



Bruxelles, 29.5.2019
COM(2019) 250 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

**Orientări referitoare la Regulamentul privind un cadru pentru libera circulație a
datelor fără caracter personal în Uniunea Europeană**

Cuprins

1	Introducere.....	2
	Scopul prezentelor orientări.....	3
2	Interacțiunea dintre Regulamentul privind libera circulație a datelor fără caracter personal și Regulamentul general privind protecția datelor – seturile de date mixte.....	5
2.1	Conceptul de date fără caracter personal în Regulamentul privind libera circulație a datelor fără caracter personal.....	5
	Date cu caracter personal.....	5
	Date fără caracter personal	6
2.2	Seturi de date mixte.....	8
3	Libera circulație a datelor și eliminarea cerințelor de localizare a datelor	12
3.1	Libera circulație a datelor fără caracter personal.....	12
3.2	Libera circulație a datelor cu caracter personal.....	15
3.3	Domeniul de aplicare al Regulamentului privind libera circulație a datelor fără caracter personal	16
3.4	Activități legate de organizarea internă a statelor membre	17
4	Abordări de autoreglementare care susțin libera circulație a datelor.....	19
4.1	Portarea datelor și schimbarea furnizorilor de servicii de cloud.....	19
	Noțiunea de portabilitate și interacțiunea cu Regulamentul general privind protecția datelor..	20
4.2	Coduri de conduită și sisteme de certificare privind protecția datelor cu caracter personal	22
4.3	Consolidarea încrederii în prelucrarea datelor la nivel transfrontalier – certificarea securității.....	24
	Observații finale	24

Prezentul document a fost elaborat de Comisia Europeană numai în scop informativ. Acesta nu conține nicio interpretare cu valoare de autoritate a Regulamentului (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană și nu constituie o decizie sau o poziție a Comisiei Europene. Documentul nu aduce atingere niciunei astfel de decizii sau poziții a Comisiei Europene și nici competențelor Curții de Justiție a Uniunii Europene de a interpreta regulamentul în conformitate cu tratatele UE.

1 Introducere

Într-o economie bazată din ce în ce mai mult pe date, fluxurile de date se află în centrul proceselor de afaceri ale societăților de toate dimensiunile și din toate sectoarele. Noile tehnologii digitale creează oportunități noi pentru publicul larg, întreprinderile și administrațiile publice din Uniunea Europeană („UE”).

Pentru a spori și mai mult schimbul transfrontalier de date și pentru a stimula economia datelor, în noiembrie 2018, Parlamentul European și Consiliul au adoptat Regulamentul (UE) 2018/1807 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană¹ („Regulamentul privind libera circulație a datelor fără caracter personal”), pe baza unei propuneri din partea Comisiei Europene („Comisia”). Regulamentul se aplică de la 28 mai 2019. Principiul liberei circulații a datelor cu caracter personal este deja prevăzut în Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE („Regulamentul general privind protecția datelor”)². Prin urmare, există în prezent un cadru cuprinzător privind un spațiu european comun al datelor și libera circulație a tuturor datelor în Uniunea Europeană³.

Regulamentul privind libera circulație a datelor fără caracter personal creează securitatea juridică necesară pentru ca întreprinderile să-și prelucrez datele oriunde doresc în UE, crește încrederea în serviciile de prelucrare a datelor și combate practicile privind dependența de furnizor. Acest lucru va spori posibilitățile de alegere ale clienților, va îmbunătăți eficiența și va stimula adoptarea tehnologiilor de tip cloud, ceea ce va conduce la economii semnificative pentru întreprinderile din UE. Un studiu arată că întreprinderile din UE pot economisi 20-50 % din costurile lor informatice prin migrarea către tehnologiile de tip cloud⁴.

Datorită celor două regulamente, datele pot circula liber între statele membre, permițând utilizatorilor de servicii de prelucrare a datelor să utilizeze datele colectate pe diferite piețe din UE pentru a-și îmbunătăți productivitatea și competitivitatea. Prin urmare, utilizatorii pot beneficia pe deplin de economiile de scară oferite de importanta piață a UE, îmbunătățindu-și competitivitatea la nivel mondial și sporind interconectivitatea economiei europene a datelor.

¹ Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană, JO L 303, 28.11.2018, p. 59.

² Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), JO L 119, 4.5.2016, p. 1.

³ Regulamentul general privind protecția datelor acoperă, de asemenea, Spațiul Economic European (SEE), care include Islanda, Liechtenstein și Norvegia. În plus, Regulamentul privind libera circulație a datelor fără caracter personal are relevanță pentru SEE.

⁴ Deloitte: *Measuring the economic impact of cloud computing in Europe* (Măsurarea impactului economic al tehnologiei de tip cloud computing în Europa), SMART 2014/0031, 2016. Document disponibil online la: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

Regulamentul privind libera circulație a datelor fără caracter personal are trei caracteristici importante:

- ca regulă generală, interzice statelor membre să impună cerințe cu privire la localizarea datelor. Excepțiile de la această regulă pot fi justificate numai din motive de siguranță publică în conformitate cu principiul proporționalității;
- instituie un mecanism de cooperare pentru a se asigura că autoritățile competente își pot exercita în continuare toate drepturile de care dispun în ceea ce privește accesarea datelor care sunt prelucrate în alt stat membru;
- prevede stimulente pentru ca industria să elaboreze, cu sprijinul Comisiei, coduri de conduită de autoreglementare privind schimbarea furnizorilor de servicii și portarea datelor.

Scopul prezentelor orientări

Prezentele orientări sunt conforme cu articolul 8 alineatul (3) din Regulamentul privind libera circulație a datelor fără caracter personal, care prevede obligația Comisiei de a publica orientări privind interacțiunea dintre acest regulament și Regulamentul general privind protecția datelor, „în special în ce privește seturile de date compuse din date cu caracter personal și date fără caracter personal”.

Prezentele orientări își propun să ajute utilizatorii – în special întreprinderile mici și mijlocii – să înțeleagă interacțiunea dintre Regulamentul privind libera circulație a datelor fără caracter personal și Regulamentul general privind protecția datelor⁵. Prin urmare, orientările abordează în special: (i) conceptele de date fără caracter personal și de date cu caracter personal; (ii) principiile liberei circulații a datelor și interzicerii cerințelor de localizare a datelor în temeiul ambelor regulamente și (iii) noțiunea de portabilitate a datelor în temeiul Regulamentului privind libera circulație a datelor fără caracter personal. Acestea vizează, de asemenea, cerințele de autoreglementare prevăzute în cele două regulamente.

Regulamentul privind libera circulație a datelor fără caracter personal vizează doar „datele, altele decât datele cu caracter personal”, astfel cum sunt definite în Regulamentul general privind protecția datelor. Regulamentul general privind protecția datelor reglementează prelucrarea datelor cu caracter personal, care reprezintă o parte esențială a cadrului UE privind protecția datelor⁶. Acesta a intrat în vigoare în statele membre la 25 mai 2018.

⁵ Considerentul 37 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană.

⁶

- Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), JO L 119/1, 4.5.2016, p. 1.
- Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE, JO L 295, 21.11.2018, p. 39.

Regulamentul stabilește norme armonizate de protecție a persoanelor din UE/SEE în ceea ce privește prelucrarea datelor lor cu caracter personal și libera circulație a acestor date. Regulamentul general privind protecția datelor: (i) specifică informațiile care constituie date cu caracter personal; (ii) stabilește temeiul juridic pentru prelucrarea acestora și (iii) definește drepturile și obligațiile care trebuie respectate la prelucrarea acestor date⁷, printre alte dispoziții. În ceea ce privește principiul liberei circulații a datelor cu caracter personal, articolul 1 alineatul (3) din Regulamentul general privind protecția datelor prevede că „libera circulație a datelor cu caracter personal în interiorul Uniunii nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.”

În majoritatea situațiilor reale, este foarte probabil ca un set de date să fie compus atât din date cu caracter personal, cât și din date fără caracter personal. Acesta este adesea denumit „set de date mixte”. În secțiunea 2.2 de mai jos se explică mai detaliat interacțiunea dintre Regulamentul privind libera circulație a datelor fără caracter personal și Regulamentul general privind protecția datelor în ceea ce privește seturile de date mixte.

Din motive de claritate, nu există obligații contradictorii în temeiul Regulamentului general privind protecția datelor și al Regulamentului privind libera circulație a datelor fără caracter personal.

-
- Directiva (UE) 2016/680 a Parlamentului European și a Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, JO L 119, 4.5.2016, p. 89.
 - Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), JO L 201, 31.7.2002, p. 37 (în prezent în curs de revizuire).

⁷ Orientări suplimentare privind diferite aspecte ale Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) și ale legislației europene privind protecția datelor sunt disponibile pe pagina de internet a Comitetului european pentru protecția datelor, care a emis o serie de orientări în conformitate cu articolul 70 din Regulamentul general privind protecția datelor, disponibile la adresa: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_ro. Pagina de internet relevantă conține, de asemenea, trimiteri la orientări, recomandări și alte documente emise de către predecesorul Comitetului european pentru protecția datelor – Grupul de lucru „Articolul 29”. În plus, pentru a sensibiliza cetățenii și întreprinderile cu privire la Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), Comisia a publicat o comunicare privind protecția datelor care conține orientări privind aplicarea directă a RGPD (COM/2018/043 final), disponibilă la adresa: <https://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043>

2 Interacțiunea dintre Regulamentul privind libera circulație a datelor fără caracter personal și Regulamentul general privind protecția datelor – seturile de date mixte

2.1 Conceptul de date fără caracter personal în Regulamentul privind libera circulație a datelor fără caracter personal

Obiectivul Regulamentului privind libera circulație a datelor fără caracter personal⁸ este de a asigura libera circulație a datelor, altele decât datele cu caracter personal. În întregul text, regulamentul utilizează termenul „date”, care ar trebui înțeles ca „date, altele decât datele cu caracter personal definite la articolul 4 punctul 1 din Regulamentul (UE) 2016/679 [Regulamentul general privind protecția datelor]”⁹. Astfel de date, denumite și „**date fără caracter personal**” în prezentul document, sunt definite prin opoziție (*a contrario*) cu datele cu caracter personal, astfel cum sunt prevăzute în Regulamentul general privind protecția datelor.

Date cu caracter personal

Regulamentul general privind protecția datelor prevede următoarele: „«date cu caracter personal» înseamnă orice informații privind o persoană fizică identificată sau identificabilă («persoana vizată»); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;”

Datelor cu caracter personal li s-a dat în mod intenționat o definiție largă, care a rămas, în esență, neschimbată în Regulamentul general privind protecția datelor comparativ cu legislația anterioară¹⁰. În avizul său nr. 4/2007 privind conceptul de date cu caracter personal începând cu 20 iunie 2007, WP 136, Grupul de lucru „Articolul 29”¹¹ a abordat deja diferite aspecte

⁸ Articolul 1 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană.

⁹ A se vedea articolul 3 alineatul (1) din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană.

¹⁰ A se vedea articolul 2 litera (a) din Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (data încetării: 24 mai 2018, abrogată prin Regulamentul general privind protecția datelor). A se vedea, de asemenea, jurisprudența Curții de Justiție privind definiția datelor cu caracter personal, care admite interpretarea largă a acestei noțiuni, de exemplu hotărârea Curții de Justiție din 29 ianuarie 2009, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54; hotărârea Curții de Justiție din 24 noiembrie 2011, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; hotărârea Curții de Justiție din 19 octombrie 2016, *Patrick Breyer/Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

¹¹ Grupul de lucru „Articolul 29” a fost un organism consultativ care a oferit Comisiei consiliere cu privire la aspectele legate de protecția datelor și care a contribuit la elaborarea unor politici armonizate de protecție a datelor în UE. După ce Regulamentul general privind protecția datelor a intrat în vigoare la 25 mai 2018, Grupul de lucru „Articolul 29” a fost succedat de Comitetul european pentru protecția datelor.

legate de definiția datelor cu caracter personal, cum ar fi „orice informație”, „referitoare la”, „identificată sau identificabilă”.

Pseudonimizarea datelor cu caracter personal pentru a disimula identitatea unei persoane este o practică obișnuită în domenii precum cercetarea. **Pseudonimizarea** constituie prelucrarea datelor cu caracter personal în așa fel încât să nu fie posibilă atribuirea acestora unei anumite persoane fără a se utiliza informații suplimentare. Aceste informații suplimentare sunt păstrate separat și sunt securizate prin măsuri organizatorice sau tehnice (de exemplu, prin criptare)^{12,13}. Cu toate acestea, datele care au fost pseudonimizate sunt considerate în continuare informații despre o persoană identificabilă dacă pot fi atribuite acestei persoane prin utilizarea unor informații suplimentare¹⁴. Aceste date **constituie date cu caracter personal** în conformitate cu Regulamentul general privind protecția datelor.

Date fără caracter personal

În cazul în care datele nu sunt „date cu caracter personal”, astfel cum sunt definite în Regulamentul general privind protecția datelor, acestea sunt **fără caracter personal**. Datele fără caracter personal pot fi clasificate în funcție de origine astfel:

- în primul rând, date care inițial nu aveau legătură cu o persoană fizică identificată sau identificabilă, cum ar fi datele privind condițiile meteorologice generate de senzorii instalați pe turbinele eoliene sau datele privind nevoile de întreținere ale utilajelor industriale;
- în al doilea rând, date care au fost inițial date cu caracter personal, dar care au fost ulterior **anonimizate**¹⁵. „Anonimizarea” datelor cu caracter personal este diferită de pseudonimizare (a se vedea mai sus), deoarece datele anonimizate în mod corespunzător

¹² A se vedea articolul 4 alineatul (5) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), care definește „pseudonimizarea”.

¹³ De exemplu, se poate considera că un studiu de cercetare privind efectele unui nou medicament a făcut obiectul pseudonimizării dacă datele cu caracter personal ale participanților la studiu ar fi înlocuite cu atribute unice (de exemplu, numere sau coduri) în documentația de cercetare, iar datele lor cu caracter personal ar fi păstrate separat împreună cu atributele unice alocate, într-un document securizat (de exemplu, într-o bază de date protejată cu parolă).

¹⁴ A se vedea considerentul 26 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

¹⁵ A se vedea considerentul 26 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), care prevede că „principiile protecției datelor ar trebui, prin urmare, să nu se aplice informațiilor anonime, adică informațiilor care nu sunt legate de o persoană fizică identificată sau identificabilă sau datelor cu caracter personal care sunt anonimizate astfel încât persoana vizată nu este sau nu mai este identificabilă.”

nu pot fi atribuite unei anumite persoane, nici măcar prin utilizarea unor date suplimentare¹⁶ și, prin urmare, constituie date fără caracter personal.

Evaluarea anonimizării în mod corespunzător a datelor depinde de circumstanțele specifice și unice ale fiecărui caz individual¹⁷. Mai multe exemple de reidentificare a seturilor de date care ar fi trebuit să fi fost anonimizate au arătat că o astfel de evaluare poate fi solicitantă¹⁸. Pentru a se stabili dacă o persoană este identificabilă, ar trebui să se ia în considerare toate mijloacele pe care este probabil, în mod rezonabil, să le utilizeze un operator sau o altă persoană în scopul identificării, în mod direct sau indirect, a persoanei respective¹⁹.

Exemple de date fără caracter personal

- Datele care sunt agregate în așa fel încât evenimentele individuale (cum ar fi călătoriile individuale în străinătate sau tiparele de călătorie ale unei persoane care ar putea constitui date cu caracter personal) nu mai sunt identificabile pot fi calificate drept date anonime²⁰. Datele anonime sunt utilizate, de exemplu, în statistici sau în rapoartele privind vânzările (de exemplu, pentru a evalua popularitatea unui produs și caracteristicile acestuia).
- Datele de tranzacționare de înaltă frecvență din sectorul financiar sau datele privind agricultura de precizie care contribuie la monitorizarea și la optimizarea utilizării pesticidelor, a substanțelor nutritive și a apei.

¹⁶ A se vedea hotărârea Curții de Justiție din 19 octombrie 2016, Patrick Breyer/Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779. Curtea de Justiție a precizat că adresa de protocol internet (adresa IP) dinamică poate face parte din categoria datelor cu caracter personal chiar dacă o parte terță (de exemplu, furnizorul de servicii de internet) deține date suplimentare, care ar permite identificarea persoanei în cauză. Posibilitatea de identificare a persoanei respective trebuie să constituie un mijloc care ar putea fi utilizat în mod rezonabil în scopul acestei identificări, indiferent dacă este efectuată în mod direct sau indirect.

¹⁷ Anonimizarea datelor ar trebui să fie întotdeauna efectuată utilizând cele mai recente tehnici de anonimizare de ultimă generație.

¹⁸ Pentru exemple privind reidentificarea datelor presupus anonimizate, a se vedea studiul privind viitoarele fluxuri de date realizat pentru Comisia ITRE a Parlamentului European de către Blackman, C. și Forge, S. și intitulat *Data Flows – Future Scenarios: In-Depth Analysis for the ITRE Committee* (Fluxuri de date – Scenarii viitoare: Analiză aprofundată pentru Comisia ITRE), 2017, p. 22, caseta 2. Document disponibil online la: [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA\(2017\)607362_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf)

¹⁹ A se vedea considerentul 26 din Regulamentul (UE) 2016/679 (Regulamentul general privind protecția datelor), care menționează că „pentru a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace pentru identificarea persoanei fizice, ar trebui luați în considerare toți factorii obiectivi, precum costurile și intervalul de timp necesare pentru identificare, ținându-se seama atât de tehnologia disponibilă la momentul prelucrării, cât și de dezvoltarea tehnologică.”

²⁰ A se vedea documentul „Avizul 05/2014 privind tehnicile de anonimizare” elaborat de Grupul de lucru „Articolul 29”, adoptat la 10 aprilie 2014, GL216, p. 9, care specifică următoarele: „Numai în cazul în care operatorul ar agrega datele la un nivel la care evenimentele individuale nu mai sunt identificabile, setul de date rezultat poate fi calificat drept anonim. De exemplu: în cazul în care o organizație colectează date privind deplasările individuale, tiparele de călătorie individuale la nivelul evenimentelor ar continua să poată fi considerate drept date cu caracter personal pentru fiecare parte, atât timp cât operatorul (sau orice altă parte) are în continuare acces la datele primare colectate inițial, chiar dacă identificatorii direcți au fost eliminați din setul furnizat terților. Însă, în cazul în care operatorul ar șterge datele primare și doar ar furniza terților statistici agregate la un nivel superior, cum ar fi «în zilele de luni, pe traiectoria X există un număr de pasageri cu 160 % mai mare decât în zilele de marți», aceste date s-ar califica drept date anonime.”

Cu toate acestea, în cazul în care se poate stabili o legătură în orice fel între datele fără caracter personal și o persoană, care să permită identificarea acesteia fie în mod direct, fie indirect, datele respective trebuie considerate ca fiind date cu caracter personal.

De exemplu, dacă un raport de control al calității privind o linie de producție permite corelarea datelor cu anumiți lucrători din fabrică (de exemplu, cei care stabilesc parametrii de producție), atunci datele ar putea fi considerate drept date cu caracter personal și trebuie aplicate prevederile Regulamentului general privind protecția datelor. Aceleași norme se aplică atunci când evoluțiile tehnologice și analiza datelor permit convertirea datelor anonimizate în date cu caracter personal.²¹

Întrucât definiția datelor cu caracter personal se referă la „persoane fizice”, seturile de date care conțin numele și datele de contact ale persoanelor juridice sunt, în principiu, date fără caracter personal²². Cu toate acestea, în anumite situații, acestea pot fi date cu caracter personal²³. Acesta va fi cazul dacă, de exemplu, numele persoanei juridice este același ca cel al unei persoane fizice care o deține sau dacă informațiile se referă la o persoană fizică identificată sau identificabilă²⁴.

2.2 Seturi de date mixte

Regulamentul privind libera circulație a datelor fără caracter personal și Regulamentul general privind protecția datelor abordează libera circulație a datelor în UE din două perspective diferite.

Regulamentul privind libera circulație a datelor fără caracter personal prevede o interdicție generală în ceea ce privește cerințele de localizare a datelor pentru datele fără caracter personal. Articolul 4 alineatul (1) din regulament interzice cerințele de localizare a datelor, cu excepția cazului în care acestea sunt justificate din motive de siguranță publică, în conformitate cu principiul proporționalității.

²¹ În cazul în care datele cu caracter personal sunt prelucrate în mod ilegal sau dacă prelucrarea încalcă în alt mod Regulamentul general privind protecția datelor, persoanele vizate (persoane fizice) au dreptul, în temeiul Regulamentului general privind protecția datelor, de a depune o plângere la o autoritate națională de supraveghere („autoritatea pentru protecția datelor”) din UE sau de a introduce o cale de atac efectivă în fața unei instanțe naționale. Sarcinile și competențele autorităților naționale de supraveghere sunt reglementate în capitolul VI secțiunea 2 din Regulamentul general privind protecția datelor.

²² Considerentul 14 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) prevede că „prezentul regulament nu se aplică prelucrării datelor cu caracter personal care privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și datele de contact ale persoanei juridice.” Totuși, această dispoziție trebuie citită în lumina definiției datelor cu caracter personal de la articolul 4 alineatul (1) din Regulamentul general privind protecția datelor.

²³ A se vedea hotărârea Curții de Justiție din 9 noiembrie 2010 în cauzele conexate Volker und Markus Schecke GbR, C-92/09 și Hartmut Eifert, C-93/09/Land Hessen, ECLI:EU:C:2010:662, punctul 52.

²⁴ https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_ro

Regulamentul general privind protecția datelor, pe lângă asigurarea unui nivel ridicat de protecție a datelor cu caracter personal, asigură libera circulație a datelor cu caracter personal. În conformitate cu articolul 1 alineatul (3) din regulament, libera circulație a datelor cu caracter personal „nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.” Ambele regulamente prevăd libera circulație a „tuturor” datelor în UE. Dispozițiile specifice sunt abordate în secțiunile 3.1 și 3.2.

Un set de date mixte constă atât în date cu caracter personal, cât și în date fără caracter personal. Seturile de date mixte reprezintă majoritatea seturilor de date utilizate în economia datelor și sunt larg răspândite datorită evoluțiilor tehnologice, cum ar fi internetul obiectelor (și anume, obiectele conectate digital), inteligența artificială și tehnologiile care permit analiza volumelor mari de date.

Exemple de seturi de date mixte:

- certificatul de atestare fiscală al unei societăți, care menționează numele și numărul de telefon ale directorului general al societății;
- seturile de date de la o bancă, în special cele care conțin informații referitoare la clienți și detaliile tranzacțiilor, cum ar fi servicii de plată (carduri de credit și de debit), aplicații de gestionare a relațiilor dintre parteneri (PMR) și acorduri de împrumut, precum și documente care combină date referitoare atât la persoanele fizice, cât și la cele juridice;
- datele statistice anonimizate ale unei instituții de cercetare și datele primare colectate inițial, cum ar fi răspunsurile respondenților individuali la întrebările chestionarului statistic;
- baza de date a unei societăți cu privire la problemele informatice și soluțiile acestora, bazată pe rapoarte individuale privind incidentele informatice;
- datele referitoare la internetul obiectelor, dintre care unele date permit formularea unor ipoteze cu privire la persoane identificabile (de exemplu, prezența la o anumită adresă și modele de utilizare) și
- analiza datelor privind registrul de exploatare al echipamentelor de fabricație din industria prelucrătoare.

Exemplu: servicii de gestionare a relațiilor cu clienții

Unele bănci utilizează servicii de gestionare a relațiilor cu clienții (CRM) furnizate de terți care necesită punerea la dispoziție în mediul CRM a datelor unui client. Datele conținute în cadrul serviciului CRM vor include orice informații necesare pentru gestionarea eficientă a interacțiunii cu clienții, cum ar fi adresa lor poștală și de e-mail, numărul lor de telefon, produsele și serviciile pe care le cumpără și rapoartele de vânzare, inclusiv datele agregate. Prin urmare, aceste date pot include atât date cu caracter personal, cât și date fără caracter personal privind clienții.

În ceea ce privește seturile de date mixte, Regulamentul privind libera circulație a datelor fără caracter personal²⁵ prevede următoarele:

„În cazul unui set de date compus atât din date cu caracter personal, cât și din date fără caracter personal, prezentul regulament se aplică părții din set cu date fără caracter personal. În cazul în care datele cu caracter personal și cele fără caracter personal dintr-un set de date sunt legate între ele în mod indisolubil, prezentul regulament nu aduce atingere aplicării Regulamentului (UE) 2016/679.”

Aceasta înseamnă că, în cazul unui set de date care cuprinde atât date cu caracter personal, cât și date fără caracter personal:

- Regulamentul privind libera circulație a datelor fără caracter personal se aplică părții din set cu date fără caracter personal;
- prevederea privind libera circulație a datelor din Regulamentul general privind protecția datelor²⁶ se aplică părții din set cu date cu caracter personal și
- în cazul în care partea cu date fără caracter personal și părțile cu date cu caracter personal sunt „legate în mod indisolubil”, drepturile și obligațiile în materie de protecție a datelor care decurg din Regulamentul general privind protecția datelor se aplică pe deplin întregului set de date mixte, inclusiv atunci când datele cu caracter personal reprezintă doar o mică parte din setul de date²⁷.

Această interpretare este conformă cu dreptul la protecția datelor cu caracter personal garantat de Carta drepturilor fundamentale a Uniunii Europene²⁸ și cu considerentul 8 din Regulamentul privind libera circulație a datelor fără caracter personal²⁹. Considerentul 8 din regulamentul menționat prevede următoarele: „Cadru juridic privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, în special Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului [...] și Directivele (UE) 2016/680 [...] și 2002/58/CE [...] ale Parlamentului European și ale Consiliului nu sunt afectate de prezentul regulament”.

²⁵ Articolul 2 alineatul (2) din regulament.

²⁶ Articolul 1 alineatul (3) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor). A se vedea, de asemenea, secțiunea 3.2.

²⁷ Astfel cum se reamintește în documentul de lucru al serviciilor Comisiei *Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union* (Evaluarea impactului care însoțește Propunerea de regulament al Parlamentului European și al Consiliului privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană) [SWD (2017) 304 final], partea 1/2, p. 3, „indiferent de cât de multe dintre datele cu caracter personal sunt incluse în seturile de date mixte, trebuie respectate în totalitate prevederile RGPD [Regulamentul general privind protecția datelor] în ceea ce privește partea din set cu date cu caracter personal”.

²⁸ Carta drepturilor fundamentale a Uniunii Europene, JO C 362, 26.10.2012, p. 391.

²⁹ Considerentul 8 din regulament.

Exemplu practic:

O societate care își desfășoară activitatea pe teritoriul UE oferă servicii prin intermediul unei platforme. Întreprinderile (clienții) își încarcă documentele care conțin seturi de date mixte pe platformă. În calitate de „operator”, întreprinderea care încarcă documentele trebuie să se asigure că prelucrarea respectă Regulamentul general privind protecția datelor. Prin prelucrarea setului de date în numele operatorului, societatea care oferă servicii („persoana împuternicită de către operator”) trebuie să stocheze și să prelucreze datele în conformitate cu Regulamentul general privind protecția datelor, de exemplu pentru a se asigura că se garantează un nivel adecvat de securitate în ceea ce privește datele, inclusiv prin intermediul criptării.

Conceptul de „legat în mod indisolubil” nu este definit de niciunul dintre cele două regulamente³⁰. Din motive practice, acesta se poate referi la o situație în care un set de date conține date cu caracter personal, precum și date fără caracter personal, iar separarea celor două tipuri de date fie ar fi imposibilă, fie ar fi considerată de către operator ca ineficientă din punct de vedere economic sau nefezabilă din punct de vedere tehnic. De exemplu, atunci când cumpără sisteme de CRM și sisteme de raportare a vânzărilor, societatea ar trebui să își dubleze costul software-ului prin achiziționarea unor software-uri separate pentru sistemele de CRM (date cu caracter personal) și pentru sistemele de raportare a vânzărilor (date agregate/fără caracter personal) bazate pe datele CRM.

Separarea setului de date ar putea, de asemenea, să reducă în mod semnificativ valoarea acestuia. În plus, natura schimbătoare a datelor (a se vedea secțiunea 2.1) face mai dificilă diferențierea clară și, prin urmare, separarea diferitelor categorii de date.

Un aspect important este faptul că niciunul dintre cele două regulamente nu obligă întreprinderile să separe seturile de date pe care le controlează sau prelucrează.

În consecință, un set de date mixte va fi supus, în general, obligațiilor operatorilor și ale persoanelor împuternicite de către operatori și va respecta drepturile persoanelor vizate stabilite prin Regulamentul general privind protecția datelor.

Prelucrarea datelor privind sănătatea

Datele privind sănătatea pot face parte dintr-un set de date mixte. Printre exemple se numără dosarele electronice de sănătate, trialurile clinice sau seturile de date colectate de diverse aplicații mobile de sănătate și bunăstare (cum ar fi aplicațiile pentru măsurarea stării noastre de sănătate, cele care ne aduc aminte să ne luăm medicamentele și cele care ne urmăresc progresele înregistrate cu privire la starea fizică)³¹. Diviziunea exactă dintre datele cu caracter

³⁰ Regulamentul privind libera circulație a datelor fără caracter personal și Regulamentul general privind protecția datelor.

³¹ Dezvoltarea și exploatarea de aplicații de sănătate mobilă necesită respectarea strictă a normelor Regulamentului general privind protecția datelor. Aceste cerințe vor fi precizate mai în detaliu în Codul de conduită privind protecția vieții private pentru aplicațiile de sănătate mobilă, aflat în prezent în curs de elaborare.

personal și cele fără caracter personal din aceste seturi de date este din ce în ce mai neclară odată cu evoluțiile tehnologice. În consecință, prelucrarea acestora trebuie să fie conformă cu Regulamentul general privind protecția datelor, în special (dat fiind faptul că datele privind sănătatea reprezintă o categorie specială de date în conformitate cu regulamentul) cu articolul 9, care prevede o interdicție generală a prelucrării categoriilor speciale de date și excepțiile de la această interdicție.

Datele din seturile de date mixte care conțin date privind sănătatea pot constitui o sursă valoroasă de informații, de exemplu pentru cercetări medicale suplimentare, pentru măsurarea efectelor secundare ale unui medicament prescris, în scopuri statistice privind bolile sau pentru dezvoltarea de noi servicii sau tratamente medicale. Cu toate acestea, Regulamentul general privind protecția datelor trebuie respectat atunci când se efectuează operațiunile inițiale de prelucrare și atunci când se efectuează operațiuni suplimentare de prelucrare a datelor. Prin urmare, orice astfel de prelucrare a datelor privind sănătatea trebuie să aibă un temei juridic valabil³² și o justificare corespunzătoare, să fie sigură și să ofere garanții suficiente.

În cele din urmă, este esențial ca persoanele fizice și întreprinderile să aibă securitate juridică și încredere în prelucrarea datelor. Acest lucru este, de asemenea, vital pentru economia datelor. Cele două regulamente asigură acest lucru și urmăresc obiectivul de a nu modifica libera circulație a datelor.

3 Libera circulație a datelor și eliminarea cerințelor de localizare a datelor

Prezenta secțiune explică mai în detaliu conceptul de cerințe de localizare a datelor în temeiul Regulamentului privind libera circulație a datelor fără caracter personal și pe cel al principiului liberei circulații prevăzut de Regulamentul general privind protecția datelor. Deși aceste dispoziții vizează statele membre, ele pot ajuta întreprinderile să aibă o imagine mai exactă asupra modului în care cele două regulamente contribuie la libera circulație a tuturor datelor în cadrul UE.

3.1 Libera circulație a datelor fără caracter personal

Regulamentul privind libera circulație a datelor fără caracter personal³³ prevede că „cerințele de localizare a datelor sunt interzise, cu excepția cazului în care acestea sunt justificate din motive de siguranță publică, în conformitate cu principiul proporționalității.”

Cerințele de localizare a datelor sunt definite³⁴ ca „orice obligație, interdicție, condiție, limită sau altă cerință prevăzută în actele cu putere de lege sau actele administrative ale unui

Pentru mai multe informații privind stadiul elaborării acestuia, a se vedea: <https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps>

³² A se vedea articolul 6 alineatul (1) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

³³ Articolul 4 alineatul (1) din regulament.

stat membru sau care rezultă din practicile administrative generale și consecvențe ale unui stat membru și ale organismelor de drept public, inclusiv în domeniul achizițiilor publice, fără a aduce atingere Directivei 2014/24/UE, care impune prelucrarea datelor pe teritoriul unui anumit stat membru sau împiedică prelucrarea datelor în orice alt stat membru³⁵.”.

Definiția ilustrează faptul că măsurile de restricționare a liberei circulații a datelor în cadrul UE pot lua diverse forme. Acestea pot fi stabilite prin legi și prin regulamente și dispoziții administrative sau pot fi rezultatul unor practici administrative generale și coerente. În plus, interzicerea cerințelor de localizare a datelor acoperă atât măsurile directe, cât și pe cele indirecte care ar restricționa libera circulație a datelor fără caracter personal.

Cerințele directe de localizare a datelor pot consta, de exemplu, în obligația de a stoca date într-un amplasament geografic specific (de exemplu, serverele trebuie să se afle într-un anumit stat membru) sau o obligație de a respecta cerințe tehnice naționale unice (de exemplu, datele trebuie să utilizeze formate naționale specifice).

Cerințele indirecte de localizare a datelor, care ar împiedica prelucrarea datelor fără caracter personal în orice alt stat membru, se pot prezenta sub diverse forme. Acestea pot include cerințe de utilizare a instalațiilor tehnologice care sunt certificate sau aprobate într-un anumit stat membru sau alte cerințe care au ca efect faptul de a face mai dificilă prelucrarea datelor în afara unei anumite zone geografice sau a unui anumit teritoriu din Uniunea Europeană^{36,37}.

Atunci când se stabilește dacă o măsură specifică reprezintă o cerință indirectă de localizare a datelor trebuie să se ia în considerare circumstanțele specifice fiecărui caz.

Regulamentul privind libera circulație a datelor fără caracter personal³⁸ se referă la conceptul de **siguranță publică**, astfel cum este subliniat în jurisprudența Curții de Justiție a Uniunii Europene. Siguranța publică „cuprinde atât securitatea internă, cât și cea externă a unui stat

³⁴ Articolul 3 alineatul (5) din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană.

³⁵ Trebuie remarcat faptul că lipsa de securitate juridică cu privire la amploarea cerințelor legitime și nelegitime de localizare a datelor limitează și mai mult opțiunile aflate la dispoziția actorilor de pe piață și a sectorului public în ceea ce privește localizarea prelucrării datelor [a se vedea considerentul 4 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană].

³⁶ Considerentul 4 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană.

³⁷ A se vedea două studii privind cerințele de localizare a datelor desfășurate anterior adoptării Regulamentului privind libera circulație a datelor fără caracter personal: (1) Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Market*, număr SMART 2015/2016. Document disponibil online la: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185 și (2) Time.lex, Spark Legal Network și Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions*, număr SMART 2015/0054. Document disponibil online la: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695

³⁸ Considerentul 19 din regulament.

membru³⁹, precum și aspectele siguranței publice, în special pentru a facilita investigarea, depistarea și urmărirea penală a infracțiunilor. Aceasta presupune existența unei amenințări reale și suficient de grave care afectează unul dintre interesele fundamentale ale societății⁴⁰, cum ar fi o amenințare la adresa funcționării instituțiilor și a serviciilor publice esențiale și la adresa supraviețuirii populației, precum și riscul unei perturbări grave a relațiilor externe sau a conviețuirii pașnice a națiunilor ori un risc la adresa intereselor militare.”

În plus, orice cerință de localizare a datelor justificată din motive de securitate publică trebuie să fie proporțională. În conformitate cu jurisprudența Curții de Justiție a Uniunii Europene, principiul proporționalității prevede că măsurile adoptate trebuie să fie adecvate pentru a asigura îndeplinirea obiectivului urmărit și să nu depășească ceea ce este necesar în acest scop⁴¹.

Din motive de claritate, interzicerea cerințelor de localizare a datelor nu aduce atingere restricțiilor deja existente prevăzute de legislația UE⁴².

În plus, Regulamentul privind libera circulație a datelor fără caracter personal nu impune nicio obligație întreprinderilor și nici nu limitează libertatea contractuală a acestora de a decide unde urmează să fie prelucrate datele lor.

Statele membre sunt obligate să pună la dispoziția publicului informațiile referitoare la orice cerință de localizare a datelor aplicabilă pe teritoriul lor prin intermediul unui **punct unic de informare online național** (site-uri web naționale). Acestea trebuie să îl actualizeze periodic sau să furnizeze informații actualizate unui punct central de informare creat în temeiul altui act al Uniunii⁴³. Pentru a simplifica demersurile întreprinderilor și pentru a facilita accesul

³⁹ A se vedea, de exemplu, hotărârea Curții de Justiție din 23 noiembrie 2010, Land Baden-Württemberg/Tsakouridis, C-145/09, ECLI:EU:C:2010:708, punctul 43 și hotărârea din 4 aprilie 2017, Sahar Fahimian/Bundesrepublik Deutschland, C-544/15, ECLI:EU:C:2017:225, punctul 39.

⁴⁰ A se vedea, de exemplu, hotărârea Curții de Justiție din 22 decembrie 2008, Comisia Comunităților Europene/Republica Austria, C-161/07, ECLI:EU:C:2008:759, punctul 35 și jurisprudența menționată de aceasta, precum și hotărârea din 26 martie 2009, Comisia Comunităților Europene/Republica Italiană, C-326/07, ECLI:EC:C:2009:193, punctul 70 și jurisprudența menționată de aceasta.

⁴¹ A se vedea, de exemplu, hotărârea Curții de Justiție din 8 iulie 2010, Afton Chemical Limited/Secretary of State for Transport, C-343/09, ECLI:EU:C:2010:419, punctul 45, precum și jurisprudența menționată în aceasta.

⁴² A se vedea, de exemplu, articolul 245 alineatul (2) din Directiva 2006/112/CE din 28 noiembrie 2006 privind sistemul comun al taxei pe valoarea adăugată, care prevede că „statele membre pot solicita persoanelor impozabile stabilite pe teritoriul lor să le fie comunicat locul de stocare, în cazul în care acesta se află în afara teritoriului lor.”. Această cerință trebuie totuși interpretată în conformitate cu articolul 249, care prevede că „în cazul în care o persoană impozabilă stochează facturi pe care le emite sau le primește prin mijloace electronice ce garantează accesul on-line la date, iar locul de stocare se află într-un alt stat membru decât cel în care este stabilită, autoritățile competente din statul membru în care persoana respectivă este stabilită au, în sensul prezentei directive, dreptul de acces la facturi prin mijloace electronice, de descărcare și de utilizare a acestora, în limitele stabilite de normele statului membru în care persoana impozabilă este stabilită și în măsura în care autoritățile respective solicită acest lucru în scopul controlului.”

⁴³ Articolul 4 alineatul (4) din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană.

acestora la informații relevante în întreaga UE, Comisia va publica linkuri către aceste puncte de informare pe portalul „Europa ta”⁴⁴.

3.2 Libera circulație a datelor cu caracter personal

Regulamentul general privind protecția datelor⁴⁵ prevede că „libera circulație a datelor cu caracter personal în interiorul Uniunii nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.”

În cazul în care un stat membru impune cerințe de localizare a datelor cu caracter personal din alte motive decât protecția datelor cu caracter personal, acestea vor trebui să fie evaluate în raport cu dispozițiile privind libertățile fundamentale și motivele permise de derogare de la aceste libertăți prevăzute de Tratatul privind funcționarea Uniunii Europene^{46,47} și legislația relevantă a UE, cum ar fi Directiva privind serviciile⁴⁸ și Directiva privind comerțul electronic⁴⁹.

Exemplu:

O lege națională impune ca conturile de salarii să fie situate într-un anumit stat membru din motive legate de controlul reglementar, de exemplu de către autoritatea fiscală națională. O astfel de dispoziție națională nu ar intra în domeniul de aplicare al articolului 1 alineatul (3) din Regulamentul general privind protecția datelor, deoarece motivele sunt diferite de protecția datelor cu caracter personal. În schimb, această cerință ar trebui să fie evaluată în raport cu dispozițiile privind libertățile fundamentale și cu motivele permise de derogare de la aceste libertăți prevăzute de Tratatul privind funcționarea Uniunii Europene.

Regulamentul general privind protecția datelor⁵⁰ recunoaște faptul că statele membre pot impune condiții, inclusiv restricții, cu privire la prelucrarea datelor genetice, a datelor

⁴⁴ <https://europa.eu/youreurope/index.htm#ro>

⁴⁵ Articolul 1 alineatul (3) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

⁴⁶ Versiunea consolidată a Tratatului privind funcționarea Uniunii Europene, JO C 326, 26.10.2012, p. 47-390.

⁴⁷ A se vedea, de asemenea, hotărârea Curții de Justiție din 19 iunie 2008, Comisia Comunităților Europene/Marele Ducat al Luxemburgului, C-319/06, ECLI:EU:C:2008:350, punctele 90-91, în care Curtea a considerat că obligația de a ține la dispoziție și de a păstra anumite documente într-un anumit stat membru constituie o restricție privind libera prestare a serviciilor; o justificare conform căreia este „în general mai ușor pentru autorități să își îndeplinească sarcinile de supraveghere” nu este suficientă.

⁴⁸ Directiva 2006/123/CE a Parlamentului European și a Consiliului din 12 decembrie 2006 privind serviciile în cadrul pieței interne, JO L 376, 27.12.2006, p. 36-68.

⁴⁹ Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (directiva privind comerțul electronic), JO L 178, 17.7.2000, p. 1-16.

⁵⁰ Articolul 9 alineatul (4) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

biometrice sau a datelor privind sănătatea. Cu toate acestea, după cum se menționează în considerentul 53, astfel de limitări naționale nu ar trebui să împiedice libera circulație a datelor cu caracter personal în UE atunci când aceste condiții se aplică prelucrării transfrontaliere a unor astfel de date. Acest lucru este în conformitate cu articolul 16 din Tratatul privind funcționarea Uniunii Europene, care constituie temeiul juridic pentru adoptarea de norme privind dreptul la protecția datelor cu caracter personal și de norme privind libera circulație a acestor date.

3.3 Domeniul de aplicare al Regulamentului privind libera circulație a datelor fără caracter personal

Astfel cum s-a menționat anterior, obiectivul Regulamentului privind libera circulație a datelor fără caracter personal este de a asigura libera circulație a datelor fără caracter personal „în cadrul Uniunii”⁵¹. Prin urmare, acesta nu se aplică operațiunilor de prelucrare care au loc în afara UE și cerințelor de localizare a datelor referitoare la o astfel de prelucrare^{52,53}.

Prin urmare, în conformitate cu articolul 2 alineatul (1), domeniul de aplicare al regulamentului este limitat la prelucrarea datelor electronice fără caracter personal în UE care:

- (a) este furnizată ca serviciu utilizatorilor ce își au reședința ori au sunt stabiliți în Uniune, indiferent dacă furnizorul de servicii este stabilit sau nu în Uniune; sau
- (b) este efectuată de o persoană fizică sau juridică ce își are reședința ori este stabilită în Uniune pentru propriile sale nevoi.

Exemple:

Articolul 2 alineatul (1) litera (a) din Regulamentul privind libera circulație a datelor fără caracter personal:

- Un furnizor de servicii de cloud stabilit în SUA furnizează servicii de prelucrare unor clienți care își au reședința sau sunt stabiliți în UE. Furnizorul de servicii de cloud își administrează activitățile prin intermediul serverelor situate pe teritoriul UE, în care datele clienților săi europeni sunt stocate sau prelucrate în alt mod. Furnizorul de servicii de cloud nu este obligat să dețină propria infrastructură în UE, dar poate, de exemplu, să închirieze spațiu pe un server din UE. Regulamentul privind libera

⁵¹ A se vedea articolul 1 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană.

⁵² A se vedea considerentul 15 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană.

⁵³ Termenul de „prelucrare” este definit în termeni generali [articolul 3 alineatul (2) din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană] și, astfel cum se subliniază în considerentul 17, regulamentul ar trebui să se aplice prelucrării în sensul cel mai larg, cuprinzând utilizarea tuturor tipurilor de sisteme informatice.

circulație a datelor fără caracter personal se aplică în cazul unei astfel de prelucrări a datelor.

- Un furnizor de servicii de cloud stabilit în Japonia își oferă serviciile clienților europeni. Capacitățile de prelucrare ale furnizorului sunt situate în Japonia și toate activitățile de prelucrare au loc în această țară. Regulamentul privind libera circulație a datelor fără caracter personal nu se aplică în acest caz, dacă toate activitățile de prelucrare au loc în afara UE⁵⁴.

Articolul 2 alineatul (1) litera (b) din Regulamentul privind libera circulație a datelor fără caracter personal:

- O întreprindere europeană nou-înființată de dimensiuni mici din statul membru A decide să își extindă activitatea prin deschiderea unui sediu în statul membru B. Pentru a reduce la minimum costurile, această întreprindere nou-înființată alege să centralizeze stocarea și prelucrarea datelor noului sediu pe serverul său situat în statul membru A. Statele membre nu pot interzice astfel de eforturi de centralizare informatică, cu excepția cazului în care acest lucru este justificat de motive de siguranță publică, în conformitate cu principiul proporționalității.

Deși Regulamentul privind libera circulație a datelor fără caracter personal nu se aplică în cazul în care toate activitățile de prelucrare a datelor fără caracter personal sunt efectuate în afara UE, Regulamentul general privind protecția datelor trebuie să fie respectat atunci când din setul de date fac parte date cu caracter personal. În special, normele privind transferurile de date cu caracter personal către țări terțe sau organizații internaționale în temeiul Regulamentului general privind protecția datelor trebuie să fie respectate în orice caz⁵⁵.

3.4 Activități legate de organizarea internă a statelor membre

Regulamentul privind libera circulație a datelor fără caracter personal nu obligă statele membre să externalizeze furnizarea de servicii legate de datele fără caracter personal pe care

⁵⁴ Trebuie remarcat faptul că Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană nu se referă la cerințele de localizare a datelor impuse de statele membre cu privire la stocarea datelor fără caracter personal în țări terțe și că aceste cerințe pot fi prezente în ordinile juridice naționale. Din motive de claritate, Regulamentul general privind protecția datelor se aplică prelucrării datelor cu caracter personal ale persoanelor vizate care se află în UE, de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activitățile de prelucrare sunt legate de: (a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată; sau (b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii [a se vedea articolul 3 alineatul (2) din Regulamentul general privind protecția datelor].

⁵⁵ În ceea ce privește transferurile de date cu caracter personal către țări terțe, consultați pagina de internet a Comisiei: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_ro și Comunicarea Comisiei către Parlamentul European și Consiliu – Schimbul de date cu caracter personal și protecția acestora într-o lume globalizată, COM/2017/07 final, disponibilă la adresa: <https://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1558267768886&uri=CELEX:52017DC0007>. În cazul Japoniei, la 23 ianuarie 2019, Comisia a adoptat decizia sa privind caracterul adecvat al nivelului de protecție, permițând ca datele cu caracter personal să circule liber între cele două economii, pe baza unor garanții solide în materie de protecție.

doresc să le furnizeze ele însele sau să le organizeze prin alte mijloace decât contractele de achiziții publice⁵⁶.

Articolul 2 alineatul (3) al doilea paragraf din Regulamentul privind libera circulație a datelor fără caracter personal menționează următoarele:

„Prezentul regulament nu aduce atingere actelor cu putere de lege și actelor administrative referitoare la **organizarea internă** a statelor membre și care atribuie în rândul autorităților publice și al organismelor de drept public, astfel cum sunt definite la articolul 2 alineatul (1) punctul 4 din Directiva 2014/24/UE⁵⁷, competențe și responsabilități în materie de **prelucrare a datelor, fără remunerarea contractuală a părților private**, și nici actelor cu putere de lege și actelor administrative ale statelor membre care reglementează punerea în aplicare a acestor competențe și responsabilități.⁵⁸”

Pot exista interese legitime care ar justifica alegerea acestui tip de „furnizare internă” a serviciilor de prelucrare a datelor, cum ar fi „internalizarea” sau acordurile reciproce între administrațiile publice. Exemplele tipice includ utilizarea unui „cloud guvernamental” sau angajarea de către un guvern a unei agenții centralizate de servicii informatice pentru a furniza servicii de prelucrare a datelor pentru instituțiile și organismele publice.

Cu toate acestea, Regulamentul privind libera circulație a datelor fără caracter personal încurajează statele membre să ia în considerare eficiența economică și alte beneficii ale utilizării furnizorilor externi de servicii^{59,60}. De îndată ce autoritățile naționale încep „externalizarea” prelucrării datelor, cu remunerarea contractuală a părților private, iar prelucrarea are loc în UE, o astfel de prelucrare este reglementată de Regulamentul privind libera circulație a datelor fără caracter personal, ceea ce înseamnă că principiul liberei circulații a datelor fără caracter personal se aplică practicilor generale și administrative ale

⁵⁶ Considerentul 14 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană.

⁵⁷ Articolul 2 alineatul (1) punctul (4) din Directiva 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE, JO L 94, 28.3.2014, p. 65-242 prevede că „«organisme de drept public» înseamnă organismele care au toate caracteristicile următoare: (a) sunt înființate în scopul specific de a răspunde unor necesități de interes general, fără caracter industrial sau comercial; (b) au personalitate juridică și (c) sunt finanțate, în cea mai mare parte, de către stat, autorități regionale sau locale sau alte organisme de drept public; sau administrarea lor face obiectul supravegherii de către autoritățile sau organismele respective sau au un consiliu de administrație, de conducere sau de supraveghere alcătuit din membri desemnați în proporție de peste 50 % de către stat, de autorități regionale sau locale sau de alte organisme de drept public;”

⁵⁸ Considerentul 13 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană subliniază că regulamentul nu aduce atingere Directivei 2014/24/UE.

⁵⁹ Considerentul 14 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană.

⁶⁰ Un furnizor extern de servicii ar fi orice entitate care nu este un „organism de drept public”, astfel cum se prevede la articolul 2 alineatul (1) punctul (4) din Directiva 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE, JO L 94, 28.3.2014, p. 65-242.

autorităților naționale. În special, acestea trebuie să se abțină de la impunerea de restricții în materie de localizare a datelor, de exemplu în cadrul licitațiilor pentru achiziții publice⁶¹.

4 Abordări de autoreglementare care susțin libera circulație a datelor

Autoreglementarea contribuie la inovare și încredere în rândul actorilor de pe piață și are potențialul de a fi mai receptivă la schimbările de pe piață. Prezenta secțiune oferă o prezentare generală a inițiativelor de autoreglementare pentru prelucrarea atât a datelor cu caracter personal, cât și a celor fără caracter personal.

4.1 Portarea datelor și schimbarea furnizorilor de servicii de cloud

Unul dintre scopurile Regulamentului privind libera circulație a datelor fără caracter personal este evitarea practicilor privind dependența de furnizor. Aceste practici apar atunci când utilizatorii nu pot schimba furnizorul de servicii deoarece datele lor sunt „blocate” în sistemul furnizorului, de exemplu din cauza unui format specific al datelor sau a unor acorduri contractuale specifice, și nu pot fi transferate în afara sistemului informatic al furnizorului. Portarea datelor fără obstacole este importantă pentru a permite utilizatorilor să aleagă liber între furnizorii de servicii de prelucrare a datelor și, astfel, să se asigure o concurență efectivă pe piață.

Portabilitatea datelor între întreprinderi devine din ce în ce mai importantă pentru o gamă largă de industrii digitale, inclusiv serviciile de cloud.

În conformitate cu articolul 6 din Regulamentul privind libera circulație a datelor fără caracter personal, Comisia încurajează și facilitează elaborarea unor coduri de conduită de autoreglementare la nivelul UE („coduri de conduită”) pentru a contribui la o economie competitivă a datelor. Aceasta constituie baza pentru dezvoltarea de către industrie a codurilor de conduită de autoreglementare privind schimbarea furnizorilor de servicii și portarea datelor între diferite sisteme informatice.

La elaborarea unor astfel de coduri de conduită privind portarea datelor ar trebui să se țină seama de o serie de aspecte, în special:

- **bunele practici** menite să faciliteze schimbarea furnizorilor de servicii și portarea datelor într-un format structurat, utilizat în mod curent și care poate fi citit automat;
- **cerințele minime în materie de informare**, pentru a se asigura că utilizatorilor profesioniști li se oferă, înainte de încheierea unui contract, informații suficiente de detaliate și clare cu privire la procesele, cerințele tehnice și termenele care se aplică în cazul în care un utilizator profesionist dorește să schimbe un furnizor de servicii sau să își poarte datele înapoi către propriile sisteme informatice;
- **abordările privind sistemele de certificare**, pentru o mai bună comparabilitate a serviciilor de cloud și

⁶¹ Considerentul 13 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană.

- **foile de parcurs privind comunicarea**, în vederea sensibilizării cu privire la codurile de conduită.

Pe piața serviciilor de cloud, Comisia a început să faciliteze activitatea grupurilor de lucru ale părților interesate din domeniul tehnologiei de tip cloud de pe piața unică digitală, care reunesc experți în tehnologia de tip cloud și utilizatori profesioniști, inclusiv întreprinderi mici și mijlocii. În acest stadiu, un subgrup elaborează coduri de conduită de autoreglementare privind portarea datelor și schimbarea furnizorilor de servicii de cloud (grupul de lucru SWIPO)⁶², iar un alt subgrup lucrează la dezvoltarea certificării de securitate a serviciilor cloud (grupul de lucru CSPCERT)⁶³..

Grupul de lucru SWIPO elaborează coduri de conduită care acoperă întregul spectru de servicii de cloud: infrastructură ca serviciu (IaaS), platformă ca serviciu (PaaS) și software ca serviciu (SaaS).

Comisia se așteaptă ca diferitele coduri de conduită să fie completate cu **modele de clauze contractuale**⁶⁴. Acestea vor permite o specificitate tehnică și juridică suficientă pentru punerea în practică și aplicarea codurilor de conduită, care vor avea o importanță deosebită pentru întreprinderile mici și mijlocii. Elaborarea modelelor de clauze contractuale este planificată după elaborarea codurilor de conduită (care ar trebui să aibă loc până la 29 noiembrie 2019).

În conformitate cu articolul 8 din Regulamentul privind libera circulație a datelor fără caracter personal, Comisia va evalua punerea în aplicare a regulamentului până la 29 noiembrie 2022. Acest lucru va permite evaluarea: (i) impactului asupra liberei circulații a datelor în Europa; (ii) aplicării regulamentului, în special în cazul seturilor de date mixte; (iii) măsurii în care statele membre au abrogat în mod efectiv restricțiile nejustificate în materie de localizare a datelor și (iv) eficienței pe piață a codurilor de conduită în domeniul portării datelor și în cel al schimbării furnizorilor de servicii de cloud.

Noțiunea de portabilitate și interacțiunea cu Regulamentul general privind protecția datelor

Ambele regulamente⁶⁵ se referă la portabilitatea datelor și la obiectivul de a facilita portarea datelor de la un mediu informatic la altul, și anume fie la sistemele unui alt furnizor, fie la sistemele de la fața locului. Acest lucru împiedică dependența de furnizor și stimulează concurența între furnizorii de servicii. Cu toate acestea, regulamentele diferă în ceea ce

⁶² *Cloud Switching and Porting Data Working Group* (Grupul de lucru pentru schimbarea furnizorilor de servicii de cloud și portarea datelor).

⁶³ *European Cloud Service Provider Certification Working Group* (Grupul de lucru pentru certificarea europeană a furnizorilor de servicii de cloud). A se vedea, de asemenea, secțiunea 4.3.

⁶⁴ A se vedea considerentul 30 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană.

⁶⁵ Articolul 6 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană și articolul 20 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

privește abordarea portabilității în legătură cu relația dintre grupurile de interese vizate și natura juridică a dispozițiilor.

Dreptul la portabilitatea datelor cu caracter personal în temeiul articolului 20 din Regulamentul general privind protecția datelor se axează pe relația dintre persoana vizată și operator. Acesta se referă la dreptul persoanei vizate de a primi date cu caracter personal pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat, precum și de a transmite aceste date unui alt operator sau propriilor sale capacități de stocare fără nicio piedică din partea operatorului căruia i-au fost furnizate datele cu caracter personal⁶⁶. În general, în cadrul acestei relații, persoanele vizate sunt consumatorii de diferite servicii online care doresc să schimbe furnizorii de servicii de acest tip.

Articolul 6 din Regulamentul privind libera circulație a datelor fără caracter personal nu prevede dreptul utilizatorilor profesioniști la portarea datelor, ci are o abordare de autoreglementare care include coduri de conduită voluntare pentru industrie. În același timp, acesta vizează o situație în care un utilizator profesionist a externalizat prelucrarea datelor sale către o parte terță care oferă un serviciu de prelucrare a datelor⁶⁷. În conformitate cu articolul 3 alineatul (8) din Regulamentul privind libera circulație a datelor fără caracter personal, un „utilizator profesionist” poate include „o persoană fizică sau juridică, inclusiv o autoritate publică sau un organism de drept public, care utilizează ori solicită un serviciu de prelucrare a datelor în scopuri legate de activitatea sa comercială, industrială, artizanală sau profesională ori de sarcinile sale”.

În practică, portabilitatea în temeiul articolului 6 din Regulamentul privind libera circulație a datelor fără caracter personal se referă la interacțiunile între întreprinderi (business-to-business) între un utilizator profesionist (care, în cazurile care includ prelucrarea datelor cu caracter personal, se poate califica drept „operator” în conformitate cu Regulamentul general privind protecția datelor) și un furnizor de servicii (care, în mod similar, se poate califica drept „persoană împuternicită de către operator” în anumite cazuri).

În ciuda diferențelor, pot apărea situații în care portarea datelor ar face atât obiectul Regulamentului privind libera circulație a datelor fără caracter personal, cât și al Regulamentului general privind protecția datelor, în ceea ce privește seturile de date mixte.

⁶⁶ A se vedea documentul „Orientări privind dreptul la portabilitatea datelor” elaborat de Grupul de lucru „Articolul 29”, WP 242 rev.01, adoptat la 13 decembrie 2016, astfel cum a fost revizuit și adoptat la 5 aprilie 2017.

⁶⁷ Considerentul 29 din Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană menționează: „În timp ce consumatorii individuali beneficiază de dreptul existent al Uniunii [și anume, Regulamentul general privind protecția datelor], capacitatea de a schimba furnizorii de servicii nu este facilitată pentru utilizatori în cadrul activităților comerciale sau profesionale ale acestora.”

Exemplu:

O întreprindere care utilizează un serviciu de cloud decide să schimbe furnizorul de servicii de cloud și să poarte toate datele către un nou furnizor. Schimbarea furnizorului de servicii și portarea datelor sunt reglementate în contractul încheiat între client și furnizorul de servicii de cloud. În cazul în care vechiul furnizor de servicii de cloud aderă la codurile de conduită elaborate în temeiul Regulamentului privind libera circulație a datelor fără caracter personal, portarea datelor trebuie să aibă loc în conformitate cu cerințele specificate în regulamentul respectiv.

În cazul în care datele cu caracter personal fac, de asemenea, parte din seturile de date portate, portarea trebuie să respecte toate dispozițiile relevante ale Regulamentului general privind protecția datelor, asigurându-se în special că noul furnizor de servicii de cloud respectă cerințele aplicabile, cum ar fi securitatea⁶⁸.

Exemplu:

În cazul în care o bancă decide să își schimbe furnizorul de servicii de gestionare a relațiilor cu clienții (CRM), este posibil ca unele date (personale și fără caracter personal) să migreze de la vechiul furnizor, la cel nou. Aceste date vor face apoi obiectul unor cerințe de reglementare diferite, unele rezultând din Regulamentul general privind protecția datelor și altele din Regulamentul privind libera circulație a datelor fără caracter personal.

4.2 Coduri de conduită și sisteme de certificare privind protecția datelor cu caracter personal

Codurile de conduită și sistemele de certificare pot fi utilizate pentru a demonstra conformitatea cu obligațiile prevăzute în Regulamentul general privind protecția datelor [a se vedea articolul 24 alineatul (3) și articolul 28 alineatul (5)].

În conformitate cu articolul 40 alineatul (1) și cu articolul 42 alineatul (1) din Regulamentul general privind protecția datelor, statele membre, autoritățile de supraveghere, Comitetul european pentru protecția datelor și Comisia ar trebui să încurajeze industria să elaboreze coduri de conduită și să instituie mecanisme de certificare a protecției datelor.

Asociațiile sau alte organisme care reprezintă o anumită categorie de operatori sau persoane împuternicite de către operatori pot elabora un cod de conduită pentru sectorul specific. Un proiect al codului trebuie prezentat spre aprobare autorității de supraveghere competente respective⁶⁹. În cazul în care proiectul de cod de conduită se referă la activități de prelucrare

⁶⁸ A se vedea documentul „Avizul 05/2012 privind cloud computing” elaborat de Grupul de lucru „Articolul 29”, adoptat la 1 iulie 2012, WP196, care precizează, de asemenea, poziția și obligațiile utilizatorilor de servicii de cloud și ale furnizorilor de astfel de servicii în ceea ce privește prelucrarea datelor cu caracter personal.

⁶⁹ A se vedea articolul 40 alineatul (5) și articolul 55 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea

desfășurate în mai multe state membre, autoritatea de supraveghere trebuie să îl transmită Comitetului european pentru protecția datelor înainte de aprobare. Ulterior, comitetul va emite un aviz cu privire la conformitatea proiectului de cod cu Regulamentul general privind protecția datelor.

Comitetul european pentru protecția datelor a publicat Orientările nr. 1/2019 privind codurile de conduită și organismele de monitorizare în temeiul Regulamentului general privind protecția datelor⁷⁰. Orientările includ informații privind elaborarea codurilor de conduită, criteriile de aprobare a acestora și alte informații utile. În mod similar, Orientările Comitetului european pentru protecția datelor nr. 1/2018 privind certificarea și identificarea criteriilor de certificare în conformitate cu articolele 42 și 43 din Regulamentul general privind protecția datelor oferă informații cu privire la certificarea în temeiul acestui regulament și cu privire la elaborarea și aprobarea criteriilor de certificare⁷¹.

Exemple de coduri de conduită elaborate de sectorul serviciilor de cloud:

The EU Cloud Code of Conduct (Codul de conduită al UE în domeniul serviciilor de cloud), a cărui elaborare a fost facilitată de Comisie, a fost redactat în colaborare cu *Cloud Select Industry Group* (C-SIG) pe baza Directivei privind protecția datelor⁷² și, ulterior, a Regulamentului general privind protecția datelor. Codul de conduită al UE în domeniul serviciilor de cloud acoperă întregul spectru al serviciilor de cloud – infrastructură ca serviciu (IaaS), platformă ca serviciu (PaaS) și software ca serviciu (SaaS)⁷³.

The Code of Conduct of the Cloud Infrastructure Services Providers in Europe (CISPE)⁷⁴ (Codul de conduită al furnizorilor de servicii de infrastructură de tip cloud în Europa) se concentrează pe furnizorii de IaaS. Codul de conduită CISPE constă în cerințe privind furnizorii de IaaS care acționează în calitate de persoane împuternicite de către operator în temeiul Regulamentului general privind protecția datelor. Acesta stabilește, de asemenea, dispoziții privind structura de guvernanta pentru punerea în practică și aplicarea codului.

datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

⁷⁰ Comitetul european pentru protecția datelor: *Orientările nr. 1/2019 privind codurile de conduită și organismele de monitorizare prevăzute în Regulamentul (UE) 2016/679*, adoptate la 12 februarie 2019, versiunea pentru consultare publică, disponibilă online la adresa: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_ro

⁷¹ Comitetul european pentru protecția datelor: *Orientările nr. 1/2018 privind certificarea și identificarea criteriilor de certificare în conformitate cu articolele 42 și 43 din Regulamentul (UE) 2016/679*, adoptate la 23 ianuarie 2019, disponibile online la: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_ro

⁷² Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (data încetării: 24 mai 2018).

⁷³ Pentru mai multe informații privind Codul de conduită al UE în domeniul serviciilor de cloud, a se vedea: <https://eucoc.cloud/en/home.html>

⁷⁴ Pentru mai multe informații privind Codul de conduită CISPE, a se vedea: <https://cispe.cloud/code-of-conduct/>

The Cloud Security Alliance's Code of Conduct for GDPR Compliance (Codul de conduită al Alianței pentru securitatea tehnologiei de tip cloud în vederea respectării RGPD) vizează toate părțile interesate din domeniul serviciilor de cloud computing (cum ar fi furnizorii de servicii de cloud, clienții și clienții potențiali ai serviciilor de cloud, auditorii serviciilor de cloud și brokerii acestor servicii) și din domeniul legislației europene privind datele cu caracter personal. Codul de conduită acoperă întregul spectru al furnizorilor de servicii de cloud⁷⁵.

4.3 Consolidarea încrederii în prelucrarea datelor la nivel transfrontalier – certificarea securității

Astfel cum se menționează în considerentul 33 din Regulamentul privind libera circulație a datelor fără caracter personal, consolidarea încrederii în securitatea prelucrării datelor la nivel transfrontalier ar trebui să reducă tendința actorilor de pe piață și a sectorului public de a utiliza localizarea datelor ca un indicator pentru securitatea datelor. Împreună cu pachetul de măsuri privind securitatea cibernetică, propus de Comisie în 2017⁷⁶, grupul de lucru CSPCERT elaborează recomandări în scopul instituirii unui sistem european de certificare în domeniul tehnologiei de tip cloud, care vor fi prezentate Comisiei. Un astfel de sistem are potențialul de a facilita libera circulație a datelor, de a permite o mai bună comparabilitate a serviciilor de cloud și de a promova utilizarea tehnologiei de tip cloud. Comisia poate solicita ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) să pregătească o propunere de sistem în conformitate cu dispozițiile relevante din Legea privind securitatea cibernetică⁷⁷. Un astfel de sistem poate viza atât datele cu caracter personal, cât și pe cele fără caracter personal. Pe lângă Legea privind securitatea cibernetică și astfel cum s-a subliniat în secțiunea 4.2, RGPD poate fi, de asemenea, utilizat pentru a demonstra existența unor garanții adecvate privind securitatea datelor⁷⁸.

Observații finale

Asigurarea securității juridice și a încrederii în prelucrarea datelor este esențială pentru capacitatea UE de a utiliza datele la întregul lor potențial și pentru dezvoltarea lanțurilor valorice la nivel transsectorial și transfrontalier. Cele două regulamente asigură acest lucru și urmăresc obiectivul liberei circulații a datelor. Împreună, Regulamentul privind libera circulație a datelor fără caracter personal și Regulamentul general privind protecția datelor creează bazele pentru libera circulație a tuturor datelor în cadrul Uniunii Europene și pentru o economie europeană a datelor cu un nivel ridicat de competitivitate.

⁷⁵ Pentru mai multe informații privind Codul de conduită CSA, a se vedea: <https://gdpr.cloudsecurityalliance.org/>

⁷⁶ Pentru mai multe informații, a se vedea: <https://ec.europa.eu/digital-single-market/en/cyber-security>

⁷⁷ Regulamentul Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru securitate cibernetică) și privind certificarea securității cibernetică pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Legea privind securitatea cibernetică).

⁷⁸ A se vedea considerentul 74 din Legea privind securitatea cibernetică.