COMISIA
EUROPEANĂ

Bruxelles, 25.7.2024
COM(2024) 357 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Al doilea raport referitor la aplicarea Regulamentului general privind protecția datelor

1 INTRODUCERE

Acesta este cel de al doilea raport al Comisiei privind aplicarea Regulamentului general privind protecția datelor (RGPD), adoptat în conformitate cu articolul 97 din RGPD. Primul raport a fost adoptat la 24 iunie 2020 („raportul din 2020”) [(1)].

RGPD este una din pietrele de temelie ale abordării UE privind transformarea digitală. Principiile sale de bază – prelucrarea echitabilă, sigură și transparentă a datelor cu caracter personal, asigurarea faptului că persoanele fizice păstrează controlul asupra datelor lor – stau la baza tuturor politicilor UE care implică prelucrarea datelor cu caracter personal.

De la raportul din 2020, UE a adoptat o serie de inițiative menite să plaseze persoanele fizice în centrul tranziției digitale. Fiecare inițiativă urmărește un anumit scop, de exemplu să creeze un mediu online mai sigur, să facă economia digitală mai echitabilă și mai competitivă, să faciliteze cercetarea inovatoare, să asigure dezvoltarea unei inteligențe artificiale (IA) sigure și de încredere și să creeze o veritabilă piață unică a datelor. Ori de câte ori sunt implicate date cu caracter personal, aceste inițiative se bazează pe RGPD. RGPD oferă, de asemenea, o bază pentru inițiativele sectoriale care au un impact asupra prelucrării datelor cu caracter personal, de exemplu în domeniul serviciilor financiare, al sănătății, al ocupării forței de muncă, al mobilității și al asigurării respectării legii.

Există un consens larg în rândul părților interesate, al autorităților pentru protecția datelor și al statelor membre cu privire la faptul că, în pofida existenței unor dificultăți, RGPD a oferit rezultate importante pentru persoane fizice și întreprinderi. Abordarea bazată pe riscuri, neutră din punct de vedere tehnologic oferă o protecție solidă persoanelor vizate și obligații proporționale pentru operatorii de date și persoanele împuternicite de operatori. În același timp, ar trebui realizate progrese suplimentare într-o serie de domenii. În particular, în următorii ani, ar trebui să se pună accentul pe sprijinirea eforturilor de conformare ale părților interesate – în special ale întreprinderilor mici și mijlocii (IMM-uri), ale operatorilor de mici dimensiuni, ale cercetătorilor și ale organizațiilor de cercetare, pe furnizarea de orientări mai clare și mai ușor de aplicat din partea autorităților pentru protecția datelor și pe realizarea unei interpretări și a unei aplicări mai consecvente a RGPD în întreaga UE.

În conformitate cu articolul 97 din RGPD, Comisia ar trebui să examineze în special aplicarea și funcționarea transferului internațional de date cu caracter personal către țări terțe (și anume țări din afara UE/SEE) (capitolul V din RGPD), precum și mecanismele de cooperare și de asigurare a coerenței între autoritățile naționale pentru protecția datelor (capitolul VII din RGPD). Însă, la fel ca în cazul raportului din 2020, prezentul raport oferă o evaluare generală a aplicării RGPD care depășește aceste două elemente: raportul identifică o serie de acțiuni necesare pentru a sprijini aplicarea eficace a RGPD în domenii-cheie prioritare.

Prezentul raport ia în considerare următoarele surse: (i) poziția și constatările Consiliului, adoptate în decembrie 2023 ([2]); (ii) contribuțiile colectate de la părțile interesate, în special prin intermediul Grupului multipartit pentru RGPD ([3]) și al unei cereri publice de contribuții ([4]) și (iii) contribuțiile din partea autorităților pentru protecția datelor [prin

---

([1]) Protecția datelor ca pilon al capacitării cetățenilor și al abordării UE privind tranziția digitală – doi ani de aplicare a Regulamentului general privind protecția datelor, 24.6.2020, COM(2020) 264 final.

([2]) https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/ro/pdf.

([3]) Un rezumat al contribuțiilor Grupului multipartit de experți pentru RGPD este disponibil la adresa: Report from Multistakeholder Expert group on GDPR application - June 2024.pdf. Contribuțiile primite ca răspuns la cererea publică de contribuții și prin intermediul reuniunilor bilaterale cu părțile interesate reflectă în mare măsură opiniile exprimate de membrii Grupului multipartit de experți privind RGPD.

([4]) https://ec.europa.eu/info/law/better-regulation/have-your-say_ro.

contribuția Comitetului european pentru protecția datelor ([5]) („comitetul”) și un raport elaborat de Agenția pentru Drepturi Fundamentale (FRA)] pe baza interviurilor desfășurate cu autorități individuale pentru protecția datelor ([6]) („raportul FRA”). Raportul se bazează, de asemenea, pe monitorizarea continuă de către Comisie a aplicării RGPD, inclusiv pe dialogurile bilaterale cu statele membre cu privire la conformitatea legislației naționale, pe contribuția activă la activitatea comitetului și pe contactele strânse cu o gamă largă de părți interesate cu privire la aplicarea practică a regulamentului.

2 ASIGURAREA RESPECTĂRII RGPD ȘI FUNCȚIONAREA MECANISMELOR DE COOPERARE ȘI DE ASIGURARE A COERENȚEI

Sistemul de tip ghișeu unic de asigurare a respectării RGPD urmărește să asigure o interpretare și o aplicare armonizată de către autoritățile independente pentru protecția datelor. Acesta necesită cooperare între autoritățile pentru protecția datelor în cazurile de prelucrare transfrontalieră, în cazul în care persoane vizate din mai multe state membre sunt afectate în mod substanțial. Litigiile dintre autorități sunt soluționate de comitet în cadrul mecanismului pentru asigurarea coerenței prevăzut în RGPD.

2.1 Eficientizarea gestionării cazurilor transfrontaliere: propunerea privind normele de procedură

Raportul din 2020 a remarcat necesitatea unei gestionări mai eficiente și mai armonizate a cazurilor transfrontaliere în UE, în special având în vedere diferențele majore dintre procedurile administrative naționale și interpretările conceptelor din cadrul mecanismului de cooperare privind RGPD. Prin urmare, în iulie 2023, Comisia a adoptat o propunere de regulament privind normele procedurale ([7]), care se bazează, de asemenea, pe o listă de aspecte prezentată Comisiei de către comitet în octombrie 2022 ([8]), precum și pe contribuții din partea părților interesate ([9]) și a statelor membre ([10]). Propunerea completează RGPD prin stabilirea unor norme detaliate privind plângerile transfrontaliere, implicarea reclamantului, dreptul la un proces echitabil al părților care fac obiectul investigației (operatori și persoane împuternicite de operatori) și cooperarea dintre autoritățile pentru protecția datelor. Armonizarea acestor aspecte procedurale ar urma să sprijine încheierea la timp a investigațiilor și asigurarea unei soluționări rapide a plângerilor persoanelor fizice. Propunerea este negociată în prezent de către Parlamentul European și Consiliu.

2.2 Intensificarea cooperării dintre autoritățile pentru protecția datelor și utilizarea mecanismului pentru asigurarea coerenței

Numărul cazurilor transfrontaliere a crescut semnificativ în ultimii ani. Autoritățile pentru protecția datelor au demonstrat o disponibilitate sporită de a utiliza instrumentele de cooperare prevăzute în RGPD. Toate autoritățile pentru protecția datelor au utilizat instrumentul de

([5]) Contribuția CEPD la evaluarea RGPD în temeiul articolului 97 | Comitetul european pentru protecția datelor (europa.eu).

([6]) RGPD în practică – Experiențe ale autorităților pentru protecția datelor |. Agenția pentru Drepturi Fundamentale a Uniunii Europene (europa.eu).

([7]) Propunere de regulament al Parlamentului European și al Consiliului de stabilire a unor norme procedurale suplimentare referitoare la asigurarea respectării Regulamentului (UE) 2016/679 [COM(2023) 348 final].

([8]) https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-eu-commission-procedural-aspects-could-be_en.

([9]) Prin intermediul Grupului multipartit de experți privind RGPD și al unei cereri de contribuții lansate în februarie 2023.

([10]) În special prin intermediul grupului de experți al statelor membre privind RGPD: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&do=groupDetail.groupDetail&groupID=3461.

asistență reciprocă ([11]), precum și cereri „informale” pentru a se sprijini reciproc în mod voluntar. Autoritățile pentru protecția datelor favorizează cererile informale, care nu impun un termen sau o obligație strictă de a răspunde. Deși comitetul a adoptat orientări privind operațiunile comune în 2021 ([12]), autoritățile nu au utilizat încă într-o măsură semnificativă acest instrument ([13]) și menționează existența unor diferențe între procedurile naționale și lipsa de claritate în ceea ce privește procedura ca fiind principalele motive pentru utilizarea sa redusă.

RGPD oferă autorităților pentru protecția datelor vizate posibilitatea de a formula o obiecție relevantă și motivată în cazul în care nu sunt de acord cu un proiect de decizie a autorității principale pentru protecția datelor într-un caz transfrontalier. În cazul în care autoritățile pentru protecția datelor nu pot ajunge la un consens cu privire la o obiecție relevantă și motivată, RGPD prevede soluționarea litigiilor de către comitet ([14]). Subiectele cel mai frecvent abordate în obiecțiile relevante și motivate au fost: (i) temeiul juridic al prelucrării; (ii) obligațiile în materie de informare și transparență; (iii) notificarea încălcărilor securității datelor; (iv) drepturile persoanelor vizate; (v) derogările pentru transferurile internaționale; (vi) utilizarea de măsuri corective și (vii) cuantumul unei amenzi administrative.

Sistemul de asigurare a respectării RGPD se bazează pe premisa unei cooperări sincere și eficace între autoritățile de protecție a datelor. Deși procedura de soluționare a litigiilor joacă un rol important în această arhitectură de asigurare a respectării legii, ea ar trebui utilizată în spiritul în care a fost concepută, și anume ținând seama în mod corespunzător de repartizarea competențelor între autoritățile pentru protecția datelor, de necesitatea de a respecta dreptul la un proces echitabil și de interesul de a soluționa cazul în timp util pentru persoanele vizate. Fiecare procedură de soluționare a litigiilor necesită resurse semnificative din partea autorității principale, a autorităților vizate și a secretariatului comitetului și întârzie soluționarea plângerilor persoanelor vizate.

([11]) Articolul 61 din RGPD.
([12]) internal_edpb_document_1_2021_on_art_62_joint_operations_en.pdf (europa.eu)
([13]) Articolul 62 din RGPD.
([14]) Articolul 65 din RGPD.

Utilizarea sporită a instrumentelor de cooperare de către autoritățile pentru protecția datelor

- În sistemul de schimb de informații al comitetului au fost înregistrate aproape 2 400 de cazuri ([15]).
- Autoritățile principale pentru protecția datelor au emis aproximativ 1 500 de proiecte de decizii ([16]), dintre care 990 au condus la decizii finale prin care se constată o încălcare a RGPD ([17]).
- Autoritățile pentru protecția datelor au inițiat aproape 1 000 de cereri de asistență reciprocă „formale” ([18]) și aproximativ 12 300 de cereri „informale” ([19]).
- Au fost inițiate cinci operațiuni comune, la care au participat autorități pentru protecția datelor din șapte state membre.
- Autoritățile pentru protecția datelor din 18 state membre au formulat obiecții relevante și motivate ([20]).

Mecanismul pentru asigurarea coerenței prevăzut în RGPD este utilizat din ce în ce mai mult de autoritățile pentru protecția datelor. Acesta are trei componente: (i) avizele comitetului; (ii) soluționarea litigiilor de către comitet și (iii) procedura de urgență ([21]).

Comitetul abordează din ce în ce mai mult aspecte importante cu aplicabilitate generală în avizele sale ([22]). Comitetul ar trebui să asigure consultări semnificative și desfășurate în timp util înainte de adoptarea avizelor respective. Cazurile supuse soluționării litigiilor au privit chestiuni precum temeiul juridic pentru prelucrarea datelor pentru publicitatea comportamentală pe platformele de comunicare socială și prelucrarea online a datelor copiilor. Majoritatea deciziilor obligatorii ulterioare au fost contestate în fața Tribunalului.

Transparența procesului decizional al comitetului este esențială pentru a asigura respectarea dreptului la bună administrare prevăzut în Carta drepturilor fundamentale a UE. Procedura de urgență prevăzută în RGPD permite autorităților pentru protecția datelor să deroge de la mecanismul de cooperare și de asigurare a coerenței pentru a lua măsuri urgente, dacă este necesar, pentru a proteja drepturile și libertățile persoanelor vizate. Ca derogare de la procedura normală de cooperare prevăzută în RGPD, instrumente precum procedura de urgență sunt concepute pentru a fi utilizate numai în circumstanțe excepționale și în cazul în care procedura normală de cooperare nu poate proteja drepturile și libertățile persoanelor vizate.

([15]) Situație la data de 3 noiembrie 2023 (contribuția comitetului).
([16]) Conform articolului 60 alineatul (3) din RGPD.
([17]) Situație la data de 3 noiembrie 2023.
([18]) Autoritatea irlandeză a formulat cele mai multe cereri formale (246), iar autoritățile germane au primit cele mai multe cereri (516).
([19]) Autoritatea irlandeză a formulat cele mai multe cereri informale (4 245), urmată de autoritățile germane (2 036).
([20]) Dintre cele 289 de obiecții relevante și motivate raportate de autorități, 101 (35 %) au fost formulate de autoritățile germane. Rata de succes în ajungerea la un consens cu privire la obiecțiile relevante și motivate variază între 15 % (dintre obiecțiile formulate de autoritățile germane) și 100 % (dintre obiecțiile formulate de autoritatea poloneză).
([21]) Articolele 64, 65 și, respectiv, 66 din RGPD.
([22]) Avize emise în temeiul articolului 64 alineatul (2) din RGPD.

Mecanismul pentru asigurarea coerenței

- Comitetul a adoptat 190 de avize privind coerența.
- Nouă decizii obligatorii au fost adoptate în cadrul soluționării litigiilor ([23]). Toate acestea au solicitat autorității principale pentru protecția datelor să își modifice proiectul de decizie, iar mai multe dintre ele au condus la amenzi semnificative.
- Cinci autorități de protecție a datelor au adoptat măsuri provizorii în cadrul procedurii de urgență (Germania, Finlanda, Italia, Norvegia și Spania).
- Două autorități pentru protecția datelor au solicitat o decizie obligatorie urgentă a comitetului ([24]), iar comitetul a dispus măsuri definitive urgente într-un caz.

2.3 O mai bună asigurare a respectării legii

În ultimii ani, autoritățile pentru protecția datelor au înregistrat o creștere semnificativă a activității de asigurare a respectării legislației, inclusiv prin aplicarea unor amenzi substanțiale în cazuri de referință împotriva unor societăți multinaționale din domeniul „*big tech*”. De exemplu, au fost aplicate amenzi pentru: (i) încălcarea legalității și securității prelucrării; (ii) încălcarea prelucrării unor categorii speciale de date cu caracter personal și (iii) nerespectarea drepturilor persoanelor fizice ([25]). Acest lucru a determinat societățile private să „ia în serios protecția datelor” ([26]) și a contribuit la integrarea unei culturi a conformității în organizații. Autoritățile pentru protecția datelor adoptă decizii prin care constată încălcări ale RGPD în cazurile bazate pe plângeri și în cele deschise din proprie inițiativă. Deși astfel de proceduri nu sunt disponibile în toate statele membre, multe autorități pentru protecția datelor au utilizat în mod eficace procedurile de „soluționare pe cale amiabilă” pentru a soluționa rapid cazurile bazate pe plângeri astfel încât reclamantul să fie mulțumit. Propunerea privind normele de procedură recunoaște posibilitatea ca plângerile să fie soluționate pe cale amiabilă ([27]).

Autoritățile pentru protecția datelor și-au utilizat pe scară largă competențele corective, deși numărul măsurilor corective impuse variază foarte mult de la o autoritate la alta. În afară de amenzi, măsurile corective cel mai frecvent utilizate au fost avertismentele, mustrările și ordinele de respectare a RGPD. Operatorii și persoanele împuternicite de operatori contestă frecvent deciziile de constatare a unor încălcări ale RGPD la instanțele naționale, cel mai adesea din motive procedurale ([28]).

([23]) Prevăzută la articolul 65 alineatul (1) litera (a) din RGPD.
([24]) În temeiul articolului 66 alineatul (2) din RGPD.
([25]) A se vedea punctul 5.3.4 din contribuția comitetului.
([26]) Raportul FRA, pagina 36.
([27]) Propunerea privind normele procedurale, articolul 5.
([28]) În România, toate cele 26 de decizii de constatare a unei încălcări au fost contestate în instanță, în timp ce în Țările de Jos rata de contestare a fost de 23 %. Cea mai ridicată rată de succes a contestărilor a fost înregistrată în Belgia (39 %).

O mai bună asigurare a respectării legii

- Autoritățile pentru protecția datelor au inițiat peste 20 000 de investigații din proprie inițiativă ([29]).
- Acestea primesc împreună peste 100 000 de plângeri pe an ([30]).
- Timpul median pentru tratarea plângerilor de către autoritățile pentru protecția datelor (de la primire până la închiderea cazului) variază între 1 și 12 luni și este de cel mult 3 luni în cinci state membre [Danemarca (1 lună), Spania (1,5 luni), Estonia (3 luni), Grecia (3 luni) și Irlanda (3 luni)].
- Peste 20 000 de plângeri au fost soluționate pe cale amiabilă. Această procedură este utilizată cel mai frecvent în Austria, Ungaria, Luxemburg și Irlanda.
- În 2022, autoritățile pentru protecția datelor din Germania au adoptat cel mai mare număr de decizii de impunere a unei măsuri corective (3 261), urmate de Spania (774), Lituania (308) și Estonia (332). Cele mai puține măsuri corective au fost impuse în Liechtenstein (8), Cehia (8), Islanda (10), Țările de Jos (17) și Luxemburg (22).
- Autoritățile pentru protecția datelor au aplicat peste 6 680 de amenzi în valoare de aproximativ 4,2 miliarde EUR ([31]). Cea mai mare valoare totală a amenzilor aplicate a fost înregistrată de autoritatea din Irlanda (2,8 miliarde EUR), urmată de Luxemburg (746 de milioane EUR), Italia (197 de milioane EUR) și Franța (131 de milioane EUR). Liechtenstein (9 600 EUR), Estonia (201 000 EUR) și Lituania (435 000 EUR) au aplicat amenzile cu cea mai mică valoare totală.

Deși majoritatea autorităților pentru protecția datelor consideră că instrumentele lor de investigare sunt adecvate, unele dintre ele necesită instrumente suplimentare la nivel național, de exemplu sancțiuni adecvate în cazul în care operatorii nu cooperează sau nu furnizează informațiile necesare ([32]). Autoritățile pentru protecția datelor consideră că resursele insuficiente și lacunele în materie de expertiză tehnică și juridică reprezintă principalul factor care le afectează capacitatea de asigurare a respectării legislației ([33]).

2.4 Comitetul

Comitetul este alcătuit din șeful unei autorități pentru protecția datelor din fiecare stat membru și din Autoritatea Europeană pentru Protecția Datelor, Comisia participând fără drept de vot. Comitetul, sprijinit în activitatea sa de secretariatul său, are sarcina de a asigura aplicarea coerentă a RGPD ([34]). Majoritatea autorităților pentru protecția datelor consideră că comitetul a jucat un rol pozitiv în consolidarea cooperării dintre acestea ([35]). Multe autorități pentru protecția datelor alocă resurse semnificative activităților

([29]) Autoritățile pentru protecția datelor din Germania au inițiat cel mai mare număr de investigații din proprie inițiativă (7 647), urmate de Ungaria (3 332), Austria (1 681) și Franța (1 571).

([30]) În 2022, nouă autorități pentru protecția datelor au primit peste 2 000 de plângeri. Cele mai multe plângeri au fost înregistrate de Germania (32 300), Italia (30 880), Spania (15 128), Țările de Jos (13 133) și Franța (12 193), iar cele mai puține au fost înregistrate de Liechtenstein (40), Islanda (140) și Croația (271).

([31]) Toate autoritățile au aplicat amenzi administrative, cu excepția Danemarcei, care nu prevede amenzi administrative. Cele mai multe amenzi au fost aplicate în Germania (2 106) și Spania (1 596). Cele mai puține amenzi au fost aplicate în Liechtenstein (3), Islanda (15) și Finlanda (20).

([32]) Raportul FRA, pagina 38.

([33]) Raportul FRA, paginile 20 și 23. A se vedea și poziția și constatările Consiliului, punctul 17.

([34]) Articolul 70 alineatul (1) din RGPD.

([35]) Raportul FRA, pagina 64.

comitetului, însă autoritățile mai mici indică faptul că dimensiunea lor le împiedică să se implice pe deplin ([36]). Unele autorități consideră că ar trebui îmbunătățită eficiența proceselor comitetului, în special reducând numărul reuniunilor și acordând mai puțină atenție aspectelor minore ([37]). În funcție de rezultatul negocierilor referitoare la propunerea privind normele procedurale ale RGPD, care vizează reducerea numărului de cazuri prezentate comitetului pentru soluționarea litigiilor, ar putea fi necesar să se analizeze dacă comitetul are nevoie de resurse suplimentare.

Până în noiembrie 2023, comitetul a adoptat 35 de orientări. Deși părțile interesate și autoritățile pentru protecția datelor le-au considerat utile, ambele consideră că orientările ar trebui puse la dispoziție mai rapid și că ar trebui îmbunătățită calitatea lor ([38]). Părțile interesate remarcă faptul că acestea sunt adesea excesiv de teoretice, prea lungi și nu reflectă abordarea bazată pe riscuri a RGPD ([39]). Autoritățile pentru protecția datelor și comitetul ar trebui să ofere orientări concise și practice care să ofere răspunsuri la probleme concrete și să reflecte un echilibru între protecția datelor și alte drepturi fundamentale. De asemenea, orientările ar trebui să fie ușor de înțeles pentru persoanele fără studii juridice, de exemplu în cadrul IMM-urilor și al organizațiilor de voluntariat ([40]). O modalitate de a realiza acest lucru este printr-un proces mai transparent de elaborare a orientărilor și prin consultări într-un stadiu incipient pentru a permite o mai bună înțelegere a dinamicii pieței, a practicilor comerciale și a modului de aplicare a orientărilor în practică ([41]). Este binevenit faptul că, în cadrul strategiei sale pentru perioada 2024-2027, comitetul și-a subliniat obiectivul de a oferi orientări practice accesibile publicului relevant ([42]).

Părțile interesate subliniază necesitatea unor orientări suplimentare, în special în ceea ce privește anonimizarea și pseudonimizarea ([43]), interesul legitim și cercetarea științifică ([44]). În raportul din 2020, Comisia a invitat comitetul să adopte orientări privind cercetarea științifică, dar orientările nu au fost încă adoptate. Recunoscând importanța cercetării științifice în societate, în special pentru a monitoriza bolile și a dezvolta tratamente, precum și pentru a stimula inovarea, este esențial ca autoritățile pentru protecția datelor să acționeze pentru a clarifica aceste chestiuni fără întârziere ([45]). De asemenea, autorităților publice le-ar fi utile orientări care să abordeze provocările specifice cu care se confruntă ([46]).

2.5 Autoritățile pentru protecția datelor

2.5.1 Independență și resurse

Independența autorităților pentru protecția datelor este consacrată în Carta drepturilor fundamentale a UE și în Tratatul privind funcționarea UE. RGPD prevede cerințe pentru

([36]) Raportul FRA, pagina 67. În 2023, autoritățile germane pentru protecția datelor au alocat cele mai multe resurse activităților comitetului [26 de echivalente normă întreagă (ENI)], urmate de Irlanda (16) și Franța (12) (contribuția comitetului).
([37]) Raportul FRA, pagina 67.
([38]) Raportul FRA, pagina 67; rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([39]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([40]) A se vedea și poziția și constatările Consiliului, punctul 45.
([41]) A se vedea și poziția și constatările Consiliului, punctul 34.
([42]) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf.
([43]) A se vedea și poziția și constatările Consiliului, punctul 31 litera (d).
([44]) Acestea necesită clarificări, în special în ceea ce privește semnificația termenului „cercetare științifică”, rolul consimțământului pentru prelucrarea datelor cu caracter personal în scopul cercetării, temeiul juridic relevant și rolurile și responsabilitatea actorilor implicați.
([45]) A se vedea și poziția și constatările Consiliului, punctul 31 litera (b).
([46]) Poziția și constatările Consiliului, punctele 27-28.

asigurarea „independenței depline” a autorităților pentru protecția datelor ([47]). Raportul FRA a concluzionat că majoritatea autorităților pentru protecția datelor funcționează independent de guvern, de parlament și de orice alte organisme publice ([48]).

Autoritățile pentru protecția datelor au nevoie de resurse umane, tehnice și financiare adecvate pentru a-și putea îndeplini în mod eficace și independent sarcinile care le revin conform RGPD. În raportul din 2020, Comisia a remarcat că alocarea de resurse autorităților pentru protecția datelor nu era încă satisfăcătoare și a abordat în mod constant această problemă cu statele membre. Situația s-a îmbunătățit de atunci.

Resurse sporite pentru autoritățile pentru protecția datelor ([49])

- În perioada 2020-2024, toate autoritățile pentru protecția datelor cu excepția a două au beneficiat de o creștere a personalului, iar creșterea a depășit 25 % în 14 state membre.
- Autoritatea pentru protecția datelor din Irlanda a înregistrat cea mai mare creștere a personalului (79 %), urmată de Estonia, Suedia (ambele cu 57 %) și Bulgaria (56 %).
- În Cehia s-a înregistrat o ușoară scădere a personalului autorității (-1 %), în timp ce în Liechtenstein nu a existat nicio creștere, iar creșteri minore s-au înregistrat în Cipru (4 %) și Ungaria (8 %).
- În perioada 2020-2024, toate autoritățile pentru protecția datelor cu excepția uneia au înregistrat o creștere a bugetului, iar creșterea a depășit 50 % în 13 state membre.
- Autoritatea pentru protecția datelor din Cipru a înregistrat cea mai mare creștere a bugetului (130 %), urmată de Austria (107 %), Bulgaria (100 %) și Estonia (97 %).
- Bugetul autorității elene pentru protecția datelor a scăzut cu 15 %, iar creșteri bugetare minore au înregistrat autoritățile din Liechtenstein (1 %), Slovacia (6 %) și Cehia (8 %).

Deși aceste statistici indică o tendință generală ascendentă în ceea ce privește alocarea de resurse autorităților pentru protecția datelor, autoritățile însele consideră că încă nu dispun de resurse umane suficiente ([50]). Ele subliniază că sunt necesare cunoștințe tehnice foarte specializate, în special în ceea ce privește tehnologiile noi și emergente ([51]), și că lipsa acestora afectează cantitatea și calitatea muncii lor, precum și că întâmpină dificultăți în a concura pentru resursele umane cu sectorul privat. Autoritățile pentru protecția datelor menționează insuficiența cunoștințelor juridice și lipsa competențelor lingvistice ca factori care le afectează performanța. Remunerația scăzută, incapacitatea de a-și selecta în mod autonom personalul și volumul mare de muncă sunt evidențiate ca fiind factorii-cheie care afectează capacitatea autorităților de a recruta și de a păstra personalul ([52]). Autoritățile pentru protecția datelor subliniază, de asemenea, că au nevoie de resurse financiare pentru

([47]) Articolul 52 din RGPD.
([48]) Raportul FRA, pagina 31.
([49]) A se vedea secțiunea 4.4.1 din contribuția comitetului, inclusiv pentru cifrele absolute.
([50]) Doar cinci autorități pentru protecția datelor consideră că dispun de resurse umane adecvate (contribuția comitetului, pagina 33).
([51]) Raportul FRA, pagina 20. Unele autorități pentru protecția datelor externalizează unor contractanți externi anumite sarcini, cum ar fi tratarea plângerilor, analiza juridică și analiza criminalistică.
([52]) Raportul FRA, pagina 24.

a-și moderniza și digitaliza procesele și pentru a achiziționa echipamente tehnice ([53]). Toate autoritățile pentru protecția datelor îndeplinesc sarcini care le depășesc pe cele care le-au fost încredințate prin RGPD ([54]), de exemplu în calitate de autorități de supraveghere pentru Directiva privind protecția datelor în scopul asigurării respectării legii și Directiva asupra confidențialității și comunicațiilor electronice, iar multe dintre ele își exprimă îngrijorarea cu privire la asumarea unor responsabilități suplimentare în temeiul noii legislații în domeniul digital ([55]).

2.5.2 Dificultăți în tratarea unui număr mare de plângeri

Mai multe autorități pentru protecția datelor indică faptul că prea multe dintre resursele lor sunt utilizate pentru tratarea unui număr mare de plângeri, dintre care majoritatea sunt considerate banale și nefondate, întrucât tratarea fiecărei plângeri este o obligație în temeiul RGPD care face obiectul controlului jurisdicțional ([56]). Aceasta înseamnă că autoritățile pentru protecția datelor nu pot aloca suficiente resurse pentru alte activități, cum ar fi investigațiile din proprie inițiativă, campaniile de sensibilizare a publicului și colaborarea cu operatorii ([57]). În calitate de autorități publice, autoritățile pentru protecția datelor au libertatea de a-și aloca resursele după cum consideră necesar pentru a-și îndeplini fiecare dintre sarcinile [enumerate la articolul 57 alineatul (1) din RGPD] de interes public. Multe autorități pentru protecția datelor au adoptat strategii de eficientizare a tratării plângerilor, cum ar fi automatizarea ([58]), utilizarea procedurilor de soluționare pe cale amiabilă ([59]) și „gruparea” plângerilor care se referă la probleme similare ([60]).

2.5.3 Interpretarea RGPD de către autoritățile naționale pentru protecția datelor

Un obiectiv central al RGPD a fost eliminarea abordării fragmentate a protecției datelor care exista în temeiul Directivei anterioare privind protecția datelor (Directiva 95/46/CE) ([61]). Cu toate acestea, autoritățile pentru protecția datelor continuă să adopte interpretări divergente cu privire la concepte-cheie privind protecția datelor ([62]). Părțile interesate apreciază că acest lucru este principalul obstacol în calea aplicării consecvente a RGPD în UE. Persistența interpretărilor divergente creează insecuritate juridică și mărește costurile întreprinderilor (de exemplu prin faptul că se solicită documente diferite pentru mai multe state membre), perturbându-se astfel libera circulație a datelor cu caracter personal în UE, împiedicându-se activitățile comerciale transfrontaliere și îngreunându-se cercetarea și inovarea cu privire la provocările societale urgente.

Printre problemele specifice menționate de părțile interesate se numără următoarele: (i) faptul că autoritățile pentru protecția datelor din trei state membre au puncte de vedere diferite în ceea ce privește temeiul juridic adecvat pentru prelucrarea datelor cu caracter personal atunci când realizează un trial clinic; (ii) faptul că există frecvent opinii divergente cu privire la statutul unei entități de operator sau de persoană împuternicită de operator și (iii) faptul că, în unele cazuri, autoritățile pentru protecția datelor nu respectă orientările comitetului sau publică orientări la nivel național care contravin celor emise de

([53]) Raportul FRA, pagina 22.
([54]) A se vedea secțiunea 4.4.5 din contribuția comitetului.
([55]) Contribuția comitetului, pagina 32.
([56]) Raportul FRA, pagina 48.
([57]) Raportul FRA, pagina 45. Autoritățile pentru protecția datelor consideră că investigațiile din oficiu sunt deosebit de importante, deoarece este posibil ca reclamanții să nu aibă cunoștință de multe încălcări ale RGPD.
([58]) Raportul FRA, pagina 8.
([59]) Raportul FRA, pagina 39.
([60]) Raportul FRA, pagina 41.
([61]) Considerentul 9 din RGPD.
([62]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.

comitet ([63]). Aceste aspecte sunt agravate atunci când mai multe autorități pentru protecția datelor din cadrul unui singur stat membru adoptă interpretări contradictorii.

Unele părți interesate consideră, de asemenea, că anumite autorități pentru protecția datelor și comitetul adoptă interpretări care se abat de la abordarea bazată pe riscuri a RGPD, ceea ce reprezintă o provocare pentru dezvoltarea economiei digitale ([64]) și pentru libertatea și pluralitatea mass-mediei. Acestea menționează ca aspecte care generează îngrijorări: (i) interpretarea anonimizării; (ii) temeiul juridic al interesului legitim și al consimțământului ([65]) și (iii) excepțiile de la interzicerea procesului decizional individual automatizat ([66]). Ar trebui reamintit faptul că autoritățile pentru protecția datelor și comitetul au sarcina de a asigura atât protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal, cât și libera circulație a datelor cu caracter personal în cadrul UE. Astfel cum se recunoaște în RGPD ([67]), dreptul la protecția datelor cu caracter personal trebuie să fie luat în considerare în raport cu funcția sa în societate și să fie echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității.

2.5.4 Colaborarea cu operatorii și cu persoanele împuternicite de operatori

Părțile interesate subliniază avantajul de a se putea angaja într-un dialog constructiv cu autoritățile pentru protecția datelor pentru a se asigura că respectă RGPD de la bun început, în special în ceea ce privește tehnologiile emergente. Părțile interesate remarcă faptul că unele autorități pentru protecția datelor colaborează activ cu operatorii, în timp ce altele răspund târziu, dau răspunsuri vagi sau nu răspund deloc ([68]).

3 PUNEREA ÎN APLICARE A RGPD DE CĂTRE STATELE MEMBRE

3.1 Fragmentarea aplicării la nivel național

Fiind regulament, RGPD este direct aplicabil, dar el impune statelor membre să legifereze în anumite domenii și le oferă posibilitatea de a detalia mai mult dispozițiile privind aplicarea sa într-un număr redus de domenii ([69]). Atunci când legiferează la nivel național, statele membre trebuie să facă acest lucru în condițiile și în limitele prevăzute în RGPD. La fel ca în 2020, părțile interesate declară că se confruntă cu dificultăți care decurg din fragmentarea normelor naționale în situațiile în care statele membre au posibilitatea de a detalia dispozițiile RGPD, în special în ceea ce privește:

- vârsta minimă pentru consimțământul copilului în legătură cu oferirea de servicii ale societății informaționale copilului respectiv ([70]);
- introducerea de către statele membre a unor condiții suplimentare privind prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea ([71]);
- prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni ([72]), ceea ce creează dificultăți în anumite sectoare reglementate.

([63]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([64]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([65]) Articolul 6 alineatul (1) litera (f) și, respectiv, articolul 6 alineatul (1) litera (a) din RGPD.
([66]) Articolul 22 alineatul (2) din RGPD.
([67]) Considerentul 4.
([68]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([69]) De exemplu, vârsta minimă pentru consimțământul copiilor în legătură cu serviciile societății informaționale [articolul 8 alineatul (1) din RGPD].
([70]) Articolul 8 alineatul (1) din RGPD.
([71]) Posibilitate prevăzută la articolul 9 alineatul (4) din RGPD.
([72]) Articolul 10 din RGPD.

În același timp, un aspect important este faptul că multe părți interesate declară că problemele de fragmentare apar în principal din interpretările divergente ale RGPD de către autoritățile pentru protecția datelor, mai degrabă decât din utilizarea clauzelor facultative de precizare de către statele membre.

Statele membre consideră că un grad limitat de fragmentare poate fi acceptabil, iar clauzele de precizare prevăzute în RGPD rămân utile, în special pentru prelucrarea de către autoritățile publice ([73]). RGPD impune statelor membre să consulte autoritatea națională pentru protecția datelor atunci când elaborează legislație referitoare la prelucrarea datelor cu caracter personal ([74]). Raportul FRA a concluzionat că unele guverne au stabilit termene foarte scurte pentru aceste autorități și, în unele cazuri, nu le consultă deloc ([75]).

3.2 Monitorizarea de către Comisie

Comisia monitorizează în permanență punerea în aplicare a RGPD. Comisia a inițiat proceduri de constatare a neîndeplinirii obligațiilor împotriva statelor membre cu privire la aspecte precum independența autorităților pentru protecția datelor (inclusiv libertatea de a rămâne fără influență externă și disponibilitatea unei căi de atac judiciare în caz de concediere) ([76]) și dreptul la o cale de atac judiciară eficientă pentru persoanele vizate în cazul în care autoritatea pentru protecția datelor nu tratează o plângere ([77]). În cadrul monitorizării sale, Comisia solicită, de asemenea, ca autoritățile pentru protecția datelor să furnizeze, în mod strict confidențial, informații periodice ([78]) privind cazurile transfrontaliere la scară largă aflate în derulare, în special cele referitoare la marile societăți multinaționale din domeniul „*big tech*”.

Comisia comunică periodic cu statele membre cu privire la punerea în aplicare a RGPD. Astfel cum se prevede în raportul din 2020, Comisia a continuat să utilizeze Grupul de experți al statelor membre privind RGPD ([79]) pentru a facilita discuțiile și schimbul de experiență privind punerea în aplicare eficace a RGPD. Grupul de experți a purtat discuții specifice referitoare la: (i) supravegherea instanțelor care acționează în exercițiul funcției lor judiciare (articolul 55 din RGPD; articolul 8 din Cartă); (ii) reconcilierea dreptului la protecția datelor cu dreptul la libertatea de exprimare (articolul 85 din RGPD) și (iii) dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere (articolul 78 din RGPD). În urma acestor discuții, Comisia a compilat prezentări generale ale abordărilor adoptate privind punerea în aplicare a dispozițiilor respective în statele membre ([80]). De asemenea, Comisia a utilizat acest grup pentru a face schimb de opinii cu statele membre atunci când a elaborat propunerea privind normele procedurale.

Conformitatea legislației și practicilor naționale cu normele în materie de protecție a datelor prevăzute în corpusul legislativ al UE privind spațiul Schengen este, de asemenea, evaluată în cadrul evaluărilor Schengen, efectuate în comun de statele membre și de Comisie. Se efectuează cel puțin cinci evaluări ale protecției datelor la fața locului pe an,

---

([73]) Poziția și constatările Consiliului, punctul 30.
([74]) Articolul 36 din RGPD.
([75]) Raportul FRA, pagina 11.
([76]) Belgia (2021/4045) și Belgia (2022/2160).
([77]) Finlanda (2022/4010) și Suedia (2022/2022).
([78]) Cu informații privind numărul de referință al cazului, tipul investigației (din proprie inițiativă sau ca urmare a unei plângeri), un rezumat al domeniului de aplicare al investigației, autoritățile pentru protecția datelor vizate, principalele etape procedurale parcurse și datele aferente, măsurile de investigare sau orice alte măsuri luate și datele aferente.
([79]) https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&do=groupDetail.groupDetail&groupID=3461.
([80]) https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=31754&fromExpertGroups=3461.

axate în prezent pe sistemele informatice la scară largă și pe Sistemul de informații Schengen, pe Sistemul de informații privind vizele, precum și pe rolul de supraveghere al autorităților naționale pentru protecția datelor asupra acestor sisteme.

Comisia contribuie în mod activ la numărul mare de cauze aflate pe rolul Curții de Justiție (cu aproximativ 30 de decizii preliminare pe an în ultimii ani), ceea ce joacă un rol central în interpretarea coerentă a conceptelor-cheie ale RGPD. Un corpus din ce în ce mai mare de jurisprudență a Curții a oferit mai multe clarificări, de exemplu privind definiția datelor cu caracter personal ([81]), categoriile speciale de date cu caracter personal ([82]), operatorul ([83]), consimțământul ([84]), interesul legitim ([85]), dreptul de acces ([86]), dreptul la ștergerea datelor ([87]), dreptul la despăgubiri ([88]), procesul decizional individual automatizat ([89]), amenzile administrative ([90]), responsabilii cu protecția datelor ([91]), publicarea datelor cu caracter personal în registre ([92]) și aplicarea RGPD în activitățile parlamentelor ([93]).

4 DREPTURILE PERSOANELOR VIZATE

Sensibilizarea persoanelor cu privire la RGPD și la autoritățile pentru protecția datelor (Eurobarometrul 549 din 2024 privind justiția, drepturile și valorile)

- 72 % dintre respondenții din întreaga UE declară că au auzit de RGPD, iar 40 % dintre aceștia știu ce este RGPD.
- În 19 state membre, peste 70 % dintre respondenți declară că sunt conștienți de RGPD, respondenții din Suedia (92 %) fiind cei mai conștienți, urmați de cei din Țările de Jos (88 %), Malta și Danemarca (84 %), în timp ce respondenții din Bulgaria (59 %) sunt cei mai puțin conștienți, urmați de cei din Lituania (63 %) și Franța (64 %).
- 68 % dintre respondenții din întreaga UE declară că au auzit de o autoritate națională responsabilă cu protecția drepturilor lor în materie de protecție a datelor, 24 % dintre respondenți declarând că știu și ce autoritate publică are această responsabilitate.
- În toate statele membre, cel puțin jumătate dintre respondenți au auzit de o astfel de autoritate națională, cele mai ridicate niveluri fiind înregistrate în Țările de Jos (82 %), Cehia, Slovenia și Polonia (toate 75 %) și Portugalia (74 %). Respondenții din Austria (56 %) și Spania (58 %) cunosc cel mai puțin această autoritate.

Persoanele fizice sunt din ce în ce mai familiarizate și își exercită în mod activ drepturile în temeiul RGPD ([94]). Autoritățile pentru protecția datelor alocă resurse substanțiale pentru promovarea sensibilizării publicului larg cu privire la drepturile și obligațiile în materie de

([81]) Cauza C-319/22, ECLI:EU:C:2023:837.
([82]) Cauzele C-184/20, ECLI:EU:C:2022:601; C-252/21, ECLI:EU:C:2023:537.
([83]) Cauzele C-683/21, ECLI:EU:C:2023:949; C-604/22, ECLI:EU:C:2024:214; C-231/22, ECLI:EU:C:2024:7.
([84]) Cauza C-61/19, ECLI:EU:C:2020:901.
([85]) Cauzele C-597/19, ECLI:EU:C:2021:492; C-252/21, ECLI:EU:C:2023:537.
([86]) Cauzele C-307/22, ECLI:EU:C:2023:811; C-154/21, ECLI:EU:C:2023:3.
([87]) Cauza C-460/20, ECLI:EU:C:2022:962.
([88]) Cauza C-300/21, ECLI:EU:C:2023:370; cauza C-687/21, ECLI:EU:C:2024:72; cauza C-667/21, ECLI:EU:C:2023:1022.
([89]) Cauzele conexate C-26/22 și C-64/22, ECLI:EU:C:2023:958.
([90]) Cauzele C-807/21, ECLI:EU:C:2023:950; Cauza C-683/21, ECLI:EU:C:2023:949.
([91]) Cauza C-453/21, ECLI:EU:C:2023:79.
([92]) Cauzele C-439/19, ECLI:EU:C:2021:504; C-184/20, ECLI:EU:C:2022:601.
([93]) Cauzele C-33/22, ECLI:EU:C:2024:46; C-272/19, ECLI:EU:C:2020:535.
([94]) Poziția și constatările Consiliului, punctul 13.

protecție a datelor, de exemplu prin intermediul platformelor de comunicare socială și al campaniilor de televiziune, al liniilor de asistență telefonică, al buletinelor informative și al prezentărilor în cadrul instituțiilor de învățământ ([95]). Multe dintre aceste inițiative au beneficiat de finanțare din partea UE ([96]). Agenția pentru Drepturi Fundamentale observă că, deși gradul de sensibilizare a publicului larg cu privire la protecția datelor a crescut, încă lipsește înțelegerea protecției datelor, după cum o demonstrează numărul mare de plângeri banale sau nefondate ([97]). Au fost dezvoltate mai multe instrumente digitale ușor de utilizat pentru a facilita exercitarea drepturilor persoanei vizate ([98]). Actele legislative, în special Regulamentul privind guvernanța datelor ([99]), ar trebui să conducă la crearea unor modalități suplimentare pentru ca persoana vizată să își exercite drepturile în viitor. Întreprinderile remarcă faptul că dreptul la ștergerea datelor este utilizat din ce în ce mai mult, deși dreptul de rectificare și dreptul la opoziție sunt utilizate rareori.

4.1 Dreptul de acces

Operatorii raportează că dreptul de acces (articolul 15 din RGPD) este dreptul invocat cel mai frecvent de persoanele vizate. Deși comitetul a adoptat orientări privind acest drept în 2022, operatorii continuă să raporteze că întâmpină dificultăți, de exemplu atunci când interpretează noțiunea de „cereri nefondate sau excesive” ([100]), atunci când răspund unui număr mare de cereri și atunci când tratează cereri care sunt formulate în scopuri care nu au legătură cu protecția datelor, de exemplu pentru a colecta probe în cadrul procedurilor judiciare ([101]). Organizațiile societății civile observă că răspunsurile la cererile de acces sunt adesea întârziate sau incomplete, iar datele primite nu sunt întotdeauna într-un format lizibil ([102]). Autoritățile publice invocă dificultăți în interacțiunea dintre dreptul de acces și normele privind accesul public la documente ([103]). Prin urmare, este binevenit faptul că, în februarie 2024, comitetul a lansat o acțiune comună privind un cadru coordonat de asigurare a respectării normelor cu privire la dreptul de acces ([104]).

4.2 Dreptul la portabilitatea datelor

În raportul din 2020, Comisia s-a angajat să exploreze mijloace practice de facilitare a unei utilizări sporite a dreptului la portabilitatea datelor (articolul 20 din RGPD) de către persoane fizice, în concordanță cu strategia privind datele. Între timp, Comisia a adoptat o serie de inițiative care completează acest drept. Aceste inițiative facilitează trecerea de la un serviciu la altul, creând astfel o gamă mai largă de opțiuni pentru persoanele fizice, sprijinind concurența și inovarea și permițând persoanelor să profite de avantajele utilizării datelor lor. Regulamentul privind datele oferă utilizatorilor de dispozitive inteligente un drept sporit la portabilitatea datelor generate prin intermediul dispozitivelor respective și prevede ca proiectarea produsului sau a unui server *back-end* al producătorului sau al deținătorului de date să facă posibilă din punct de vedere tehnic o astfel de portabilitate.

([95]) Contribuția comitetului, secțiunea 6.
([96]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en.
([97]) Raportul FRA, paginile 9 și 48.
([98]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([99]) Articolul 10 din Regulamentul (UE) 2022/868 (Regulamentul privind guvernanța datelor), JO L 152, 3.6.2022, p. 1.
([100]) Articolul 12 alineatul (5) din RGPD.
([101]) Totuși, Curtea de Justiție a clarificat faptul că persoana vizată nu este obligată să precizeze motivele pentru care solicită accesul la datele cu caracter personal: cauza C-307/22, CS ECLI:EU:C:2023:811, punctul 38.
([102]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([103]) Poziția și constatările Consiliului, punctele 27-28.
([104]) https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_en.

Regulamentul privind piețele digitale impune furnizorilor de servicii de platformă esențiale identificați drept „controlori de acces” să asigure portabilitatea efectivă a datelor utilizatorilor, inclusiv accesul continuu și în timp real la astfel de date. Alte câteva inițiative ale Comisiei aflate în curs de negociere sau cu privire la care s-a ajuns la un acord politic prevăd drepturi sporite la portabilitatea datelor în anumite domenii, cum ar fi Directiva privind lucrul pe platforme ([105]), spațiul european comun al datelor privind sănătatea ([106]) și cadrul pentru accesul la date financiare ([107]).

4.3 Dreptul de a depune o plângere

După cum arată din numărul mare de plângeri, există o cunoaștere largă a dreptului de a depune o plângere la o autoritate pentru protecția datelor. Organizațiile societății civile evidențiază diferențele nejustificate dintre practicile naționale de tratare a plângerilor, aspect care este abordat în propunerea Comisiei privind normele procedurale. Puține state membre și-au exercitat opțiunea în temeiul RGPD de a oferi unui organism fără scop lucrativ dreptul de a lua măsuri independent de mandatul unei persoane vizate [articolul 80 alineatul (2)]. Cu toate acestea, Directiva privind acțiunile în reprezentare ([108]), adoptată în 2020, va conduce la o mai mare armonizare în acest sens prin facilitarea acțiunilor colective ale persoanelor fizice pentru încălcarea RGPD. Măsurile naționale de punere în aplicare a directivei au devenit aplicabile în iunie 2023.

4.4 Protecția datelor cu caracter personal ale copiilor

Copiii au nevoie de o protecție specifică atunci când le sunt prelucrate datele cu caracter personal ([109]). RGPD face parte dintr-un cadru juridic cuprinzător care asigură protecția copiilor atât offline, cât și online ([110]). Având în vedere prezența sporită a copiilor în mediul online, în ultimii ani au fost întreprinse o serie de acțiuni la nivelul UE și la nivel național pentru a sprijini protecția copiilor în mediul online. Autoritățile pentru protecția datelor au aplicat amenzi semnificative societăților care gestionează platforme de comunicare socială pentru încălcarea RGPD atunci când prelucrează datele copiilor. De asemenea, ele cooperează cu alte autorități pentru a impune o mai bună protecție a copiilor în domeniul publicității. În raportul din 2020, Comisia a invitat comitetul să adopte orientări privind prelucrarea datelor copiilor, iar această activitate este în desfășurare ([111]). Regulamentul privind serviciile digitale cuprinde dispoziții specifice pentru asigurarea unui nivel ridicat de confidențialitate, siguranță și securitate pentru copiii care utilizează platforme online.

Unele părți interesate raportează că întâmpină dificultăți în ceea ce privește exercitarea drepturilor persoanelor vizate, atunci când persoanele vizate sunt copii. În special, acestea

([105]) Lucrătorii pe platforme: Consiliul confirmă acordul cu privire la noi norme pentru îmbunătățirea condițiilor lor de muncă – Consilium (europa.eu).

([106]) Propunere de regulament referitor la spațiul european al datelor privind sănătatea [COM(2022) 197 final].

([107]) Propunere de regulament privind un cadru pentru accesul la date financiare și de modificare a Regulamentelor (UE) nr. 1093/2010, (UE) nr. 1094/2010, (UE) nr. 1095/2010 și (UE) 2022/2554 [COM(2023) 360 final].

([108]) Directiva (UE) 2020/1828 din 25 noiembrie 2020 privind acțiunile în reprezentare pentru protecția intereselor colective ale consumatorilor și de abrogare a Directivei 2009/22/CE, JO L 409, 4.12.2020, p. 1.

([109]) Considerentul 38 din RGPD.

([110]) Recomandare privind dezvoltarea și consolidarea unor sisteme integrate de protecție a copilului în interesul superior al copilului: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/combating-violence-against-children-and-ensuring-child-protection_ro.

([111]) A se vedea și poziția și constatările Consiliului, punctul 31 litera (a).

raportează că copiii nu își înțeleg pe deplin drepturile, nu au competențe de alfabetizare digitală și pot face obiectul unei influențe necuvenite ([112]). Comisia a finanțat mai multe inițiative la nivel național privind protecția datelor copiilor și promovarea sensibilizării copiilor cu privire la protecția datelor ([113]). În cadrul strategiei „Un internet mai bun pentru copii” (BIK+), Comisia le oferă copiilor resurse de sensibilizare și cursuri de formare cu privire la drepturile lor digitale, inclusiv la protecția datelor (de exemplu consimțământul digital) ([114]). Se pune un accent tot mai mare pe necesitatea unor instrumente eficace și favorabile vieții private de verificare a vârstei. La începutul anului 2024, Comisia a înființat împreună cu statele membre, cu comitetul și cu Grupul autorităților europene de reglementare pentru serviciile mass-media audiovizuale, un grup operativ privind verificarea vârstei, cu scopul de a discuta și de a sprijini dezvoltarea unei abordări la nivelul UE pentru verificarea vârstei. Această activitate va continua de acum în cadrul comitetului instituit în temeiul Regulamentului privind serviciile digitale, în Grupul de lucru pentru protecția minorilor. În contextul Regulamentului privind identitatea digitală europeană ([115]), care a intrat în vigoare în mai 2024, Comisia depune eforturi pentru a se asigura că portofelul european pentru identitatea digitală este oferit tuturor cetățenilor și rezidenților UE în 2026, inclusiv pentru verificarea vârstei. Între timp, înainte ca ecosistemul portofelului să fie pe deplin operațional, va fi dezvoltată și va deveni disponibilă în întreaga UE o soluție pe termen scurt pentru verificarea vârstei.

5 OPORTUNITĂȚI ȘI PROVOCĂRI PENTRU ORGANIZAȚII, ÎN SPECIAL PENTRU IMM-URI

RGPD a creat condiții de concurență echitabile pentru întreprinderile care își desfășoară activitatea pe piața internă, iar abordarea sa neutră din punct de vedere tehnologic și favorabilă inovării le permite întreprinderilor să reducă birocrația și să beneficieze de o mai mare încredere a consumatorilor ([116]). Multe întreprinderi au dezvoltat o cultură internă a protecției datelor și consideră protecția vieții private și a datelor drept parametri esențiali ai concurenței. Întreprinderile apreciază abordarea bazată pe riscuri a RGPD ca principiu director care permite flexibilitatea și scalabilitatea obligațiilor lor ([117]).

5.1 Set de instrumente pentru întreprinderi

RGPD oferă un set de instrumente care le permit organizațiilor să își gestioneze și să își demonstreze în mod flexibil conformitatea, incluzând coduri de conduită, mecanisme de certificare și clauze contractuale standard. Astfel cum s-a anunțat în raportul din 2020, Comisia a adoptat clauze contractuale standard privind relația operator-persoană împuternicită de operator în 2021 ([118]). Aceste clauze contractuale standard oferă un instrument voluntar de asigurare a conformității pregătit și ușor de pus în aplicare, care

([112]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([113]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en.
([114]) https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids.
([115]) Regulamentul (UE) 2024/1183 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală, JO L, 2024/1183, 30.4.2024.
([116]) Astfel cum se recunoaște în raportul platformei „Pregătiți pentru viitor”, un grup de experți la nivel înalt instituit pentru a ajuta Comisia în eforturile sale de simplificare a legislației UE și de reducere a costurilor inutile aferente: https://commission.europa.eu/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof/fit-future-platform-f4f_ro. A se vedea și rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD și poziția și constatările Consiliului, punctul 12.
([117]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([118]) Decizia de punere în aplicare (UE) 2021/915 a Comisiei din 4 iunie 2021 privind clauzele contractuale standard dintre operatori și persoanele împuternicite de operatori prevăzute la articolul 28 alineatul (7) din RGPD și la articolul 29 alineatul (7) din RGPD (C/2021/3701), JO L 199, 7.6.2021, p. 18.

este deosebit de util pentru IMM-uri sau pentru organizațiile care ar putea să nu dispună de resursele necesare pentru a negocia contracte individuale cu partenerii lor comerciali. Întreprinderile raportează un feedback mixt cu privire la utilizarea clauzelor contractuale standard, în sensul că unele societăți (în principal IMM-uri) le utilizează integral sau parțial, în timp ce altele (în cea mai mare parte societăți mai mari) tind să nu le utilizeze deoarece preferă să utilizeze propriile clauze.

Întreprinderile subliniază că codurile de conduită au un potențial major ca instrument de asigurare a conformității specific sectorului și eficient din punctul de vedere al costurilor ([119]). Cu toate acestea, elaborarea de coduri de conduită a fost redusă ([120]). Conform informațiilor disponibile până în prezent, la nivelul UE au fost aprobate doar două coduri (ambele în sectorul serviciilor de cloud), iar la nivel național au fost aprobate șase coduri ([121]). Părțile interesate raportează că se confruntă cu cerințe împovărătoare (printre care și necesitatea de a înființa un organism de monitorizare acreditat), cu o lipsă de implicare din partea autorităților pentru protecția datelor și cu un proces de aprobare îndelungat, aceștia fiind principalii factori care limitează adoptarea codurilor de conduită ([122]).

Este nevoie de o mai mare transparență a procesului și de termene clare de aprobare. Autoritățile pentru protecția datelor și, în cazul codurilor la nivelul UE, comitetul ar trebui să încurajeze mai activ elaborarea codurilor de conduită prin colaborarea cu asociațiile care elaborează codurile. Acest lucru va contribui la soluționarea diferențelor de interpretare și la accelerarea procesului de aprobare. Părțile interesate regretă întârzierile mari în adoptarea codurilor de conduită, cauzate de chestiunile discutate în paralel în cadrul lucrărilor privind orientările. Întreprinderile raportează, de asemenea, că certificarea nu este utilizată pe scară largă, deoarece procesul de dezvoltare este lent și complex. Ca și în cazul codurilor de conduită, autoritățile pentru protecția datelor ar trebui să prevadă termene mai clare pentru revizuire și aprobarea certificărilor.

În strategia sa pentru perioada 2024-2027, comitetul s-a angajat să sprijine în continuare măsurile de asigurare a conformității precum certificarea și codurile de conduită, inclusiv prin colaborarea cu principalele grupuri de părți interesate pentru a explica modul în care pot fi utilizate instrumentele ([123]).

5.2 Provocări specifice pentru IMM-uri și operatorii de mici dimensiuni

În raportul din 2020, Comisia a solicitat intensificarea eforturilor de sprijinire a respectării RGPD de către IMM-uri. În ultimii ani, autoritățile pentru protecția datelor și comitetul au continuat să dezvolte instrumente de asigurare a conformității pentru IMM-uri, sprijinite parțial prin finanțare din partea Comisiei ([124]). În aprilie 2023, comitetul a lansat un ghid privind protecția datelor pentru întreprinderile mici ([125]), care oferă IMM-urilor informații practice într-un format accesibil și ușor de înțeles.

IMM-urile din multe state membre subliniază beneficiile unui sprijin adaptat din partea autorităților lor locale pentru protecția datelor. Cu toate acestea, abordările diferite în materie de sensibilizare și orientare ale autorităților pentru protecția datelor arată că IMM-

([119]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([120]) Poziția și constatările Consiliului, punctul 25.
([121]) https://www.edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en?f%5B0%5D=coc_scope%3Anational.
([122]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([123]) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf.
([124]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en.
([125]) https://edpb.europa.eu/sme-data-protection-guide/home_en.

urile din anumite state membre percep conformitatea ca fiind complexă și se tem de procedurile de aplicare a legii ([126]). Autoritățile pentru protecția datelor ar trebui să își dubleze eforturile pentru a răspunde acestor provocări, inclusiv prin colaborarea proactivă cu IMM-urile pentru a elimina orice preocupări nefondate legate de conformitate. Autoritățile pentru protecția datelor ar trebui să se concentreze pe furnizarea de sprijin personalizat și de instrumente practice, de cum ar fi modele (de exemplu pentru efectuarea de evaluări ale impactului asupra protecției datelor), linii de asistență telefonică, exemple ilustrative, liste de verificare și orientări privind operațiuni de prelucrare specifice (de exemplu facturare sau buletine informative) și măsuri tehnice și organizatorice. Întrucât majoritatea IMM-urilor nu dispun de expertiză internă în materie de protecție a datelor, orice orientări destinate IMM-urilor ar trebui să fie ușor de înțeles de către persoanele fără studii juridice ([127]).

În concordanță cu abordarea bazată pe riscuri a RGPD, IMM-urile care desfășoară activități de prelucrare cu risc scăzut nu sunt confruntate cu o sarcină substanțială de asigurare a conformității. Deși derogarea de la păstrarea evidențelor privind activitățile de prelucrare ([128]) se aplică în circumstanțe limitate ([129]), IMM-urile care efectuează operațiuni de prelucrare cu risc scăzut se pot conforma păstrând evidențe simplificate pe baza modelelor furnizate de autoritățile pentru protecția datelor. În plus, astfel de evidențe ar trebui considerate un instrument util pentru ca IMM-urile să facă un bilanț al activităților lor de prelucrare.

5.3 Responsabilii cu protecția datelor

Responsabilii cu protecția datelor joacă un rol important în ceea ce privește asigurarea conformității cu RGPD în cadrul organizațiilor în care lucrează. În general, responsabilii cu protecția datelor care își desfășoară activitatea în UE dispun de cunoștințele și competențele necesare pentru a-și îndeplini sarcinile care le revin în temeiul RGPD, iar independența lor este respectată ([130]). Cu toate acestea, persistă o serie de provocări, printre care: (i) dificultăți legate de numirea unor responsabili cu protecția datelor cu expertiza necesară; (ii) lipsa unor standarde la nivelul UE pentru educație și formare; (iii) neintegrarea adecvată a responsabililor cu protecția datelor în procesele organizaționale; (iv) lipsa resurselor; (v) sarcini suplimentare în afara protecției datelor și (vi) vechime insuficientă ([131]). Comitetul a observat că este necesar ca autoritățile pentru protecția datelor să își intensifice activitățile de sensibilizare, precum și acțiunile de informare și de asigurare a respectării legii pentru a se asigura că responsabilii cu protecția datelor își pot îndeplini rolul care le revine în temeiul RGPD ([132]).

([126]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([127]) A se vedea poziția și constatările Consiliului, punctul 24; rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([128]) Articolul 30 alineatul (5) din RGPD.
([129]) În cazul în care organizația are mai puțin de 250 de angajați, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, nu este ocazională sau include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1) din RGPD, sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează la articolul 10 din RGPD.
([130]) Poziția și constatările Consiliului, punctul 26; Acțiunea coordonată privind asigurarea respectării legii 2023 a CEPD – Desemnarea și poziția responsabililor cu protecția datelor: https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf.
([131]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([132]) A se vedea recomandările din Acțiunea coordonată a CEPD privind asigurarea respectării legii.

6 RGPD CA PIATRĂ DE TEMELIE PENTRU POLITICA UE ÎN DOMENIUL DIGITAL

6.1 Politica în domeniul digital bazată pe RGPD

În raportul din 2020, Comisia s-a angajat să sprijine aplicarea consecventă a cadrului de protecție a datelor în ceea ce privește noile tehnologii, pentru a sprijini inovarea și evoluțiile tehnologice. Între timp, UE a adoptat o serie de inițiative, dintre care unele completează RGPD sau precizează modul în care acesta ar trebui aplicat în anumite domenii, pentru a urmări obiective specifice, astfel cum sunt prezentate mai jos.

- Regulamentul privind serviciile digitale ([133]), care urmărește să ofere un mediu online sigur persoanelor fizice și întreprinderilor, interzice platformelor online să prezinte reclame bazate pe crearea de profiluri utilizând „categorii speciale de date cu caracter personal”, astfel cum sunt definite în RGPD.
- Pentru ca piețele digitale să devină mai echitabile și mai deschise concurenței, Regulamentul privind piețele digitale ([134]) interzice operatorilor desemnați drept „controlori de acces” să „combine” și „să utilizeze încrucișat” datele cu caracter personal între serviciile lor de platformă esențiale și alte servicii, cu excepția cazului în care utilizatorul și-a dat consimțământul, astfel cum este definit în RGPD.
- Regulamentul privind inteligența artificială ([135]) specifică normele UE privind protecția datelor în anumite domenii în care este utilizată inteligența artificială, de exemplu sistemele de identificare biometrică la distanță, prelucrarea categoriilor speciale de date pentru a detecta prejudecățile și prelucrarea ulterioară a datelor cu caracter personal în spațiile de testare în materie de reglementare.
- Directiva privind lucrul pe platforme ([136]) completează RGPD în domeniul ocupării forței de muncă prin stabilirea unor norme privind sistemele automatizate de monitorizare și de luare a deciziilor utilizate de platformele digitale de muncă, în special a unor limitări privind prelucrarea datelor cu caracter personal, transparența, supravegherea umană și revizuirea și portabilitatea.
- Regulamentul privind publicitatea politică ([137]) interzice utilizarea categoriilor speciale de date cu caracter personal în publicitatea politică și impune o mai mare transparență în ceea ce privește tehnicile de vizare a unui public-țintă și de amplificare utilizate.
- Regulamentul privind identitatea digitală europeană permite crearea unui portofel european universal, fiabil și securizat pentru identitatea digitală. Acest lucru le va permite persoanelor fizice să facă dovada unor atribute personale, cum ar fi vârsta, permisele de conducere, diplomele și conturile bancare, având un control deplin asupra datelor lor cu caracter personal și fără partajarea inutilă de date.

([133]) Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale), JO L 277, 27.10.2022, p. 1.

([134]) Regulamentul (UE) 2022/1925 (Regulamentul privind piețele digitale), JO L 265, 12.10.2022, p. 1.

([135]) Regulamentul (UE) 2024/1689 (Regulamentul privind inteligența artificială), JO L, 2024/1689, 12.7.2024.

([136]) Lucrătorii pe platforme: Consiliul confirmă acordul cu privire la noi norme pentru îmbunătățirea condițiilor lor de muncă – Consilium (europa.eu).

([137]) Regulamentul (UE) 2024/900 privind transparența și vizarea unui public-țintă în publicitatea politică, JO L, 2024/900, 20.3.2024.

Propunerea de regulament privind viața privată și comunicațiile electronice ([138]) care să înlocuiască actuala Directivă asupra confidențialității și comunicațiilor electronice ([139]) și să completeze cadrul legislativ privind protecția vieții private și a datelor este în curs de negociere de mai mulți ani. Este necesar să se reflecteze asupra următoarelor etape ale acestei inițiative, inclusiv asupra relației sale cu RGPD.

Regulamentul privind Europa interoperabilă ([140]) urmărește să asigure interoperabilitatea serviciilor publice digitale în întreaga UE. Acesta sprijină cooperarea dintre autoritățile pentru protecția datelor, în special prin intermediul spațiilor de testare în materie de reglementare a interoperabilității.

Mai multe inițiative ale UE oferă un temei juridic pentru prelucrarea datelor cu caracter personal de către entități private în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor. Orice astfel de act legislativ trebuie să fie atent orientat pentru a reduce la minimum interferența cu dreptul la protecția datelor cu caracter personal și trebuie să fie proporțional cu scopul urmărit ([141]). Carta, RGPD și jurisprudența Curții de Justiție oferă un cadru în raport cu care ar trebui evaluate aceste inițiative. Pachetul propus privind combaterea spălării banilor ([142]) conține garanții substanțiale pentru protecția datelor cu caracter personal, fără a compromite obiectivul de atenuare a riscurilor de spălare a banilor și de finanțare a terorismului sau obiectivul de detectare eficace a tentativelor infracționale de a utiliza abuziv sistemul financiar al UE.

În acest context, Consiliul a subliniat că orice nouă act legislativ al UE care conține dispoziții privind prelucrarea datelor cu caracter personal ar trebui să fie în concordanță cu RGPD și cu jurisprudența Curții de Justiție.

6.2 Un cadru juridic pentru îmbunătățirea schimbului de date

Strategia privind datele urmărește să creeze o piață unică a datelor, în cadrul căreia datele să circule liber în interiorul UE și între sectoare, în beneficiul întreprinderilor, al cercetătorilor și al administrațiilor publice. Un obiectiv esențial al strategiei privind datele este crearea unor spații europene comune ale datelor, care să faciliteze punerea în comun, accesarea și partajarea datelor. În ceea ce privește datele cu caracter personal, RGPD oferă cadrul pentru toate inițiativele care urmăresc să consolideze libera circulație a datelor în UE – care este, la rândul său, un obiectiv al RGPD. În ceea ce privește datele cu caracter personal, nu se aduce atingere protecției prevăzute în RGPD.

Regulamentul privind guvernanța datelor ([143]) și Regulamentul privind datele ([144]) sunt piloni ai strategiei privind datele. Regulamentul privind guvernanța datelor prevede norme concrete în contextul reutilizării datelor din sectorul public care conțin date cu caracter personal, stabilește un cadru legislativ pentru serviciile de intermediere de date – inclusiv pentru serviciile de gestionare a informațiilor cu caracter personal (*personal information management services* – PIMS) sau pentru cloudurile de date cu caracter personal oferite pentru a capacita persoanele vizate atunci când își exercită drepturile în temeiul RGPD. Acesta stabilește, de asemenea, condițiile de utilizare a datelor în scopuri altruiste.

([138]) Propunere de regulament privind viața privată și comunicațiile electronice [COM(2017) 010 final].
([139]) Directiva 2002/58/CE (Directiva asupra confidențialității și comunicațiilor electronice), JO L 201, 31.7.2002, p. 37.
([140]) Regulamentul (UE) 2024/903 (Regulamentul privind Europa interoperabilă), JO L, 2024/903, 22.3.2024.
([141]) A se vedea poziția și constatările Consiliului, punctul 31 litera (f).
([142]) https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en.
([143]) Regulamentul (UE) 2022/868 (Regulamentul privind guvernanța datelor), JO L 152, 3.6.2022, p. 1.
([144]) Regulamentul (UE) 2023/2854 (Regulamentul privind datele), JO L, 2023/2854, 22.12.2023.

Regulamentul privind datele consolidează controlul persoanelor vizate asupra datelor pe care le generează prin utilizarea obiectelor inteligente pe care le dețin, le închiriază sau le iau în leasing, prin impunerea unor cerințe tehnice pentru accesul la date și portabilitatea acestora.

Spațiul european al datelor privind sănătatea (*European Health Data Space* – EHDS) ([145]) reflectă nevoile specifice identificate în sectorul datelor privind sănătatea, bazându-se totodată și pe RGPD. Acesta le permite persoanelor fizice să își acceseze cu ușurință datele privind sănătatea în format electronic și să le partajeze cu cadrele medicale, inclusiv din alte state membre, îmbunătățind astfel furnizarea de asistență medicală și sporind controlul pacienților asupra datelor lor. De asemenea, el instituie un cadru juridic comun pentru reutilizarea datelor privind sănătatea în scopuri precum cercetarea, inovarea și sănătatea publică, pe baza unei autorizații emise de un organism de acces la datele privind sănătatea. Pentru a asigura protecția datelor cu caracter personal, EHDS va oferi un cadru fiabil pentru accesul sigur la datele privind sănătatea și pentru prelucrarea acestora. Comisia continuă să sprijine activitatea de dezvoltare a unor spații europene comune ale datelor în 14 sectoare prin punerea în aplicare a noului cadru legislativ și prin finanțarea inițiativelor sectoriale.

6.3 Guvernanța noilor norme în domeniul digital

Elaborarea reglementărilor în domeniul digital atrage atenția asupra necesității unei cooperări strânse în toate domeniile de reglementare ([146]). O astfel de cooperare este cu atât mai necesară cu cât aspectele legate de protecția datelor se intersectează din ce în ce mai mult cu domenii precum dreptul concurenței, dreptul consumatorilor, normele privind piețele digitale, reglementarea comunicațiilor electronice și securitatea cibernetică. Acest lucru este valabil, de exemplu, atunci când se evaluează compatibilitatea modelelor „*pay or OK*” cu dreptul Uniunii.

În unele cazuri, autoritățile pentru protecția datelor au sarcina de a asigura respectarea dispozițiilor specifice ale noii legislații în domeniul digital a UE ([147]). Noile reglementări în domeniul digital creează, de asemenea, structuri personalizate care reunesc autoritățile de reglementare competente pentru a asigura o aplicare coerentă, cum ar fi Grupul la nivel înalt pentru Regulamentul privind piețele digitale, Comitetul european pentru inovare în domeniul datelor (instituit în temeiul Regulamentului privind guvernanța datelor) și Comitetul european pentru servicii digitale (instituit în temeiul Regulamentului privind serviciile digitale). Directiva NIS 2 ([148]) stabilește norme mai detaliate referitoare la cooperarea dintre autoritățile de reglementare și autoritățile pentru protecția datelor privind gestionarea incidentelor de securitate care constituie încălcări ale securității datelor cu caracter personal.

În afara acestor structuri formale, autoritățile pentru protecția datelor iau măsuri pentru a se asigura că acțiunile lor sunt complementare și coerente cu alte domenii de reglementare. În iulie 2020, autoritățile pentru protecția consumatorilor și a datelor au înființat un „grup de voluntari” pentru a stabili cele mai bune practici și pentru a face schimb de experiență în materie de asigurare a respectării legii. Autoritățile pentru protecția datelor continuă să participe la ateliere comune cu Rețeaua de cooperare pentru protecția consumatorilor. În

([145]) https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_RO.html.

([146]) A se vedea poziția și constatările Consiliului, punctele 40-41; Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.

([147]) A se vedea, de exemplu, articolul 37 alineatul (3) din Regulamentul privind datele.

([148]) Directiva (UE) 2022/2555 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80).

2023, comitetul a înființat un grup operativ privind interacțiunea dintre protecția datelor, concurență și protecția consumatorilor.

Deși aceste evoluții sunt pozitive, este nevoie de mijloace de cooperare mai structurate și mai eficiente, în special pentru a aborda situațiile care afectează un număr mare de persoane fizice din UE și implică mai multe autorități de reglementare ([149]). Orice astfel de structură ar trebui să se asigure că autoritățile rămân în permanență responsabile pentru toate chestiunile legate de respectarea normelor în domeniile lor de competență. Statele membre ar trebui, de asemenea, să depună eforturi pentru a se asigura că are loc o cooperare adecvată la nivel național ([150]).

7 TRANSFERURILE INTERNAȚIONALE ȘI COOPERAREA GLOBALĂ

7.1 Setul de instrumente al RGPD pentru transferuri

Fluxurile de date au devenit parte integrantă a transformării digitale a societății și a globalizării economiei. Mai mult ca oricând, respectarea vieții private este o condiție pentru fluxuri comerciale stabile, sigure și competitive, precum și un factor favorizant pentru numeroase forme de cooperare internațională. Setul de instrumente pentru transferuri prevăzut în capitolul V din RGPD oferă o varietate de instrumente pentru a aborda diferite scenarii de transfer, asigurându-se totodată că datele continuă să beneficieze de un nivel ridicat de protecție atunci când părăsesc UE.

De la raportul din 2020, cerințele privind transferurile de date prevăzute în legislația UE privind protecția datelor au fost clarificate suplimentar, iar setul de instrumente pentru transferuri a continuat să evolueze. O clarificare importantă se referă la noțiunea de „transfer internațional”, care a fost definită de comitet ([151]) ca incluzând orice divulgare de date cu caracter personal de către un operator sau o persoană împuternicită de operator a cărui (cărei) prelucrare face obiectul RGPD către un alt operator sau o altă persoană împuternicită de operator dintr-o țară terță, indiferent dacă prelucrarea de către acesta (aceasta) din urmă face sau nu obiectul RGPD ([152]). Aceste orientări ale comitetului au fost deosebit de importante pentru a oferi securitate juridică operatorilor și persoanelor împuternicite de operatori din UE cu privire la scenariile în care este necesar un instrument de transfer în temeiul capitolului V din RGPD.

De asemenea, Curtea de Justiție a furnizat clarificări suplimentare în hotărârea Schrems II ([153]) cu privire la protecția care trebuie asigurată prin diferite instrumente de transfer pentru a se asigura că nivelul de protecție garantat de RGPD nu este subminat ([154]). În particular, aceste instrumente trebuie să garanteze că persoanele fizice ale căror date sunt transferate în afara UE beneficiază de un nivel de protecție în esență echivalent cu cel garantat în UE ([155]). Este responsabilitatea exportatorului de date din UE să evalueze dacă acest lucru este valabil, ținând seama de circumstanțele specifice ale transferurilor sale ([156]).

([149]) A se vedea poziția și constatările Consiliului, punctele 18 și 40-41 și rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.

([150]) Germania a instituit un „cluster digital”, care include autorități de reglementare din diferite domenii, cu scopul de a-și extinde cooperarea cu privire la toate aspectele digitalizării și de a face schimb de cunoștințe și de bune practici: https://www.dataguidance.com/news/germany-bsi-announces-formation-digital-cluster-bonn.

([151]) Orientările CEPD 05/2021.

([152]) Secțiunea 2 din Orientările CEPD 05/2021.

([153]) Cauza C-311/18, ECLI:EU:C:2020:559 (Schrems II).

([154]) Hotărârea Schrems II, punctul 93.

([155]) Hotărârea Schrems II, punctele 96 și 105.

([156]) Hotărârea Schrems II, punctul 131.

Pentru a evalua nivelul de protecție, exportatorii de date trebuie să ia în considerare atât garanțiile privind protecția datelor prevăzute în instrumentul de transfer (de exemplu un contract) încheiat cu un importator de date din afara UE, cât și aspectele relevante ale sistemului juridic al țării în care este situat importatorul de date, în special în ceea ce privește posibilul acces la date al autorităților publice din țara respectivă ([157]). Acestea din urmă trebuie evaluate în lumina criteriilor de evaluare a caracterului adecvat al nivelului de protecție prevăzute la articolul 45 din RGPD. De asemenea, Curtea a detaliat aceste criterii, în special în ceea ce privește normele privind accesul autorităților publice la datele cu caracter personal în scopul asigurării respectării legii și al securității naționale.

Această interpretare s-a reflectat și în orientările comitetului, care și-a actualizat „criteriile de referință privind caracterul adecvat al nivelului de protecție" ([158]) (care au oferit orientări cu privire la elementele pe care Comisia trebuie să le ia în considerare atunci când efectuează o evaluare a caracterului adecvat al nivelului de protecție). De asemenea, comitetul a adoptat noi orientări care oferă clarificări suplimentare cu privire la: (i) elementele care trebuie luate în considerare de exportatorii individuali de date atunci când evaluează nivelul de protecție; (ii) o prezentare generală a surselor potențiale care pot fi utilizate și (iii) exemple de posibile măsuri suplimentare (de exemplu garanții contractuale și tehnice) ([159]). Orientările subliniază în mod special că fiecare evaluare efectuată de exportatorii de date este unică și că, prin urmare, aceștia trebuie să țină seama de caracteristicile specifice ale fiecărui transfer, care pot varia în funcție de scopul transferului de date, de tipurile de entități implicate, de sectorul în care are loc transferul, de categoriile de date cu caracter personal transferate etc. ([160]).

Ținând seama de aceste clarificări diferite cu privire la cerințele pentru transferurile internaționale de date, în ultimii ani s-au luat măsuri semnificative pentru a dezvolta și a operaționaliza în continuare setul de instrumente pentru transferuri al RGPD.

7.1.1 Deciziile privind caracterul adecvat al nivelului de protecție

Astfel cum se reflectă și în feedbackul primit de la părțile interesate, deciziile privind caracterul adecvat al nivelului de protecție continuă să joace un rol esențial în setul de instrumente pentru transferuri al RGPD ([161]), oferind o soluție simplă și cuprinzătoare pentru transferurile de date, fără a fi necesar ca exportatorul de date să ofere garanții suplimentare sau să obțină vreo autorizație. Permițând libera circulație a datelor cu caracter personal, aceste decizii au deschis canale comerciale pentru operatorii din UE, inclusiv prin completarea și amplificarea beneficiilor acordurilor comerciale și prin facilitarea colaborării cu partenerii străini într-o gamă largă de domenii, de la cooperarea în materie de reglementare până la cercetare.

De la raportul din 2020, numărul țărilor care au adoptat legi moderne în materie de protecție a datelor – care prevăd, printre altele, principii esențiale de protecție a datelor, drepturi individuale și aplicarea efectivă de către autoritățile de reglementare independente – a continuat să crească. Această tendință ([162]) a permis, de asemenea, Comisiei să își intensifice activitatea privind caracterul adecvat al nivelului de protecție. Aceasta include adoptarea unei decizii privind caracterul adecvat al nivelului de protecție pentru Regatul

([157]) Hotărârea Schrems II, punctul 105.
([158]) Recomandările CEPD 02/2020 și Criteriile de referință privind caracterul adecvat al nivelului de protecție, WP 254 rev. 01.
([159]) Recomandările CEPD 01/2020, completate de Recomandările 02/2020.
([160]) A se vedea, de exemplu, punctele 8-13 și 32-33 din Recomandările CEPD 01/2020.
([161]) A se vedea, de exemplu, contribuția comitetului, paginile 7-8; poziția și constatările Consiliului, punctul 36; Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([162]) Comunicarea Comisiei intitulată „Schimbul de date cu caracter personal și protecția acestora într-o lume globalizată", 10.1.2017 [COM(2017) 7 final].

Unit ([163]), care este esențială pentru a asigura buna funcționare a diferitelor acorduri încheiate cu Regatul Unit în urma Brexitului. Pentru a se asigura că rămâne adaptată exigențelor viitorului, decizia privind caracterul adecvat al nivelului de protecție include o „clauză de caducitate” care urmează să expire în 2025, după care poate fi reînnoită dacă nivelul de protecție continuă să fie adecvat. De asemenea, Comisia a adoptat o decizie privind caracterul adecvat al nivelului de protecție pentru Republica Coreea ([164]), care completează Acordul de liber schimb UE-Coreea privind fluxurile de date cu caracter personal și facilitează cooperarea în materie de reglementare. O primă revizuire a deciziei privind caracterul adecvat al nivelului de protecție este planificată spre sfârșitul anului 2024.

În plus, în urma invalidării deciziei privind caracterul adecvat al nivelului de protecție pentru Scutului de confidențialitate UE-SUA, Comisia a inițiat discuții cu Guvernul Statelor Unite (SUA) pentru a elabora un acord succesor în conformitate cu cerințele clarificate de Curte ([165]). Președintele SUA a adoptat un nou ordin executiv privind „Consolidarea garanțiilor pentru activitățile Statelor Unite de colectare a informațiilor de tip SIGINT”, care a introdus noi garanții obligatorii și executorii pentru a se asigura că datele pot fi accesate în scopuri de securitate națională numai în măsura necesară și proporțională și că europenii au la dispoziție căi de atac eficace. Pe această bază, Comisia a adoptat decizia referitoare la caracterul adecvat al nivelului de protecție pentru Cadrul UE-SUA privind confidențialitatea datelor (CCD) ([166]), care permite circulația liberă a datelor cu caracter personal din UE către societățile din SUA care aderă la CCD. Întrucât garanțiile instituite de Guvernul SUA în domeniul securității naționale se aplică tuturor transferurilor de date către societăți din SUA, indiferent de mecanismul de transfer prevăzut în RGPD care este utilizat, utilizarea altor instrumente, cum ar fi clauzele contractuale standard și regulile corporatiste obligatorii, a fost facilitată în mod semnificativ. O primă revizuire a funcționării CCD va avea loc în vara anului 2024 pentru a verifica dacă toate elementele relevante au fost puse în aplicare pe deplin în cadrul juridic al SUA și dacă funcționează în mod eficace în practică.

În prezent, sunt în curs negocieri privind caracterul adecvat al nivelului de protecție cu Brazilia și Kenya, precum și, pentru prima dată, cu mai multe organizații internaționale (de exemplu discuțiile privind caracterul adecvat al nivelului de protecție se află într-un stadiu avansat cu Organizația Europeană de Brevete) ([167]). În concordanță și cu solicitările diferitelor părți interesate ([168]), Comisia s-a angajat activ în discuții preliminare cu țări din diferite regiuni ale lumii.

Comisia monitorizează în permanență și evoluțiile din țările care beneficiază deja de constatările privind caracterul adecvat al nivelului de protecție și revizuiește periodic deciziile existente, în conformitate cu obligațiile care îi revin în temeiul RGPD ([169]). În aprilie 2023, Comisia a adoptat raportul privind prima revizuire periodică a deciziei privind

([163]) Decizia de punere în aplicare (UE) 2021/1772 a Comisiei, JO L 360, 11.10.2021, p. 1.
([164]) Decizia de punere în aplicare (UE) 2022/254 a Comisiei, JO L 44, 24.2.2022, p. 1.
([165]) https://commission.europa.eu/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-2020-08-10_en.
([166]) Decizia de punere în aplicare (UE) 2023/1795 a Comisiei, JO L 231, 20.9.2023, p. 118.
([167]) Organizația Europeană de Brevete este o organizație interguvernamentală înființată pe baza Convenției brevetului european. Principala sa sarcină este acordarea de brevete europene. În acest context, Comisia cooperează strâns cu societățile și cu autoritățile publice din statele membre ale UE, precum și cu diferite instituții și organisme ale UE.
([168]) Contribuția comitetului, paginile 7-8.
([169]) Articolul 45 alineatele (4) și (5) din RGPD. A se vedea și hotărârea Schrems I, punctul 76.

caracterul adecvat al nivelului de protecție pentru Japonia ([170]), care a concluzionat că Japonia continuă să asigure un nivel adecvat de protecție ([171]). Revizuirea a demonstrat că cadrele de protecție a datelor din UE și Japonia au continuat să conveargă de la adoptarea deciziilor reciproce privind caracterul adecvat al nivelului de protecție.

În plus, în conformitate cu articolul 97 din RGPD, a fost inițiată prima revizuire a celor 11 decizii privind caracterul adecvat al nivelului de protecție ([172]) adoptate în temeiul cadrului anterior al UE privind protecția datelor (Directiva privind protecția datelor), în cadrul evaluării din 2020 a aplicării și funcționării RGPD. Concluzia acestui aspect al revizuirii a fost amânată, în special pentru a se ține seama de hotărârea Curții de Justiție în cauza Schrems II și de interpretarea ulterioară de către comitet. Clarificările sus-menționate ale Curții cu privire la elementele-cheie ale standardului privind caracterul adecvat al nivelului de protecție au condus la schimburi detaliate cu țările și teritoriile în cauză cu privire la aspecte relevante ale cadrului lor juridic, precum și la mecanisme de supraveghere și de asigurare a respectării legii.

La 15 ianuarie 2024, Comisia și-a publicat raportul privind aceste 11 decizii, împreună cu rapoarte de țară detaliate care descriu evoluțiile din fiecare țară și teritoriu de la adoptarea deciziilor privind caracterul adecvat al nivelului de protecție, precum și normele care se aplică accesului autorităților publice la date, în special în scopul asigurării respectării legii și al securității naționale ([173]). Raportul concluzionează că toate cele 11 țări și teritorii continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE. Această concluzie reflectă faptul că toate țările și teritoriile în cauză și-au modernizat și consolidat, în moduri diferite, cadrul juridic privind protecția vieții private. În plus, pentru a aborda diferențele relevante în ceea ce privește nivelul de protecție, au fost negociate și convenite cu unele dintre țările și teritoriile în cauză garanții suplimentare pentru datele cu caracter personal transferate din Europa, atunci când acestea au fost necesare pentru a se asigura continuitatea deciziei privind caracterul adecvat.

Aceste revizuiri arată, de asemenea, că deciziile privind caracterul adecvat al nivelului de protecție, în loc să fie un „punct de destinație”, au pus bazele unei cooperări mai strânse și ale unei convergențe mai mari în materie de reglementare între UE și acești parteneri care împărtășesc aceeași viziune. De exemplu, raportul privind prima revizuire a deciziei privind caracterul adecvat al nivelului de protecție pentru Japonia recunoaște că consolidarea în continuare a cadrului japonez de protecție a datelor poate deschide calea pentru extinderea deciziei privind caracterul adecvat al nivelului de protecție dincolo de schimburile comerciale, pentru a acoperi transferurile excluse în prezent din domeniul său de aplicare, de exemplu în domeniul cooperării în materie de reglementare și al cercetării. Sunt în derulare discuții pentru explorarea unei astfel de posibile prelungiri. În general, deciziile privind caracterul adecvat al nivelului de protecție au devenit o componentă strategică a relației generale a UE cu acești parteneri străini și sunt recunoscute ca un factor major pentru aprofundarea cooperării într-o gamă largă de domenii.

([170]) Decizia de punere în aplicare (UE) 2019/419 a Comisiei, JO L 76, 19.3.2019, p. 1. A se vedea și https://ec.europa.eu/commission/presscorner/detail/ro/IP_19_421. Această decizie a constituit prima decizie privind caracterul adecvat al nivelului de protecție adoptată în temeiul RGPD și primul acord reciproc privind caracterul adecvat al nivelului de protecție.

([171]) Raportul Comisiei referitor la prima revizuire a funcționării deciziei privind caracterul adecvat al nivelului de protecție pentru Japonia, 3.4.2023, COM(2023) 275 final [și SWD(2023) 75 final].

([172]) Andorra, Argentina, Canada (pentru operatorii comerciali), Insulele Feroe, Guernsey, Insula Man, Israel, Jersey, Noua Zeelandă, Elveția și Uruguay.

([173]) Raportul Comisiei privind prima revizuire a funcționării deciziilor privind caracterul adecvat al nivelului de protecție adoptate în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE, 15.1.2024, COM(2024) 7 final [și SWD(2024) 3 final].

Pe lângă faptul că oferă o bază solidă pentru o cooperare bilaterală sporită, rețeaua tot mai mare de țări și teritorii pentru care UE a adoptat decizii privind caracterul adecvat al nivelului de protecție oferă noi oportunități de a maximiza beneficiile fluxurilor de date sigure și libere și de a coopera mai strâns cu parteneri care împărtășesc aceeași viziune în ceea ce privește asigurarea respectării normelor de protecție a datelor. Prin urmare, în martie 2024, Comisia a găzduit prima reuniune la nivel înalt privind fluxurile de date sigure, care a reunit miniștri responsabili și șefi ai autorităților pentru protecția datelor din 15 țări și teritorii pentru care UE a adoptat decizii privind caracterul adecvat al nivelului de protecție, precum și președintele Comitetului european pentru protecția datelor ([174]). Cu ocazia reuniunii au fost identificate mai multe puncte de acțiune concrete cu privire la care lucrările subsecvente sunt în desfășurare în cadrul acestui grup.

Un aspect mai general este faptul că, datorită „efectului de rețea", deciziile privind caracterul adecvat al nivelului de protecție adoptate de Comisia Europeană sunt din ce în ce mai relevante și în afara UE, deoarece permit libera circulație a datelor nu doar în cele 30 de economii ale SEE, ci și în multe alte jurisdicții din întreaga lume care recunosc țările pentru care există o decizie a UE privind caracterul adecvat al nivelului de protecție ca „destinații sigure" în temeiul propriilor norme de protecție a datelor ([175]).

7.1.2 Instrumente care prevăd garanții adecvate

De la raportul din 2020 și până în prezent, au fost elaborate instrumente suplimentare care prevăd garanții adecvate și au fost emise orientări practice pentru a facilita utilizarea acestora.

Astfel cum s-a anunțat în raportul din 2020, Comisia a adoptat clauze contractuale standard (CCS) modernizate ([176]), elaborate pe scară largă pe baza feedbackului primit de la diferite părți interesate ([177]). Noile CCS au înlocuit cele trei seturi de CCS care au fost adoptate în temeiul Directivei privind protecția datelor. Printre principalele inovații se numără următoarele: (i) garanții actualizate în concordanță cu RGPD; (ii) o abordare modulară care oferă un singur punct de intrare care acoperă o gamă largă de scenarii de transfer; (iii) o flexibilitate sporită pentru utilizarea CCS de către mai multe părți și (iv) un set practic de instrumente pentru conformarea cu hotărârea Schrems II.

CCS modernizate au fost salutate de părțile interesate, iar feedbackul primit confirmă faptul că CCS rămân de departe cel mai utilizat instrument pentru transferurile efectuate de exportatorii de date din UE ([178]). Pentru a sprijini exportatorii de date în eforturile lor de asigurare a conformității, Comisia a elaborat o listă de întrebări și răspunsuri care oferă orientări suplimentare cu privire la utilizarea clauzelor ([179]), care va fi actualizată din nou dacă apar noi întrebări, inclusiv în lumina feedbackului suplimentar primit în cadrul acestei evaluări.

Numeroși exportatori de date se confruntă cu dificultăți în ceea ce privește efectuarea „evaluărilor privind impactul transferului" impuse de hotărârea Schrems II, referindu-se în special la complexitatea lor, precum și la costurile și la timpul necesar pentru efectuarea

([174]) https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307#11.
([175]) De exemplu Argentina, Columbia, Israel, Maroc, Elveția și Uruguay.
([176]) Decizia de punere în aplicare (UE) 2021/914 a Comisiei, JO L 199, 7.6.2021, p. 31.
([177]) Acesta a inclus, de exemplu, Avizul comun 2/2021 al CEPD-AEPD, ca parte a procedurii de adoptare a CCS.
([178]) Poziția și constatările Consiliului, punctul 37, contribuția comitetului, pagina 9, rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.
([179]) https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en.

acestora ([180]). Deși apreciază orientările comitetului și CCS, aceștia solicită orientări suplimentare (de exemplu cu privire la responsabilitățile părților implicate și la nivelul de detaliere necesar în evaluările privind impactul transferului) și instrumente suplimentare care să îi ajute la efectuarea unor astfel de evaluări (de exemplu modele, evaluări de țară generale, cataloage de risc). Deși părțile interesate au furnizat în principal un astfel de feedback cu privire la CCS, aceleași evaluări sunt necesare și pentru alte instrumente de transfer (cum ar fi regulile corporatiste obligatorii). Prin urmare, este important ca comitetul – pe baza experienței dobândite în ultimii ani în ceea ce privește aplicarea cerințelor din hotărârea Schrems II, inclusiv ca parte a activităților de asigurare a respectării legislației ale autorităților naționale de protecție a datelor – să analizeze modalități/instrumente pentru a sprijini în continuare exportatorii de date în eforturile lor de asigurare a conformității în acest context.

Pentru a completa CCS existente, Comisia elaborează în prezent seturi suplimentare de clauze pentru a oferi exportatorilor de date din UE un pachet cuprinzător și coerent. Printre acestea se vor număra CCS în temeiul Regulamentului (UE) 2018/1725 pentru transferurile de date ale instituțiilor și organelor UE către operatori comerciali din țări terțe ([181]) și CCS pentru transferurile de date către importatorii de date din țări terțe ale căror operațiuni de prelucrare fac în mod direct obiectul RGPD. Acestea din urmă răspund solicitării părților interesate de a acoperi în mod specific scenariile în care importatorul de date intră în domeniul de aplicare teritorial al RGPD [de exemplu deoarece prelucrarea în cauză vizează piața UE în conformitate cu articolul 3 alineatul (2) din RGPD] ([182]). Astfel cum a clarificat comitetul, și în acest caz este necesar un instrument de transfer în temeiul capitolului V din RGPD, din cauza riscurilor sporite pentru datele cu caracter personal prelucrate în afara UE, de exemplu din cauza unor posibile legislații naționale contradictorii sau a accesului disproporționat al autorităților publice din țara terță ([183]). Noile CCS elaborate de Comisie vor aborda în mod special acest scenariu și vor ține seama pe deplin de cerințele care se aplică deja în mod direct operatorilor și persoanelor împuternicite de operatori în temeiul RGPD ([184]).

După cum au recunoscut și diferitele tipuri de părți interesate ([185]), clauzele standard joacă un rol din ce în ce mai important în facilitarea fluxurilor de date în întreaga lume. Mai multe jurisdicții au aprobat CCS ale UE ca mecanism de transfer în temeiul propriilor legi privind protecția datelor, cu adaptări formale reduse ale ordinii lor juridice interne ([186]). O serie de alte țări au adoptat propriile clauze standard care au caracteristici comune importante cu CCS ale UE ([187]). Un exemplu deosebit de relevant este crearea de clauze standard de către alte organizații sau rețele internaționale/regionale, cum ar fi Comitetul consultativ al Consiliului Europei din cadrul Convenției 108, Rețeaua ibero-americană

([180]) A se vedea, de exemplu, rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.

([181]) În conformitate cu articolul 48 alineatul (2) litera (b) din Regulamentul (UE) 2018/1725.

([182]) Poziția și constatările Consiliului, punctul 37, contribuția comitetului, pagina 9, rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.

[183]Orientările CEPD 05/2021, pagina 3.

([184]) Astfel cum se prevede și în Orientările CEPD 05/2021, secțiunea 4.

([185]) Contribuția comitetului, pagina 9, rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.

([186]) De exemplu, Regatul Unit (https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) și Elveția (https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html).

([187]) De exemplu, Noua Zeelandă (https://privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/) și Argentina (https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm).

pentru protecția datelor și Asociația Națiunilor din Asia de Sud-Est (ASEAN) ([188]). Acest lucru deschide noi oportunități de facilitare a fluxurilor de date între diferite regiuni ale lumii pe baza unor clauze standard. Un exemplu concret este Ghidul UE-ASEAN privind CCS ale UE și clauzele standard ale ASEAN care, pe baza contribuțiilor din partea societăților, le sprijină în eforturile lor de asigurare a conformității conform ambelor seturi de clauze ([189]).

Pe lângă CCS, regulile corporatiste obligatorii (RCO) continuă să fie utilizate pe scară largă pentru fluxurile de date între membrii grupurilor corporative sau între întreprinderile implicate într-o activitate economică comună. Întrucât se aplică RGPD, comitetul a adoptat 80 de avize pozitive cu privire la deciziile naționale de aprobare a RCO ([190]). De asemenea, comitetul a emis orientări privind elementele care trebuie incluse în RCO pentru operatori (și informațiile care trebuie furnizate în cadrul aplicării RCO), care au fost actualizate pentru a reflecta cerințele RGPD și hotărârea Schrems II ([191]). Sunt, de asemenea, în curs de elaborare orientări actualizate privind RCO pentru persoanele împuternicite de operatori ([192]). Deoarece RCO vizează instituirea unor politici/programe obligatorii de protecție a datelor în întreprinderi, multe părți interesate le consideră un instrument de asigurare a conformității deosebit de util și un instrument de transfer fiabil ([193]). În același timp, părțile interesate continuă să raporteze că durata și complexitatea procesului de aprobare de către autoritățile naționale pentru protecția datelor împiedică adoptarea pe scară mai largă a RCO. Prin urmare, este important ca autoritățile să continue să lucreze la simplificarea și scurtarea procesului de aprobare.

De la raportul din 2020 și până în prezent s-au luat, de asemenea, măsuri pentru a facilita utilizarea certificării și a codurilor de conduită ca instrumente pentru transferuri, de exemplu prin adoptarea de către comitet a unor orientări specifice privind ambele instrumente ([194]). În același timp, părțile interesate raportează aceleași aspecte ca și cele menționate mai sus în materie de calendar și complexitate a procesului de aprobare în ceea ce privește certificarea și codurile de conduită ca instrumente de responsabilizare.

În fine, RGPD prevede, de asemenea, instrumente specifice – acorduri internaționale și acorduri administrative aprobate de autoritățile de protecție a datelor – care urmează să fie utilizate de autoritățile publice pentru a transfera date cu caracter personal omologilor lor din țări terțe sau organizațiilor internaționale. Comitetul a adoptat orientări privind garanțiile care ar trebui incluse în astfel de instrumente ([195]), care pot sprijini negocierea unor astfel de acorduri și înțelegeri.

7.1.3 Asigurarea complementarității cu alte politici

Întrucât fluxurile de date au devenit esențiale pentru un număr atât de mare de activități, este esențial să se asigure că politicile de protecție a datelor și celelalte politici se completează reciproc. Includerea garanțiilor privind protecția datelor în instrumentele

([188]) A se vedea https://rm.coe.int/t-pd-2022-1rev10-en-final/1680abc6b4; https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf și https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.

([189]) https://commission.europa.eu/document/download/df5cd5a0-7387-4a2a-8058-8d2ccfec3062_en?filename=%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf.

([190]) Contribuția comitetului, pagina 9.

([191]) Recomandările CEPD 1/2022.

([192]) Contribuția comitetului, pagina 9.

([193]) Rezumatul feedbackului primit de la Grupul multipartit de experți privind RGPD.

([194]) Orientările CEPD 07/2022 și 04/2021.

([195]) Orientările CEPD 2/2020.

internaționale nu este doar o condiție prealabilă pentru fluxurile de date, ci și un factor important pentru o cooperare stabilă și fiabilă.

De exemplu, acordurile internaționale care prevăd garanțiile necesare în materie de protecție a datelor, inclusiv prin asigurarea continuității protecției din partea unei autorități solicitante, sunt esențiale pentru a asigura curtoazia și a facilita accesul transfrontalier al autorităților de aplicare a legii la probele electronice deținute de societăți și, astfel, pentru o combatere mai eficace a criminalității. Această abordare se reflectă în cel de Al doilea protocol adițional la Convenția privind criminalitatea informatică ([196]), care consolidează normele existente pentru obținerea accesului transfrontalier la probele electronice în cadrul investigațiilor penale, asigurând totodată garanții adecvate în materie de protecție a datelor. Între timp, protocolul a fost semnat de mai multe state membre ale UE. În mod similar, între UE și SUA avansează negocierile bilaterale cu privire la un acord privind accesul transfrontalier la probele electronice pentru cooperarea în materie penală ([197]).

Schimbul de date din registrul cu numele pasagerilor (PNR) este un alt domeniu al politicii de securitate a UE care a beneficiat de dezvoltarea unor garanții solide în materie de protecție a datelor. În 2023, UE și Canada și-au încheiat negocierile cu privire la un nou acord privind PNR, în concordanță cu cerințele stabilite de Curtea de Justiție în Avizul 1/15 ([198]). Garanții similare au fost introduse în capitolul privind PNR din Acordul privind comerțul și cooperarea dintre UE și Regatul Unit. Includerea protecției sporite a vieții private în aceste acorduri, care pot servi drept model pentru acordurile viitoare cu alți parteneri, oferă securitate juridică transportatorilor aerieni, asigurând totodată stabilitatea schimburilor importante de informații pentru combaterea terorismului și a altor infracțiuni transnaționale grave.

Comisia este, de asemenea, un susținător al unor dispoziții ferme pentru protejarea vieții private și pentru stimularea comerțului digital în cadrul Organizației Mondiale a Comerțului în contextul negocierilor aflate în derulare cu privire la inițiativa referitoare la declarația comună privind comerțul electronic. Dispoziții similare privind combaterea obstacolelor nejustificate din calea comerțului digital, protejând totodată spațiul de politică necesar al părților în domeniul protecției datelor, au fost incluse în mod consecvent în acordurile de liber schimb încheiate de UE în urma intrării în vigoare a RGPD, în special în Acordul comercial și de cooperare UE-Regatul Unit și în acordurile cu Chile, Japonia și Noua Zeelandă. Dispozițiile privind confidențialitatea și fluxurile de date sunt, de asemenea, discutate în cadrul negocierilor comerciale în domeniul digital aflate în derulare cu Singapore și Coreea de Sud.

7.2 Cooperarea internațională în domeniul protecției datelor

7.2.1 Dimensiunea bilaterală

Comisia a continuat să se angajeze într-un dialog cu țările și organizațiile internaționale cu privire la dezvoltarea, reforma și punerea în aplicare a normelor privind viața privată, inclusiv prin prezentarea de contribuții la consultări publice privind proiectele legislative sau măsurile de reglementare în domeniul vieții private ([199]), prin depunerea de mărturii în

([196]) Al doilea protocol adițional la Convenția privind criminalitatea informatică referitor la cooperarea consolidată și divulgarea probelor electronice (CETS nr. 224).

([197]) https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en.

([198]) Propunerea Comisiei de decizie a Consiliului privind semnarea, în numele Uniunii Europene, a unui acord între Canada și Uniunea Europeană referitor la transferul și prelucrarea datelor din registrul cu numele pasagerilor (PNR) [COM(2024) 94 final].

([199]) Aceasta a vizat consultările organizate, de exemplu, de Australia, China, Rwanda, Argentina, Brazilia, Etiopia, Indonezia, Peru, Malaysia și Thailanda.

fața organismelor parlamentare competente ([200]) și prin participarea la reuniuni specifice cu reprezentanți ai guvernului, cu delegații parlamentare și cu autorități de reglementare din numeroase regiuni ale lumii ([201]). O serie de astfel de activități au fost desfășurate prin intermediul proiectului „Consolidarea protecției datelor și a fluxurilor de date”, finanțat de UE, care sprijină țările care intenționează să dezvolte cadre moderne de protecție a datelor sau să consolideze capacitatea autorităților lor de reglementare, prin formare, schimb de cunoștințe, consolidarea capacităților și schimb de bune practici. Comisia a contribuit și la alte inițiative, cum ar fi Alianța digitală UE-CELAC.

Protecția datelor va continua să joace un rol esențial și în activitatea Comisiei legată de extindere. Legislația UE privind protecția datelor este o componentă importantă a efortului global al țărilor implicate în procesul de aderare de a-și alinia cadrele juridice la cele ale UE (în special deoarece prelucrarea și schimbul de date cu caracter personal se află în centrul unui număr atât de mare de politici). În plus, independența și buna funcționare a unei autorități pentru protecția datelor reprezintă un element esențial al sistemului global de control și echilibru și al statului de drept și vor deveni din ce în ce mai importante pe măsură ce UE integrează treptat țările implicate în procesul de aderare pe piața unică (astfel cum se prevede în inițiative precum planul de creștere pentru Balcanii de Vest).

Un aspect din ce în ce mai important al dialogului purtat de UE cu țările terțe se concentrează asupra schimburilor dintre autoritățile de reglementare. Astfel cum s-a anunțat în raportul din 2020, Comisia a creat o „academie de protecție a datelor”, pentru a încuraja schimburile dintre autoritățile de protecție a datelor din UE și din țările terțe și pentru a contribui astfel la consolidarea capacităților și la îmbunătățirea cooperării „pe teren”. Academia oferă cursuri de formare personalizate la cererea autorităților din țări terțe și reunește expertiza reprezentanților comunității de aplicare a legii, ai mediului academic, ai sectorului privat și ai instituțiilor europene. Valoarea adăugată a cursurilor de formare constă în adaptarea diferitelor componente la interesele și nevoile autorității solicitante. În plus, aceste cursuri de formare permit autorităților pentru protecția datelor din UE și din țările terțe să stabilească contacte, să facă schimb de cunoștințe, să facă schimb de experiență și de bune practici și să identifice domenii potențiale de cooperare. Până în prezent, Academia a oferit cursuri de formare autorităților pentru protecția datelor din Indonezia, Brazilia, Kenya, Nigeria și Rwanda și pregătește în prezent cursuri de formare pentru alte câteva țări.

Pe lângă importanța menținerii unui dialog între autoritățile de reglementare, există o nevoie din ce în ce mai mare, astfel cum se recunoaște și în feedbackul primit din partea Consiliului și a comitetului ([202]), de a dezvolta instrumente juridice adecvate pentru forme mai strânse de cooperare și asistență reciprocă, inclusiv prin permiterea schimbului necesar de informații în contextul investigațiilor. Într-adevăr, întrucât încălcările vieții private produc din ce în ce mai multe efecte la nivel transfrontalier, acestea pot fi adesea investigate și abordate în mod eficace numai prin cooperarea dintre autoritățile de reglementare din UE și din afara UE. Prin urmare, Comisia va solicita autorizarea de a deschide negocieri pentru a încheia acorduri de cooperare în materie de asigurare a respectării legislației cu țările terțe relevante (astfel cum se prevede și la articolul 50 din RGPD). În acest sens, Comisia ia act de solicitarea comitetului de a lua în considerare drept potențiali omologi mai ales țările cu cei mai mulți operatori care fac în mod direct obiectul

([200]) De exemplu, în fața organelor parlamentare din Chile, Ecuador și Paraguay.

([201]) Aceasta a inclus și organizarea de seminare și vizite de studiu, de exemplu cu Kenya, Indonezia și Singapore.

([202]) Contribuția comitetului, pagina 8; poziția și constatările Consiliului, punctul 38.

RGPD, în special țările G7 și/sau țările care beneficiază de decizii privind caracterul adecvat al nivelului de protecție ([203]).

Instituirea unor astfel de acorduri de cooperare și de asistență reciprocă în materie de asigurare a respectării legislației ar contribui și la asigurarea conformării operatorilor străini care fac obiectul RGPD și la asigurarea respectării efective a legislației împotriva acestora, de exemplu deoarece aceștia vizează în mod special piața UE, oferind bunuri sau servicii. Consiliul observă importanța asigurării respectării RGPD în astfel de cazuri și își exprimă îngrijorarea cu privire la condițiile de concurență echitabile cu entitățile din UE, precum și la protecția eficace a drepturilor persoanelor fizice ([204]). Comisia este de acord cu solicitarea Consiliului de a explora diferite modalități de facilitare a punerii în aplicare în acest scenariu. Deși formele mai formale de cooperare cu autoritățile de reglementare din țările terțe ar putea juca, cu siguranță, un rol important, utilizarea altor căi – deja existente – ar trebui, de asemenea, urmărită cu mai multă fermitate. Aceasta include utilizarea deplină a setului de instrumente de asigurare a respectării legislației prevăzut la articolul 58 din RGPD și implicarea reprezentanților societăților străine din UE (numiți în conformitate cu articolul 27 din RGPD).

7.2.2 Dimensiunea multilaterală

De asemenea, Comisia continuă să participe activ la o serie de foruri internaționale pentru a promova valorile comune și a consolida convergența la nivel regional și mondial.

Aceasta include, de exemplu, contribuția activă la activitatea Comitetului consultativ privind Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108), singurul instrument multilateral obligatoriu din punct de vedere juridic în domeniul protecției datelor cu caracter personal. Până în prezent, 31 de state au ratificat Protocolul de modificare pentru modernizarea Convenției 108 ([205]), inclusiv multe state membre ale UE, precum și unele state nemembre ale Consiliului Europei (Argentina, Mauritius și Uruguay). Dintre statele membre ale UE, doar semnarea de către un stat membru ([206]) este încă nesoluționată, iar opt state membre ([207]) au semnat până în prezent, dar nu au ratificat convenția modernizată. Comisia invită insistent cele trei state membre rămase să semneze convenția în forma sa modernizată și toate statele membre să ia rapid măsurile necesare în vederea ratificării acesteia, pentru a permite intrarea sa în vigoare în viitorul apropiat. În plus, Comisia va continua să încurajeze în mod proactiv aderarea țărilor terțe.

La nivelul G20 și G7, discuțiile privind viața privată și fluxurile de date s-au axat pe operaționalizarea conceptului de „liberă circulație a datelor cu încredere” (*data free flow with trust* – DFFT), propus inițial de Japonia, care recunoaște că protecția și securitatea datelor pot contribui la încrederea în economia digitală și pot facilita fluxurile de date ([208]). OCDE joacă un rol deosebit de important în acest context, oferind un forum pentru o comunitate de experți în domeniul DFFT, care reunește o gamă largă de părți interesate (guverne, autorități de reglementare, industrie, societatea civilă, mediul academic) pentru a contribui la proiecte și întrebări specifice legate de DFFT. În plus, un rezultat semnificativ al inițiativei DFFT, la care Comisia a contribuit în mod semnificativ, este

([203]) Contribuția comitetului, pagina 8.
([204]) Poziția și constatările Consiliului, punctul 39.
([205]) Protocolul de modificare a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (CETS nr. 223).
([206]) Danemarca.
([207]) Belgia, Cehia, Grecia, Irlanda, Letonia, Luxemburg, Țările de Jos și Suedia.
([208]) A se vedea, de exemplu, https://www.g7germany.de/resource/blob/974430/2062292/fbdb2c7e996205aee402386aae057c5e/2022-07-14-leaders-communique-data.pdf?download=1.

adoptarea de către OCDE a unei declarații privind accesul autorităților publice la datele cu caracter personal deținute de entitățile din sectorul privat, primul instrument internațional în acest domeniu. Acesta conține o serie de cerințe comune pentru protejarea vieții private atunci când se accesează date cu caracter personal în scopul securității naționale și al asigurării respectării legii. În contextul unei recunoașteri tot mai largi la nivel mondial a faptului că încrederea în transferurile de date este afectată în mod negativ de accesul disproporționat al autorităților publice, această declarație reprezintă o contribuție importantă la facilitarea fluxurilor de date de încredere. Comisia va continua să încurajeze țările să adere la declarație, care este deschisă și țărilor care nu sunt membre ale OCDE.

Comisia colaborează și cu diferite organizații și rețele regionale care modelează garanții comune în materie de protecție a datelor. Este vorba, de exemplu, de ASEAN, Uniunea Africană, Forumul autorităților pentru protecția vieții private din zona Asia-Pacific, Rețeaua ibero-americană pentru protecția datelor și Rețeaua autorităților africane pentru protecția datelor (NADPA – RADPD). Elaborarea Ghidului UE-ASEAN menționat mai sus privind clauzele standard este un exemplu concret de astfel de cooperare fructuoasă.

În cele din urmă, Comisia menține un dialog cu diferite organizații internaționale, inclusiv pentru a explora modalități de a facilita și mai mult fluxurile de date dintre UE și astfel de organizații. Întrucât multe organizații și-au modernizat sau sunt pe cale să își modernizeze cadrele de protecție a datelor în ultimii ani, apar și noi oportunități de schimb de experiență și de bune practici. În acest sens, atelierele anuale cu organizațiile internaționale și un grup operativ dedicat transferurilor internaționale de date organizate de Autoritatea Europeană pentru Protecția Datelor s-au dovedit a fi foruri deosebit de utile pentru schimbul și explorarea unor instrumente concrete de cooperare, inclusiv pentru schimbul de date cu caracter personal ([209]).

8 CONCLUZIE

În cei 6 ani care au trecut de la momentul când a devenit aplicabil, RGPD a împuternicit persoanele fizice, permițându-le să aibă control asupra datelor lor. Acesta a contribuit, de asemenea, la crearea unor condiții de concurență echitabile pentru întreprinderi și a reprezentat o piatră de temelie pentru panoplia de inițiative care stimulează tranziția digitală în UE.

Pentru a realiza pe deplin dublul obiectiv al RGPD, respectiv o protecție solidă pentru persoanele fizice, asigurând în același timp libera circulație a datelor cu caracter personal în cadrul UE și fluxuri de date sigure în afara UE, este necesar să se pună accentul pe:

- o aplicare riguroasă a RGPD, începând cu adoptarea rapidă a propunerii Comisiei privind normele procedurale pentru a oferi soluționări rapide și securitate juridică în cazurile care afectează persoanele fizice din întreaga UE;
- sprijin proactiv pentru părțile interesate, din partea autorităților pentru protecția datelor, în eforturile lor de asigurare a conformității, în special pentru IMM-uri și operatorii de mici dimensiuni;
- o interpretare și o aplicare consecventă a RGPD în întreaga UE;
- cooperarea eficace între autoritățile de reglementare, atât la nivel național, cât și la nivelul UE, pentru a garanta aplicarea consecventă și coerentă a setului tot mai amplu de norme în domeniul digital ale UE;

([209]) https://www.edps.europa.eu/data-protection/our-work/edps-worldwide/data-protection-and-international-organisations_en.

- promovarea în continuare a strategiei internaționale a Comisiei privind protecția datelor.

Pentru a sprijini aplicarea eficace a RGPD și pentru a contribui la reflecțiile suplimentare privind protecția datelor, sunt necesare mai multe acțiuni identificate în prezentul document. Comisia va sprijini și va monitoriza punerea în aplicare a acestora și în perspectiva următorului raport din 2028.

Dezvoltarea unor structuri de cooperare eficace

Parlamentul European și Consiliul sunt invitate să adopte rapid propunerea privind normele procedurale ale RGPD.

Comitetul și autoritățile pentru protecția datelor sunt invitate:

- să stabilească o cooperare periodică cu alte autorități de reglementare sectoriale cu privire la aspecte cu impact asupra protecției datelor, în special cu cele instituite în temeiul noii legislații în domeniul digital a UE, și să participe activ la structurile de la nivelul UE menite să faciliteze cooperarea normativă orizontală;
- să utilizeze într-o măsură și mai mare instrumentele de cooperare prevăzute în RGPD, astfel încât soluționarea litigiilor să fie utilizată numai în ultimă instanță;
- să pună în aplicare modalități de lucru mai eficiente și mai specifice pentru orientări, avize și decizii și să acorde prioritate aspectelor esențiale pentru a reduce sarcina autorităților de protecție a datelor și pentru a reacționa mai rapid la evoluțiile pieței.

Statele membre trebuie:

- să asigure independența efectivă și deplină a autorităților naționale de protecție a datelor;
- să aloce resurse suficiente autorităților pentru protecția datelor pentru a le permite să își îndeplinească sarcinile, în special prin punerea la dispoziția acestora a resurselor tehnice și a expertizei necesare pentru tehnologiile emergente și pentru îndeplinirea de noi responsabilități introduse prin legislația din domeniul digital;
- să doteze autoritățile pentru protecția datelor cu instrumentele de investigare necesare pentru ca acestea să utilizeze în mod eficace competențele de asigurare a respectării legii prevăzute în RGPD;
- să sprijine dialogul dintre autoritățile pentru protecția datelor și alte autorități naționale de reglementare, în special cele instituite în temeiul noii legislații în domeniul digital.

Comisia:

- va sprijini în mod activ adoptarea rapidă de către colegiuitori a propunerii privind normele procedurale ale RGPD;
- va continua să monitorizeze îndeaproape independența efectivă și deplină a autorităților naționale pentru protecția datelor;
- va crea sinergii și coerență între RGPD și toate actele legislative care vizează prelucrarea datelor cu caracter personal pe baza experienței și, dacă este necesar, va lua măsurile adecvate pentru a oferi securitate juridică;
- va reflecta asupra modului în care poate răspunde mai bine necesității unei cooperări normative orizontale structurate și eficiente pentru a garanta aplicarea eficace, consecventă și coerentă a normelor în domeniul digital ale UE, respectând totodată competența autorităților pentru protecția datelor în ceea ce privește toate aspectele legate de prelucrarea datelor cu caracter personal.

Punerea în aplicare și completarea cadrului juridic

Statele membre trebuie:

- să se asigure că autoritățile pentru protecția datelor sunt consultate în timp util înainte de adoptarea unui act legislativ privind prelucrarea datelor cu caracter personal.

Comisia:

- va continua să utilizeze toate instrumentele de care dispune, inclusiv procedurile de constatare a încălcării obligațiilor, pentru a se asigura că statele membre respectă RGPD;
- va continua să sprijine schimburile de opinii și practicile naționale dintre statele membre, inclusiv prin intermediul Grupului de experți al statelor membre privind RGPD;
- va întreprinde acțiuni pentru a se asigura că copiii sunt protejați, împuterniciți și respectați în mediul online;
- va reflecta asupra posibilelor etape următoare referitoare la propunerea de regulament privind viața privată și comunicațiile electronice, inclusiv cu privire la relația acesteia cu RGPD.

Sprijinirea părților interesate

Comitetul și autoritățile pentru protecția datelor sunt invitate:

- să se angajeze într-un dialog constructiv cu operatorii și persoanele împuternicite de operatori cu privire la respectarea RGPD;
- să își intensifice în continuare eforturile de sprijinire a conformității IMM-urilor, prin furnizarea de orientări și instrumente adaptate, prin eliminarea oricăror preocupări nefondate legate de conformitate ale IMM-urilor care nu au ca activitate principală prelucrarea datelor cu caracter personal și prin însoțirea acestora în eforturile lor de asigurare a conformității;
- să sprijine punerea în aplicare de către întreprinderi a unor măsuri eficace de asigurare a conformității, cum ar fi certificarea și codurile de conduită (inclusiv ca instrumente pentru transferuri), colaborând cu părțile interesate în cursul procesului de aprobare, oferind termene clare pentru aprobări și, astfel cum s-a promis în strategia comitetului pentru perioada 2024-2027, explicând principalelor grupuri de părți interesate modul în care pot fi utilizate aceste instrumente;
- să se asigure că orientările naționale și aplicarea RGPD la nivel național sunt în concordanță cu orientările comitetului și cu jurisprudența Curții de Justiție;
- să soluționeze interpretările divergente ale RGPD între autoritățile de protecție a datelor, inclusiv între autoritățile din același stat membru;
- să furnizeze orientări concise, practice și accesibile publicului relevant, astfel cum s-a promis în strategia comitetului pentru perioada 2024-2027;
- să asigure o consultare mai timpurie și mai semnificativă cu privire la orientări și avize pentru a înțelege mai bine dinamica pieței și practicile comerciale, să acorde atenția cuvenită feedbackului primit și să ia în considerare aplicarea concretă a interpretărilor adoptate;
- să finalizeze cu prioritate lucrările în curs referitoare la orientările privind datele copiilor, cercetarea științifică, anonimizarea, pseudonimizarea și interesul legitim;

- să intensifice activitățile de sensibilizare, informarea și acțiunile de asigurare a respectării legii pentru a se asigura că responsabilii cu protecția datelor își pot îndeplini rolul care le revine în temeiul RGPD.

Comisia:

- va continua să ofere sprijin financiar pentru activitățile autorităților pentru protecția datelor care facilitează punerea în aplicare a obligațiilor prevăzute în RGPD de către IMM-uri;
- va utiliza toate mijloacele disponibile pentru a oferi clarificări rapide cu privire la aspecte importante pentru părțile interesate, inclusiv pentru IMM-uri, în special prin solicitarea de avize din partea comitetului.

Dezvoltarea în continuare a setului de instrumente pentru transferurile de date și cooperarea internațională

Comitetul și autoritățile pentru protecția datelor sunt invitate:

- să finalizeze lucrările de simplificare și scurtare a procesului de aprobare a regulilor corporatiste obligatorii, precum și de actualizare a orientărilor privind elementele care trebuie să se regăsească în regulile corporatiste obligatorii ale persoanei împuternicite de operator;
- să exploreze modalități/instrumente pentru a sprijini în continuare exportatorii de date în eforturile lor de asigurare a conformității în ceea ce privește cerințele prevăzute în hotărârea Schrems II;
- să exploreze noi modalități eficace de asigurare a respectării normelor împotriva operatorilor stabiliți în țări terțe care intră în domeniul de aplicare teritorial al RGPD.

Statele membre trebuie:

- să asigure semnarea și ratificările rămase ale Convenției 108+ modernizate a Consiliului Europei cât mai curând posibil, pentru a permite intrarea în vigoare a acesteia.

Comisia:

- va realiza progrese suplimentare în cadrul discuțiilor în curs privind caracterul adecvat al nivelului de protecție, va explora dezvoltarea în continuare a constatărilor existente privind caracterul adecvat al nivelului de protecție și va urmări noi dialoguri cu partenerii interesați privind caracterul adecvat al nivelului de protecție;
- va sprijini o cooperare sporită în cadrul rețelei de țări care beneficiază de decizii privind caracterul adecvat al nivelului de protecție;
- va finaliza lucrările privind clauzele contractuale standard suplimentare, în special pentru transferurile de date către importatorii de date a căror prelucrare face în mod direct obiectul RGPD și pentru transferurile de date efectuate de instituțiile și organele UE în temeiul Regulamentului (UE) 2018/1725;
- va coopera cu partenerii internaționali în ceea ce privește facilitarea fluxurilor de date pe baza unor clauze contractuale standard;
- va sprijini procesele de reformă aflate în curs în țările terțe cu privire la normele noi sau modernizate de protecție a datelor, prin schimburi de experiență și de bune practici;
- va colabora cu organizații internaționale și regionale, cum ar fi OCDE, ASEAN sau G7, pentru a promova fluxurile de date de încredere bazate pe standarde ridicate de

protecție a datelor, inclusiv în contextul inițiativei „Libera circulație a datelor cu încredere”;

- va facilita și va sprijini schimburile dintre autoritățile de reglementare europene și internaționale, inclusiv prin intermediul Academiei sale de protecție a datelor;
- va contribui la promovarea cooperării internaționale în materie de asigurare a respectării legii între autoritățile de supraveghere, inclusiv prin negocierea unor acorduri de cooperare și asistență reciprocă.