoanei vizate[7]. Portabilitatea datelor poate promova partajarea controlată și limitată către utilizatorii de date cu caracter personal între organizații și, astfel, poate îmbunătăți serviciile și experiența clienților[8]. Portabilitatea datelor poate facilita transmiterea și reutilizarea datelor cu caracter personal privind utilizatori între diferitele servicii de care aceștia sunt interesați.

- **Controlul**

Portabilitatea datelor garantează dreptul de a primi datele cu caracter personal și de a le prelucra potrivit dorințelor persoanei vizate[9].

Operatorii de date care răspund cererilor de portabilitate a datelor, în condițiile prevăzute la art. 20, nu sunt responsabili pentru prelucrarea efectuată de persoana vizată sau de o altă companie ce primește datele. Aceștia acționează în numele persoanei viate, inclusiv în cazul în care datele cu caracter personal sunt transmise direct altui operator. În acest sens, operatorul de date nu este responsabil pentru respectarea legii privind protecția datelor de către operatorul ce primește datele, întrucât acesta nu este cel care alege destinatarul. În același timp, operatorul trebuie să stabilească măsuri de protecție pentru a se asigura că aceștia acționează cu adevărat în numele persoanei vizate. De exemplu, pot stabili 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 de la persoana vizată fie anterior transmiterii, fie mai devreme, atunci când este oferit consimțământul inițial pentru prelucrare sau atunci când contractul este finalizat.

Operatorii de date ce răspund unei cereri de portabilitate a datelor nu au obligații specifice de a verifica calitatea datelor anterior transmiterii. Bineînțeles, aceste date ar trebui să fie deja exacte și actualizate, în conformitate cu principiile stabilite în art. 5 (1) din RGPD. Mai mult, portabilitatea datelor nu impune o obligație operatorului de date de a păstra datele cu caracter personal pe o perioadă mai mare decât cea necesară sau pe o perioadă de stocare mai mare decât cea specificată[10].

Foarte important, nu există nici o cerință suplimentară de a păstra datele pe o perioadă mai mare decât perioadele de păstrare aplicabile pur și simplu pentru a soluționa orice potențiale cereri viitoare de portabilitate a datelor.

[7] A se vedea aplicațiile experimentale în Europa, de exemplu MiData în UK, MesInfos / SerftData de la FING în Franța.

[8] Așa-numitele industrii autocuantificate și IoT au demonstrat beneficiul (și riscurile) de conectare a datelor cu caracter personal de la diferite aspecte ale vieții unei personae fizice, cum ar fi de fitness, activitatea și aportul de calorii pentru a oferi o imagine mai completă a vieții unei personae fizice individ într-un singur fișier .

[9] Dreptul la portabilitatea datelor nu este limitat la datele cu character personal care sunt utile și relevante pentru serviciile similare oferite de competitorii operatorului.

[10] În exemplul de mai sus, în situația în care operatorul nu păstrează o evidență a melodiilor ascultate de un utilizator, datele cu caracter personal nu pot fi incluse în cererea de portabilitate a datelor.

În situația în care datele cu caracter personal solicitate sunt prelucrate de o persoană împuternicită de operator, contractul încheiat în conformitate cu art. 28 din RGPD trebuie să includă obligația de a oferi asistență „operatorului prin măsuri tehnice și organizatorice adecvate (...) pentru a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor sale". Prin urmare, operatorul trebuie să implementeze proceduri specifice în colaborare cu persoanele împuternicite de acesta pentru a răspunde cererilor de portabilitate a datelor. În cazul operatorilor asociați, responsabilitățile fiecărui operator cu privire la prelucrarea cererilor de portabilitate a datelor trebuie alocate în mod clar printr-un contract.

În plus, operatorul ce primește datele[11] este responsabil pentru asigurarea faptului că datele portabile furnizate sunt relevante și neexcesive cu privire la noua prelucrare de date. De exemplu, în cazul unei cereri de portabilitate a datelor către un serviciu de webmail, în cazul în care cererea este folosită de persoana vizată pentru a obține e-mail-uri și de a le trimite către o platformă securizată de arhivare, noul operator de date nu are nevoie să prelucreze datele de contact ale corespondenților persoanei vizate. Dacă această informație nu este relevantă în ceea ce privește scopul noii prelucrări, nu ar trebui păstrată și prelucrată. În orice caz, operatorii care primesc date nu sunt obligați să accepte și să prelucreze datele cu caracter personal transmise în urma unei cereri de portabilitate a datelor. În mod similar, în cazul în care o persoană vizată solicită transmiterea detaliile tranzacțiilor sale bancare către un serviciu care ajută în gestionarea bugetului său, operatorul care primește datele nu trebuie să accepte taote datele sau să păstreze toate detaliile tranzacțiilor odată ce acestea au fost etichetate pentru scopurile noului serviciu. Cu alte cuvinte, datele acceptate și păstrate trebuie să fie doar cele necesare și relevante serviciului oferit de operatorul ce primește datele.

O organizație „importatoare" devine un nou operator de date cu privire la aceste date cu caracter personal și trebuie să respecte principiile enunțate la art. 5 din RGPD. Prin urmare, „noul" operator importator trebuie să precizeze în mod clar și direct scopul noii prelucrări anterior oricărei cereri de transmitere a datelor portabile, în conformitate cu cerințele de transparență enunțate la art. 14[12]. În ceea ce privește orice alt tip de prelucrare a datelor efectuată în cadrul acestei responsabilități, operatorul trebuie să aplice principiile prevăzute la art. 5, cum ar fi legalitatea, echitatea și transparența, limitarea scopului, reducerea la minimum a datelor, exactitatea, integritatea și confidențialitatea, limitarea stocării și responsabilitatea[13].

Operatorii de date care dețin date cu caracter personal ar trebui să fie pregătiți pentru a facilita persoanei vizate dreptul la portabilitatea datelor. Operatorii pot, de asemenea, să aleagă dacă acceptă date de la o persoană vizată, însă nu sunt obligați să facă acest lucru.

[11] De exemplu, primește date cu caracter personal ca urmare a unei cereri de portabilitate a datelor depusă de persoana vizată pentru un alt operator.

[12] În plus, noul operator nu ar trebui să prelucreze datele cu character personal care nu sunt relevante, iar prelucrarea trebuie să fie limitată la ceea ce este necesar petnru noile scopuri, chiar dacă datele cu caracter personal fac parte dintr-un set global de date transmise prin intermediul procesului de portabilitate. Datele cu caracter personal care nu sunt necesare pentru îndeplinirea scopului noii prelucrării ar trebui șterse cât mai curând posibil.

[13] Odată ce au fost primite de operator, datele cu caracter personal transmise ca parte a dreptului la portabilitatea datelor pot fi considerate ca fiind „furnizate de" persoana vizată și pot fi retransmise potrivit dreptului la portabilitatea datelor, în măsura în care sunt respectate celelalte condiții aplicabile acestui drept (de exemplu, baza legală a prelucrării...).

- **Portabilitatea datelor față de alte drepturi ale persoanelor vizate**

Atunci când o persoană fizică își exercită dreptul la portabilitatea datelor, ea face acest lucru fără a aduce atingere vreunui alt drept (așa cum este cazul altor drepturi din RGPD). O persoană vizată poate continua să utilizeze și să beneficieze de serviciu unui operator de date chiar și după o operațiune de portabilitate a datelor. Portabilitatea datelor nu declanșează automat ștergerea datelor[14] din sistemele operatorului și nu afectează perioada inițială de păstrare aplicabilă datelor care au fost transmise. Persoana vizată își poate exercita drepturile sale atâta timp cât operatorul de date încă prelucrează datele.

De asemenea, în cazul în care persoana vizată dorește să-și exercite dreptul său la ștergerea datelor („dreptul de a fi uitat" în conformitate cu art. 17), portabilitatea datelor nu poate fi utilizată de către un operator de date ca o modalitate de a întârzia sau de a refuza o astfel de ștergere.

În situația în care o persoană vizată constată că datele cu caracter personal solicitate potrivit dreptului la portabilitatea datelor nu răspund pe deplin cererii sale, orice solicitare suplimentară de date cu caracter personal potrivit dreptului de acces ar trebui să fie pe deplin respectată, în conformitate cu art. 15 din RGPD.

Mai mult decât atât, în cazul în care o lege europeană sau o lege națională specifică pentru alt domeniu prevede o anumită formă de portabilitate a datelor respective, trebuie luate în considerare condițiile prevăzute în aceste legi specifice pentru soluționarea unei cereri de portabilitate a datelor potrivit RGPD. În primul rând, în cazul în care din cererea înaintată de persoana vizată reiese faptul că intenția acesteia nu este de a-și exercita drepturile potrivit RGPD, ci, mai degrabă, de a-și exercita drepturile în conformitate cu legislația sectorială, doar atunci dispozițiile privind portabilitatea datelor din RGPD nu vor fi aplicabile respectivei cereri[15]. Pe de altă parte, în situația în care cererea are drept scop portabilitatea potrivit RGPD, existența unei astfel de legislații specifice nu prevalează aplicarea generală a principiului de portabilitate a datelor de la orce operatori, așa cum este prevăzut de RGPD. În schimb, trebuie evaluat, de la caz la caz, modul în care o astfel de legislație poate afecta, sau deloc, dreptul la portabilitatea datelor.

III. <u>Când se aplică portabilitatea datelor?</u>

- **Ce operațiuni de prelucrare sunt acoperite de dreptul la portabilitatea datelor?**

Respectarea RGPD impune ca operatorii să aibă un temei legal clar pentru prelucrarea datelor cu caracter personal.

În conformitate cu art. 20 (1) a) din RGPD, **pentru a intra sub incidența scopului** portabilității datelor, operațiunile de prelucrare trebuie să se bazeze pe:

[14] Așa cum este prevăzut la art. 17 din RGPD.

[15] De exemplu, dacă cererea persoanei vizate se referă în mod particular la oferirea accesului la istoricul contului banca la informațiile din contul unui furnizor de servicii, pentru scopurile precizate în Directiva privind Serviciile de Plată 2 (DSP2), un astfel de acces ar fi oferit potrivit prevederilor acestei directive.

- fie pe consimțământul persoanei vizate (în temeiul cu art. 6 (1) a) sau al art. 9 (2) a) atunci când este vorba de categorii speciale de date cu caracter personal);

- fie pe un contract în temeiul art. 6 (1) b) la care persoana vizată este parte.

Ca exemplu, titlurile cărților achiziționate de către o persoană fizică dintr-o librărie on-line sau melodiile ascultate prin intermediul unui serviciu de streaming de muzică sunt exemple de date cu caracter personal, care intră, în general, sub incidența scopului portabilității datelor, deoarece acestea sunt prelucrate pe baza derulării unui contract la care persoana vizată este parte.

RGPD nu stabilește un drept general la portabilitatea datelor pentru situațiile în care prelucrarea datelor cu caracter personal nu se bazează pe consimțământ sau contract[16]. De exemplu, nu există nicio oblicație pentru instituțiile financiare să răspundă unei cereri de portabilitate a datelor cu privire la datele cu caracter personal prelucrate ca parte a obligației de a preveni și detecta spălarea banilor și alte infracțiuni financiare; în egală măsură, portabilitatea datelor nu acoperă datele de contact profesionale prelucrate în cadrul unei afaceri pentru relațiile de afaceri în situațiile în care prelucrarea nu se bazează nici pe consimțământul persoanei vizate, nici pe contractul la care persoana vizată este parte.

Atunci când vine vorba de datele angajaților, dreptul la portabilitatea datelor se aplică, de obicei, doar dacă prelucrarea se bazează pe un contract la care persoana vizată este parte. În multe cazuri, consimțământul nu va fi considerat ca fiind liber exprimat în acest context ca urmare a dezechilibrului de putere între angajator și angajat[17]. Unele prelucrări de resurse umane au drept temei legal interesul legitim sau sunt necesare pentru respectarea obligațiilor legale specifice în domeniul ocupării forței de muncă. În practică, dreptul la portabilitatea datelor în contextul resurselor umane se va referi, fără îndoială, la unele operațiuni de prelucrare (cum ar fi serviciile de plată și compensare, recrutare internă), dar, în multe alte situații, va fi nevoie de 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 numai în cazul în care prelucrarea datelor este „efectuată prin mijloace automate“ și, prin urmare, nu acoperă majoritatea documentelor pe hârtie.

– **Ce date cu caracter personal trebuie incluse?**

În conformitate cu art. 20 (1), pentru a intra sub incidența scopului dreptului la portabilitatea datelor, datele trebuie să fie:

[16] A se vedea Considerentul 68 și art. 20 (3) din RGPD. Art. 20 (3) și Considerentul 68 prevede faptul că portabilitatea datelor nu se aplică în cazul în care prelucrarea este necesară îndeplinirea unei atribuții executate în interesul public sau în cadrul exercitării unei autorități oficialec cu care este investit operatorul sau atunci când operatorul își exercită atribuțiile publice respectă o obligație legală. Prin urmare, nu există o obligație pentru operatori să ofere portabilitatea în aceste situații. Cu toate acestea, o bună practică este reprezentată de dezvoltarea de procese prin care se răspunde în mod automat cererilor de portabilitate, cu respectarea principiilor ce guvernează dreptul la portabilitatea datelor. Un exemplu poate fi reprezentat de un serviciu guvernamental ce oferă posbilitatea de descărcare ușoară a declarațiilor personale de venit din trecut. Pentru portabilitatea datelor, o bună practică în cazul prelucrării ce are drept temei necesitatea pentru interesul legitim și pentru schemele voluntare existente pot fi consultate pag. 47 și 48 din Avizul WP29 6/2014 privind interesul legitim (WP217).

[17] Așa cum a fost subliniat de WP29 în Avizul său 8/2001 din 13 septembrie 2001 (WP48).

- date cu caracter personal care o privesc și
- date pe care persoana vizată *le-a furnizat* operatorului de date.

Art. 20 (4) prevede, de asemenea, că respectarea acestui drept nu va afecta în mod negativ drepturile și libertățile altor persoane.

Prima condiție: datele cu caracter personal ale persoanei vizate

Numai datele cu caracter personal intră în domeniul de aplicare al unei cereri de portabilitate a datelor. Prin urmare, orice date care sunt anonime[18] sau nu privesc persoana vizată nu se află în domeniul de aplicare. Cu toate acestea, datele pseudonime care pot fi legate în mod clar de o persoană vizată (de exemplu, furnizând identificatorul respectiv, conform art. 11 (2)) se află în domeniul de aplicare.

În multe situații, operatorii vor prelucra informații care conțin datele cu caracter personal ale mai multor persoane vizate. În acest caz, operatorii nu ar trebui să abordeze o interpretarea prea restrictivă a sintagmei „datele cu caracter personal referitoare la o persoană vizată". Ca exemplu, telefonul, mesajele interpersonale sau înregistrările VoIP pot include (în istoricul contului abonatului) detalii ale unor părți terțe implicate în apelurile primite sau efectuate. Cu toate că înregistrările vor conține date cu caracter personal referitoare la mai multe persoane, abonații ar trebui să poată să aibă aceste înregistrări furnizate ca răspuns la cererile de portabilitate a datelor, întrucât înregistrările se referă (de asemenea) la persoana vizată. Totuși, în situația în care aceste înregistrări sunt transmise către un nou operator, acest nou operator nu ar trebui să le prelucreze în alt scop care ar putea afecta în mod negativ drepturile și libertățile unot părți terțe (a se vedea mai jos: a treia condiție).

A doua condiție: datele furnizate de persoana vizată

Cea de-a doua condiție îngustează sfera de aplicare a datelor „furnizate" de persoana vizată.

Există multe exemple de date cu caracter personal, precum datele de cont (de exemplu, adresa poștală, numele de utilizator, vârsta), care vor fi „furnizate de" persoana vizată cu bună știință și în mod activ prin formularele online. Cu toate acestea, datele „furnizate de" persoana vizată rezultă și din observarea activității sale. În consecință, WP29 consideră că, pentru a oferi o valoare completă acestui nou drept, „furnizat de" ar trebui să includă, de asemenea, datele cu caracter personal care sunt observate din activitățile utilizatorilor, cum ar fi datele brute prelucrate de un contor inteligent sau alte tipuri de obiecte conectate[19], jurnale de activitate, istoricul utilizării site-ului sau a activităților de căutare.

Această ultimă categorie de date nu include date care sunt create de operatorul de date (folosind datele observate sau direct furnizate ca răspuns) cum ar fi un profil de utilizator creat prin analiza datelor brute colectate de contoare inteligente.

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

[19] Prin posibilitatea de a prelua datele rezultate din observarea activității sale, persoana vizată va avea, de asemenea, posibilitatea de a obține o mai bună imagine de ansamblu a opțiunilor de implementare a opțiunilor operatorului în ceea ce privește domeniul de aplicare a datelor observate și va fi într-o mai bună situație pentru a allege ce date este dispusă să ofere pentru a obține un serviciu similar și să fie conștientă în ce măsură este respectat dreptul său la viață privată.

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

- **date furnizate de persoana vizată cu bună știință și în mod activ** (spre exemplu adresă poștală, numele de utilizator, vârstă etc.)
- **date observate furnizate de persoana vizată în virtutea utilizării serviciului sau dispozitivului.** De exemplu, acestea pot include istoricul căutărilor, datele de trafic și datele de localizare. De asemenea, acestea pot include și alte date brute precum ritmul cardiac urmărit de un dispozitiv portabil.

În schimb, datele deduse și datele obținute sunt create de operator pe baza datelor „furnizate de persoana vizată”. De exemplu, rezultatul unei evaluării cu privire la starea de sănătate a unui utilizator sau la profilul creat în contextul gestionării riscurilor și a reglementărilor în domeniul financiar (de exemplu, pentru a atribui un scor de credit sau pentru a respecta normele de combatere a spălării banilor) nu poate fi considerat în sine ca fiind „furnizat de” persoana vizată. Chiar dacă aceste date pot fi parte dintr-un profil păstrat de operator și sunt deduse sau derivate din analiza datelor furnizate de persoana vizată (spre exemplu, prin intermediul acțiunilor sale), în mod obișnuit, aceste date nu pot fi luate în considerare ca fiind „furnizate de persoana vizată” și, prin urmare, nu vor intra sub incidența scopului acestui nou drept[20].

În general, având în vedere obiectivele de politică ale dreptului la portabilitatea datelor, sintagma „furnizat de persoana vizată” trebuie interpretată în sens larg și ar trebui să excludă „date deduse” și „date derivate”, care includ date cu caracter personal care sunt create de un furnizor de servicii (spre exemplu, rezultate algoritmice). Un operator poate exclude aceste date deduse, dar ar trebui să includă toate celelalte date furnizate de persoana vizată prin mijloacele tehnice prevăzute de operator[21].

Astfel, sintagma „furnizat de” include date cu caracter personal care se referă la activitatea persoanei vizate sau rezultatul din observarea comportamentului unei persoane fizice, dar nu include datele rezultate din analiza ulterioară a acestui comportament. În schimb, orice date cu caracter personal care au fost create de operator ca parte a prelucrării datelor, de exemplu printr-un proces de personalizare sau recomandare, prin clasificarea utilizatorilor sau a profilurilor reprezintă date care sunt derivate sau deduse din datele cu caracter pesonal furnizate de persoana vizată și nu intră sub incidența dreptului la portabilitatea datelor.

[20] Cu toate acestea, persoana vizată încă are „dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele cu caracter personal”, precum și informații despre „existența unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, așa cum este precizat în art. 22 (1) și (4) și, cel puțin în acele situații, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată”, potrivit art. 15 din RGPD (care se referă la dreptul de acces).

[21] Acestea includ toate datele cu privire la persoana vizată observate pe durata activităților pentru scopul pentru care au fost colectate, cum ar fi istoricul tranzacțiilor sau evidența accesărilor. Datele colectate prin intermediul urmării și înregistării persoanei vizate (cum ar fi o aplicație care înregistrează ritmul cardiac sau o tehnologie care urmărește comportamentul persoanei în timpul căutării) ar trebui considerate, de asemenea, ca fiind „furnizate de” aceasta chiar dacă datele nu sunt transmise în mod activ și cu bună știință.

A treia condiție: dreptul la portabilitatea datelor nu trebuie să aducă atingere drepturilor și libertăților altora

În ceea ce privește datele cu caracter personal privind alte persoane vizate:

A treia condiție este menită să evite recuperarea și transmiterea de date care conțin datele cu caracter personal ale altor persoane vizate (care nu și-au dat consimțământul) către un nou operator de date în situațiile în care există posibilitatea ca aceste date să fie prelucrate într-un mod care ar afecta în mod negativ drepturile și libertățile altor persoane vizate (art. 20 (4) din RGPD)[22].

Un asemenea efect negativ ar putea apărea, spre exemplu, în cazul în care transmiterea de date de la un operator la altul ar împiedica părțile terțe să-și exercite drepturile lor în calitate de persoane vizate în temeiul RGPD (precum dreptul la informare, dreptul de acces etc.).

Persoana vizată care inițiază transmiterea datelor sale către un alt operator de date, fie își oferă consimțământul către noul operator de date pentru prelucrarea, fie încheie un contract cu respectivul operator. Trebuie identificat un alt temei juridic pentru prelucrarea în situația în care datele cu caracter personal ale unor părți terțe sunt incluse în setul de date. De exemplu, un interes legitim poate fi urmărit de operatorul de date în conformitate cu art. 6 (1) f), în special în cazul în care scopul operatorului de date este de a oferi persoanei vizate un serviciu care permite acesteia să prelucreze datele cu caracter personal pentru o activitate pur personală sau de uz casnic. Operațiunile de prelucrare inițiate de persoana vizată, în contextul activității personale care privesc și au un posibil impact asupra unor părți terțe, rămân sub responsabilitatea acesteia, în măsura în care o astfel de prelucrare nu este, în nici un fel, decisă de operatorul de date.

De exemplu, un serviciu de webmail poate permite crearea unui director referitor la contactele, prietenii, rudele, familia și mediul mai larg al persoanei vizate. Din moment ce aceste date se referă la (și sunt create de) o persoană fizică identificabilă care dorește să-și exercite dreptul la portabilitatea datelor, operatorii trebuie să transmită în totalitate directorul de e-mail-uri primite și trimise către respectiva persoană vizată.

În mod similar, contul bancar al persoanei vizate poate conține datele cu caracter personal referitoare nu doar la tranzacțiile titularului de cont, ci și ale altor persoane (de exemplu, în cazul în care au transferat bani către titularul de cont). Drepturile și libertățile acestor părți terțe sunt puțin probabil să fie afectate în mod negativ de transmiterea informațiilor privind contul bancar către titularul de cont odată ce a fost înaintată o cerere de portabilitate – cu condiția ca, în ambele exemple, datele să fie folosite în același scop (de exemplu, o adresă de contact sau un istoric al contului bancar să fie folosite numai de persoana vizată).

Pe de altă parte, drepturile și libertățile părților terțe nu vor fi respectate în cazul în care noul operator de date utilizează datele cu caracter personal pentru alte scopuri, de exemplu, în

[22] Considerentul 68 prevede că „în cazul în care, într-un anumit set de date cu caracter personal, sunt implicate mai multe personae vizate, dreptul de a primi datele cu caracter personal nu ar trebui să aducă atingere drepturile și libertățile altor personae vizate, în conformitate cu prezentul Regulament”.

cazul în care operatorul care primește datele altor persoane din directorul de contact al persoanei vizate le folosește în scopuri de marketing.

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 exclusiv al utilizatorului solicitant și este gestionat numai în scop personal sau de uz casnic. Un „nou" operator ce primește date (către care au fost transmite date la solicitarea utilizatorului) nu poate utiliza datele părților terțe transmise pentru propriile scopuri, de exemplu pentru a propune acestor persoane vizate părți terțe produse și servicii de marketing. De exemplu, această informație nu ar trebui utilizată pentru a îmbogăți profilul persoanei vizate parte terță și pentru a reconstrui mediul său social, fără știrea și consimțământul acesteia[23]. Și nici nu poate fi folosită pentru a prelua informațiile referitoare astfel de părți terțe și de a crea profiluri specifice, chiar dacă datele lor cu caracter personal sunt deja deținute de operator. În caz contrar, o astfel de prelucrarea poate fi ilegală și incorectă, mai ales în cazul în care părțile terțe în cauză nu sunt informate și nu-și pot exercita drepturile în calitate de persoane vizate.

Mai mult, este o practică de conducere pentru toți operatorii de date (atât părțile care „transmit", cât și cele care „primesc") de a pune în aplicare instrumente pentru a permite 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 fizice. Acest lucru va ajuta în continuare în reducerea riscurilor pentru părțile terțe ale căror date cu caracter personal pot fi portate.

În plus, operatorii de date ar trebui să pună în aplicare mecanisme de consimțământ pentru alte persoane vizate implicate, pentru a ușura transmiterea de date pentru acele cazuri în care aceste părți terțe sunt dispuse să consimtă, de exemplu, în cazul în care doresc, de asemenea, să mute datele lor la un alt operator. O astfel de situație ar putea apărea, de exemplu, în cazul rețelelor sociale, dar depinde de operatorii de date în a decide cu privire la practica de de urmat.

În ceea ce privește datele care fac obiectul proprietății intelectuale și secretele comerciale:

Drepturile și libertățile altora sunt menționate la art. 20 (4). Chiar dacă nu este legat direct de portabilitate, acest lucru poate fi înțeles ca „inclusiv secrete comerciale sau proprietate intelectuală" și, în special drepturile de autor care protejează software. Cu toate acestea, chiar dacă aceste drepturi trebuie luate în considerare înainte de a răspunde unei cereri de portabilitate a datelor, „rezultatul acestor considerații nu ar trebui să fie un refuz de a furniza persoanei vizate toate informațiile". Mai mult, operatorul nu trebuie să refuze o cerere de portabilitate a datelor pe baza încălcării unui alt drept contractual (de exemplu, o datorie restantă sau un conflict comercial cu persoana vizată).

[23] Un serviciu de rețea socială nu ar trebui să îmbogățească profilul membrilor săi prin utilizarea datelor cu caracter personal transmise de o persoană vizată, ca parte a dreptului său la portabilitatea datelor, fără a respecta principiul transparență și, de asemenea, fără să se asigure că acestea de bazează pe un temei juridic adecvat cu rivire la această prelucrare specifică.

Dreptul la portabilitatea datelor nu este un drept pentru o persoană vizată de a abuza de informații într-un mod care ar putea fi calificat drept practică incorectă sau care ar constitui o încălcare a drepturilor de proprietate intelectuală.

Cu toate acestea, un risc potențial de afaceri nu poate, în sine, să servească drept bază pentru refuzul de a răspunde cererii de portabilitate, iar operatorii pot transmite datele cu caracter personal furnizate de persoanele vizate într-o formă prin care nu se dezvăluie informații care fac obiectul drepturilor de proprietate intelectuale și secretele comerciale.

IV. Cum se aplică regulile generale care guvernează exercitarea drepurilor persoanelor vizate în cazul portabilității datelor?

– Ce informații prealabile trebuie furnixate persoanei vizate?

În vederea respectării noului drept la portabilitatea datelor, operatorii trebuie să informeze persoanele vizate cu privire la existența noului drept la portabilitate. În situația în care datele cu caracter personal în cauză sunt colectate direct de la persoana vizată, informarea trebuie să aibă loc „la momentul în care sunt obținute datele cu caracter personal". Dacă datele cu caracter personal nu au fost obținute de la persoana vizată, operatorul trebuie să furnizeze informațiile în conformitate cu art. 13 (2) b) și art. 14 (2) c).

„În situația în care datele cu caracter personal nu au fost obținute direct de la persoana vizată", art. 14 (3) impune ca informațiile să fie furnizate într-un termen rezonabil după opținerea datelor, dar nu mai mare de 1 lună, în momentul primei comunicări cu persoana vizată sau când sunt dezvăluite datele cu caracter personal către părți terțe[24].

Atunci când datele sunt furnizate, operatorii trebuie să se asigure că se realizează o distincție între dreptul la portabilitatea datelor și alte drepturi. Prin urmare, WP29 recomandă, în special, faptul ca operatorii de date să explice în mod clar diferența între tipurile de date pe care o persoană vizată le poate primi ca urmare a exercitării dreptului de acces și dreptului la portabilitatea datelor.

În plus, Grupul de Lucru recomandă ca operatorii să includă întotdeauna informații cu privire la dreptul la portabilitatea datelor înainte ca persoanelor vizate să închidă orice cont pe care îl pot avea. Acest lucru permite utilizatorilor să țină seama de datele lor cu caracter personal, precum și să transmită cu ușurință datele către propriul dispozitiv sau către un alt furnizor înainte ca un contract să fie reziliat.

În cele din urmă, ca practică pentru operatorii „ce primesc" date, WP29 recomandă ca persoanele vizate să primească informații complete cu privire la natura datelor cu caracter personal care sunt relevante pentru îndeplinirea serviciilor lor. În plus față de ceea ce stă la baza unei prelucrări corecte, acest lucru permite utilizatorilor să limiteze riscurile pentru părțile terțe, precum și orice altă duplicare inutilă a datelor cu caracter personal, chiar în situația în care nu sunt implicate alte persoane vizate.

[24] Art. 12 impune ca operatorii să furnizeze „orice informații […] 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."

- **Cum poate operatorul să identifice persoana vizată înainte de a răspunde la cererea acesteia?**

RGPD nu prevede cerințe stricte cu privire la modul de autentificare a persoanei vizate. Cu toate acestea, art. 12 (2) din RGPD precizează că operatorul nu poate refuza să acționeze la cererea persoanei vizate pentru exercitarea drepturilor sale (inclusiv dreptul la portabilitatea datelor), cu excepția cazului în care se prelucrează date cu caracter personal pentru un scop care nu necesită identificarea persoanei vizate și se poate demonstra că nu este în măsură să identifice persoana vizată. Cu toate acestea, în conformitate cu art. 11 (2), în astfel de circumstanțe, persoana vizată poate oferi mai multe informații pentru a permite identificarea sa. În plus, art. 12 (6) prevedă că, în cazul în care un operator are îndoieli întemeiate cu privire la identitatea persoane vizate, acesta poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate. În situația în care o persoană vizată furnizeaza informații suplimentare care să permită identificarea sa, operatorul nu trebuie să refuze să acționeze asupra cererii. În cazul în care informațiile și datele colectate online sunt legate de pseudonime sau identificatori unici, operatorii pot implementa proceduri corespunzătoare care să permită unei persoane fizice să înainteze o cerere de portabilitate a datelor și să primească datele care o privesc. În orice caz, operatorii trebuie să implementeze proceduri de autentificare pentru a stabili cu certitudine identitatea persoanei vizate care solicită datele sale personale sau, în sens larg, își exercită drepturile oferite de RGPD.

De multe ori aceste proceduri există deja. Persoanele vizate sunt adesea deja autentificate de operator înainte de a încheia un contract sau de a obține consimțământul acestora. În consecință, datele cu caracter personal folosite pentru înregistrarea unei persoane fizice vizată de prelucrare pot fi, de asemenea, utilizate ca probe pentru autentificarea persoanei vizate în scopuri de portabilitate[25].

În timp ce în aceste cazuri identificarea prealabilă a persoanei vizate poate necesita o dovadă a identității sale, o asemenea verificare nu poate fi relevantă pentru evaluarea legăturii dintre date și persoana fizică în cauză, deoarece o astfel de legătură nu este legată de identitatea oficială sau juridică. În esență, capacitatea operatorului de a solicita informații suplimentare pentru a analiza identitatea unei persoanei nu poate duce la cereri excesive și la colectarea de date cu caracter personal care nu sunt relevante sau necesare pentru a consolida relația dintre persoana fizică și datele personale solicitate.

În multe cazuri, asemenea proceduri de autentificare există deja. De exemplu, numele de utilizator și parolele sunt de multe ori folosite pentru a permite persoanelor fizice să acceseze datele sale din conturile sale de e-mail, din conturile de rețele de socializare și din conturile folosite pentru diverse alte servicii, dintre care unele persoane fizice au ales să le folosească fără a dezvălui numele complet și identitatea.

Dacă volumul datelor solicitate de persoana vizată face ca transmiterea prin intermediul Internetului să fie mai degrabă problematică, decât să permită o perioadă de timp prelungită

[25] De exemplu, în situația în care prelucrarea datelor este legată de contul unui utilizatori, ar putea fi suficientă furnizarea numelui de utilizator și a parolei pentru a identifica persoana vizată.

de cel mult trei luni pentru soluționarea cererii[26], operatorul va trebui, de asemenea, să ia în considerare mijloacele alternative de furnizare a datelor, precum utilizarea de streaming sau salvarea pe un CD, DVD sau alte suporturi fizice sau să permită transmiterea directă a datelor cu caracter personal la un alt operator de date (conform art. 20 (2) din RGPD în cazul în care este fezabil din punct de vedere tehnic).

- **Care este termenul impus pentru a răspunde la o solicitare de portabilitate?**

Art. 12 (3) prevede că operatorul furnizează persoanei vizate „informații privind acțiunile întreprinse" „fără întârzieri nejustificate" și în orice caz „în cel mult o lună de la primirea cererii". Această perioadă de o lună poate fi prelungită la maximum 3 luni, ținându-se seama de complexitatea cererilor, cu condiția ca persoana vizată să fie informată în legătură cu motivele întârzierii în terme de o lună de la primirea cererii.

Există probabilitatea ca operatorii care operează servicii ale societății informaționale să fie mai bine echipate pentru a fi în măsură să răspundă cererilor într-o perioadă foarte scurtă de timp. Pentru a satisface așteptările utilizatorilor, o bună practică ar consta în definirea intervalului de timp în care se răspunde la o cerere de portabilitate a datelor și se transmite răspunsul către persoanele vizate.

Potrivit art. 12 (4), operatorii care refuză să răspundă unei cereri de portabilitate vor informa persoana vizată, în termen de o lună de la primirea cererii, cu privire la „motivele pentru care nu se ia măsuri și la posibilitatea de a depune o plângere la autoritatea de supraveghere și de a introduce o cale de atac judiciară.

Operatorii trebuie să respecte obligația de a răspunde în termenul stabilit, chiar dacă este vorba de un refuz. Cu alte cuvinte, operatorul nu poate lăsa fără răspuns o cerere de portabilitate a datelor.

- **În ce situație poate fi respinsă o cerere de portabilitate a datelor sau se poate percepe o taxă?**

Art. 12 interzice operatorului să perceapă o taxă pentru furnizarea datelor cu caracter personal, cu excepția situației în care operatorul poate demonstra că solicitările sunt în mod vădit nefondate sau excesive, „în special din cauza caracterului lor repetitiv". Pentru serviciile societății informaționale specializate în prelucrarea automată a datelor cu caracter personal, implementarea de sisteme automate precum Interfețe de Programare a Aplicațiilor (Application Programming Interfaces - APIs)[27] poate facilita schimburile cu persoana vizată și, prin urmare, poate reduce posibila sarcină ce rezultă din cererile repetitive. Așadar, ar trebui să existe foarte puține situații în care operatorul ar putea justifica refuzul de a transmite informațiile solicitate, chiar și în situația cererilor multiple de portabilitate a datelor.

În plus, nu ar trebui luat în considerare costul total al operațiunilor create pentru a răspunde cererilor de portabilitate a datelor pentru a determina excesivitatea unei cereri. În fapt, art. 12

[26] Art. 12 (3): „Operatorul furnizează informații privind acțiunile întreprinse".

[27] Interfețe de Programare a Aplicațiilor (IPA) înseamnă interfețele aplicațiilor sau serviciilor de web puse la dispoziție de operator astfel încât alte sisteme sau aplicații se pot conecta și pot lucra cu sistemele lor.

din RGPD se concentrează pe cererile adresate de o persoană vizată și nu la numărul total de cereri primite de un operator. Ca urmare, costurile totale de implementare a sistemului nu ar trebui să fie imputate persoanelor vizate și nici nu ar trebui folosite pentru a justifica refuzul de a da curs cererilor de portabilitate.

V. Cum trebuie furnizate datele portabile?

– Care sunt mijloacele preconizate a fi implementate de operator pentru furnizarea datelor?

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

Un astfel de obstacol poate fi caracterizat ca orice obstacol legal, tehnic sau financiar introdus de operator pentru a restrânge sau a încetini accesul, transmiterea sau reutilizarea de către persoana vizată sau un alt operator. De exemplu, un asemenea obstacol ar putea fi: taxele percepute pentru furnizarea datelor, lipsa interoperabilității sau accesului la un format de date sau API sau formatul prevăzut, întârzierea excesivă sau complexitatea de a prelua întregul set de date, ascunderea deliberată a setului de date sau cereri specifice și nejustificate sau excesive de standardizare sau acreditare sectorială[28].

Art. 20 (2) stabilește, de asemenea, obligații pentru operatori pentru transmiterea datelor portabile direct către alți operatori de date „atunci când este fezabil din punct de vedere tehnic“.

Fezabilitatea tehnică a transmiterii de la un operator la altul, sub controlul persoanei vizate, ar trebui evaluat de la caz la caz. Considerentul 68 clarifică în continuare limitele a ceea ce este „punct de vedere tehnic“, indicând faptul că „nu ar trebui să creeze o obligație pentru operatori de a adopta sau de a menține sisteme de prelucrare care să fie compatibile din punct de vedere tehnic“.

Este de așteptat ca operatorii să transmită date cu caracter personal într-un format interoperabil, cu toate că acest lucru nu stabilește obligații pentru alți operatori în vederea sprijinirii acestor formate. Prin urmare, transmiterea directă de la un operator la altul ar putea apărea atunci când comunicarea între cele două sisteme este posibilă, într-un mod securizat[29], și în cazul în care sistemul de primire a datelor are capacitatea, din punct de vedere tehnic, de a primi datele transmise. În situația în care obstacolele tehnice interzic transmiterea directă, operatorul trebuie să explice aceste impedimente persoanelor vizate, întrucât, în caz contrar, decizia sa va fi similară, în efectul său, unui refuz de a lua măsuri ca urmare a unei cereri a persoanei vizate (art. 12 (4)).

[28] Ar putea apărea anumite impedimente legitime, precum cele care sunt legate de drepturile și libertățile altora menționate la art. 20 (4) sau cele care se referă la serciritatea sistemelor proprii ale ooperatorilor. Operatorul va fi responsabil pentru justificarea motivului pentru care aceste obstacole ar fi legitime și de ce nu ar constitui un impediment în senstul art. 20 (1).

[29] Printr-o comunicare autentificată cu un nivel necesar de criptare a datelor..

La nivel tehnic, operatorii ar trebui să analizeze și să evalueze două căi diferite și complementare astfel încât datele portabile să fie disponibile persoanelor vizate sau altor operatori:

- o transmitere directă a întregului set de date portabile (sau anumite extrase din setul global);
- un instrument automat care permite extragerea datelor relevante.

A doua modalitate poate fi preferată de operatorii în cazurile care implică seturi complexe și mari de date, deoarece permite extragerea oricărei părți din setul de date care este relevantă pentru persoana vizată, ținând cont de cererea acesteia, poate ajuta la minimizarea riscurilor, și, eventual, permite utilizarea mecanismelor de sincronizare[30] a datelor (de exemplu, în contextul unei comunicări regulate între operatori). Aceasta poate fi o modalitate mai bună de a asigura respectarea de către „noul" operatorul și ar putea constitui o bună practică în reducerea riscurilor de confidențialitate de către operatoul inițial.

Aceste două moduri diferite și, eventual, complementare de a furniza datele portabile relevante ar putea fi implementate prin punerea la dispoziție a datelor prin diferite mijloace precum: mesagerie securizată, un server SFTP, un WebAPI sau WebPortal securizat. Persoanele vizate ar trebui să aibă posibilitatea de a utiliza un mijloc de stocare a datelor, un sistem de management al datelor personale[31] sau alte tipuri de părți terțe de încredere, pentru a deține și a stoca datele personale și pentru a permite operatorilor să aibă acces și să prelucreze date după cum este necesar.

– **Care este formatul de date așteptat?**

RGPD stabilește pentru operatori condiții de a furniza datele cu caracter personal solicitate de o persoană fizică într-un format care permite reutilizarea datelor. Mai exact, art. 20 (1) din RGPD precizează faptul că datele cu caracter personal trebuie furnizate „într-un format structurat, utilizat în mod curent și care poate fi citit automat". Considerentul 68 oferă o clarificare suplimentară că acest format ar trebui să fie interoperabil, termen ce este definit[32] în UE după cum urmează:

> *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 respective sisteme TIC deținute de acestea.*

[30] Mecanismele de sincronizare pot ajuta la îndeplinirea obligațiilor generale stabilite de art. 5 din RGPD, care prevede că „datele cu caracter personal vor fi (...) exacte și, în cazul în care este necesar, actualizate".

[31] Cu privire la sistemele de management privind informațiile cu caracter personal (SMIP), a se vedea, de exemplu, Avizul AEPD 9/2016, disponibil la https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

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

Termenii „structurat”, „utilizat în mod curent” și „care poate fi citit automat” reprezintă un set minim de cerințe care ar facilita interoperabilitatea formatului de date furnizat de operator. În acest sens, „structurat, utilizat în mod curent și care poate fi citit automat” reprezintă specificații pentru mijloace, în timp ce interoperabilitatea se referă la rezultatul dorit.

Considerentul 21 din Directiva 2013/37/UE[33][34] definește „care poate fi citit în mod automat” după cum urmează:

> *formatul de fișier care îl conține este structurat în așa fel încât aplicațiile software să poată identifica, recunoaște și extrage cu ușurință date specifice din acesta, inclusiv declarații de fapt și structura lor internă. 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 tipuri de datele potențiale care ar putea fi prelucrate de un operator, RGPD nu impune recomandări specifice cu privire la formatul datelor cu caracter personal care urmează să fie furnizat. Formatul cel mai adecvat va fi diferit între sectoare, iar formate corespunzătoare pot exista deja și ar trebui să fie întotdeauna alese pentru a atinge obiectivul de a fi interoperabil și de a oferi persoanei vizate un grad mai mare de portabilitate a datelor. Ca atare, formatele care sunt supuse unor constrângeri de licență nu ar fi considerate 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 tehnic.”* **Astfel, portabilitatea are drept scop implementarea de sisteme interoperabile, și nu sisteme compatibile**[35].

Datele cu caracter personal sunt de așteptat să fie furnizate în formate care au un nivel ridicat de abstracție de la orice format intern sau de proprietate. Ca atare, portabilitatea datelor implică un strat suplimentar de prelucrare a datelor de către operatori, în scopul de a extrage date de pe platformă și de a filtra datele personale în afara domeniului de aplicare al portabilității, cum ar fi datele deduse sau date legate de securitatea sistemelor. În acest fel, operatorii sunt încurajați să identifice în prealabil datele care intră sfera de aplicare a portabilității în propriile lor sisteme. Această prelucrare suplimentară a datelor va fi

[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) prevede clarificări ulterioare cu privire la așteptările în ceea ce privește conceptele folosite în prezentul ghid, cum ar fi *care poate fi citit în mod automat, interoperabilitate, format deschis, standard, metadate*.

[35] ISO/IEC 2382-01 definește interoperabilitatea după cum urmează: „Capacitatea de a comunica, executa programe sau de a transfera date între diferite unități funcționale într-un mod care solicită ca utilizatorul să aibă puțină cunoaștere sau deloc a caracteristicilor respectivelor unități“.

considerată ca auxiliară la prelucrarea principală a datelor, din moment ce nu se realizează pentru a atinge un nou scop definit de operator.

În cazul în care niciun format nu este utilizat în mod obișnuit pentru o anumită industrie sau într-un anumit context, **operatorii ar trebui să furnizeze date cu caracter personal, folosind formate deschise utilizate în mod obișnuit (de exemplu, XML, JSON, CSV, ...), împreună cu metadate** utile **la cel mai bun nivel posibil de granularitate**, menținând în același timp un nivel ridicat de abstractizare. Ca atare, metadatele adecvate ar trebui utilizate pentru a descrie cu exactitate semnificația informațiilor schimbate. Aceste metadate ar trebui să fie suficiente pentru a face posibile funcția și reutilizarea datelor, dar, desigur, fără a dezvălui secrete comerciale. Prin urmare, este puțin probabil ca furnizarea de versiuni PDF al mesajelor primite pe e-mail către o persoană fizică ar fi suficient de structurată sau descriptivă pentru a permite datelor din mesajele primite să fie reutilizate într-o manieră facilă. In schimb, datele de e-mail ar trebui să fie furnizate într-un format care păstrează toate metadatele, pentru a permite reutilizarea eficientă a datelor. Ca atare, atunci când se selectează un format de date în care să se furnizeze datele cu caracter personal, operatorul ar trebui să ia în considerare modul în care acest format ar avea un impact sau ar împiedica dreptul persoanei vizate de a reutiliza datele. În situațiile în care un operator este în măsură să ofere opțiuni persoanei vizate în ceea ce privește formatul datelor cu caracter personal preferat, ar trebui să fie furnizată o explicație clară a impactului respectivei alegeri. Cu toate acestea, prelucrarea suplimentară de metadate pentru unicul scop pentru care acestea ar putea fi necesare sau ar putea să răspundă unei cereri de portabilitate a datelor nu reprezintă un motiv legitim pentru o astfel de prelucrare.

WP29 încurajează în mod ferm cooperarea între părțile interesate din industrie și asociațiile profesionale în vederea elaborării unui set comun de standarde și formate interoperabile pentru a îndeplini cerințele dreptului la portabilitatea datelor. Această provocare a fost, de asemenea, abordată de Cadrul European de Interoperabilitate (CEI), care a creat o abordare convenită a interoperabilității pentru organizațiile care doresc să livreze în comun servicii publice. Având în vedere domeniul său de aplicabilitate, cadrul specifică un set de elemente comune, cum ar fi vocabularul, conceptele, principiile, politicile, orientările, recomandările, standardele, specificațiile și practicile[36].

- **Cum să faci față unei colectări mari sau complexe de date cu caracater personal?**

RGPD nu explică modul în care să fie abordată provocarea de a răspunde în situația în care apar o colectare mare de date, o structură complexă de date sau alte probleme tehnice care ar putea crea dificultăți pentru operatori sau persoane vizate.

Cu toate acestea, este important ca, în toate situațiile, persoana fizică să poate înțelege definiția, schema și structura datelor cu caracter personal care ar putea fi furnizate de operator. De exemplu, datele ar putea fi furnizate inițial într-o formă redusă prin folosirea de tablouri de bord („dashboards") care permit persoanei vizate să suporte mai degrabă subseturi

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

de date cu caracter personal, decât datele în întregime. Operatorul ar trebui să ofere o imagine de ansamblu „într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu” (a se vedea art. 12 (1) din RGPD) astfel încât persoana vizată să aibă întotdeauna informații clare referitoare la ce date să descărce sau să transmită altui operator, în legătur cu un anumit scop. De exemplu, persoanele vizate ar trebui să fie în măsură să utilizeze aplicații de software pentru a identifica, a recunoaște și a prelucra cu ușurință date specifice.

Așa cum s-a arătat mai sus, un mod practic prin care un operator poate răspunde la cererile de portabilitate a datelor poate fi reprezentat prin furnizarea unui API documentat și securizat în mod corespunzător. Acest lucru poate permite persoanelor fizice să transmită cereri pentru datele lor cu caracter personal către operator prin intermediul propriului software sau cel al unei părți terțe sau poate permite altora să facă acest lucru în numele lor (inclusiv un alt operator de date), așa cum se specifică la art. 20 (2) din RGPD. Prin acordarea accesului la date prin intermediul unui API accesibil din exterior, furnizarea unui sistem de acces mai sofisticat, care permite persoanelor fizice să transmită cereri ulterioare de date, fie ca o descărcare completă, fie ca o funcție delta care conține numai modificări de la ultima descărcare, fără ca aceste solicitări suplimentare să fie împovărâtoare pentru operator poate fi, de asemenea posibilă.

- **Cum pot fi securizate datele portabile?**

În general, operatorii trebuie să asigure „securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale, prin luarea de măsuri tehnice sau organizaționale corespunzătoare”, potrivit art. 5 (1) din RGPD.

Cu toate acestea, transmiterea datelor cu caracter personal către persoana vizată poate ridica anumite probleme de securitate:

Cum se pot asigura operatorii că datele cu caracter personal sunt transmise în mod securizate persoanei potrivite?

În timp ce portabilitatea datelor are drept scop obținerea datelor cu caracter personal din sistemul informatic al operatorului, transmiterea poate deveni o posibil sursă de risc în ceea ce privește aceste date (în special breșe de securitate în timpul transmiterii). Operatorul este responsabil pentru luarea tuturor măsurilor de securitate necesare pentru a se asigura nu numai că datele sunt transmise în siguranță (prin utilizarea end-to-end sau criptarea datelor) către destinația corectă (prin utilizarea de măsuri puternice), ci și că va continua să protejeze datele cu caracter personal rămase în sistemele sale, precum și proceduri transparente pentru soluționarea breșelor de securitate posibile[37]. Ca atare, operatorii ar trebui să evalueze riscurile specifice legate de portabilitatea datelor și să ia măsuri corespunzătoare de reducere a riscurilor.

[37] Potrivit Directivei (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune

Astfel de măsuri de reducere a riscurilor ar putea include: folosirea de informații suplimentare de autentificare, cum ar fi un secret comun sau un alt factor de autentificare, cum ar fi o parolă ce poate fi folosită o singură dată (onetime password) pentru situația în care persoana vizată trebuie deja să fie autentificată; suspendarea sau blocarea transmiterii în cazul în care există suspiciunea că respectivul cont a fost compromis; în cazul unei transmiteri directe de la un operator la altul, ar trebui folosită autentificarea prin mandat, cum ar fi autentificare pe bază de token.

Astfel de măsuri de securitate nu trebuie să fie obstructive în natură și nu trebuie să împiedice utilizatorii să își exercite drepturile lor, de exemplu prin impunerea unor costuri suplimentare.

Cum pot fi ajutați utilizatorii să își păstreze datele personale în mod securizat în propriile lor sisteme?

Prin preluarea datelor personale de la un serviciu on-line, există întotdeauna riscul ca utilizatorii să le stocheze în sisteme cu un grad mai mic de securitate decât cel oferit de serviciu. Persoana vizată care solicită datele este responsabilă pentru identificarea măsurilor potrivite pentru a asigura securitatea datelor cu caracter personal în propriul său sistem. Cu toate acestea, ar trebui să fie conștientă de acest lucru, în vederea luării de măsuri pentru a proteja informațiile pe care le-a primit. Ca un exemplu de practică, operatorii pot recomanda, de asemenea, formatul/formatele adecvat/adecvatee, instrumente de criptare și alte măsuri de securitate pentru a ajuta persoana vizată în atingerea acestui obiectiv.

* * *

Redactat în Bruxelles, 13 decembrie 2016

Pentru Grupul de Lucru,

Președinte

Isabelle FARQUE-PIERROTIN

Revizuit și adoptat la 5 aprilie 2017

Pentru Grupul de Lucru,

Președinte

Isabelle FARQUE-PIERROTIN