COMISIA
EUROPEANĂ

Bruxelles, 24.6.2020
COM(2020) 264 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Protecția datelor ca pilon al capacitării cetățenilor și al abordării UE privind tranziția digitală - doi ani de aplicare a Regulamentului general privind protecția datelor

{SWD(2020) 115 final}

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Protecția datelor ca pilon al capacitării cetățenilor și al abordării UE privind tranziția digitală - doi ani de aplicare a Regulamentului general privind protecția datelor

1 NORMELE DE PROTECȚIE A DATELOR CA PILON AL CAPACITĂRII CETĂȚENILOR ȘI AL ABORDĂRII UE PRIVIND TRANZIȚIA DIGITALĂ

Prezentul raport este primul de acest fel referitor la evaluarea și revizuirea Regulamentului general privind protecția datelor[1] (denumit în continuare „RGPD”), în special în ceea ce privește aplicarea și funcționarea normelor privind transferul de date cu caracter personal către țări terțe și organizații internaționale și a normelor privind cooperarea și consecvența, în conformitate cu articolul 97 din RGPD.

RGPD, care se aplică începând cu 25 mai 2018, se află în centrul cadrului[2] Uniunii Europene de garantare a dreptului fundamental la protecția datelor, astfel cum este consacrat în Carta drepturilor fundamentale a Uniunii Europene (articolul 8) și în tratate (articolul 16 din Tratatul privind funcționarea Uniunii Europene, „TFUE”). RGPD a consolidat garanțiile de protecție a datelor, acordă persoanelor fizice drepturi suplimentare și mai solide, a sporit transparența și garantează că toți cei care prelucrează date cu caracter personal în conformitate cu domeniul său de aplicare sunt mai responsabili și pot fi trași mai ușor la răspundere. Regulamentul le acordă autorităților independente pentru protecția datelor atribuții mai importante și mai armonizate de aplicare a legii și stabilește un nou sistem de guvernanță. De asemenea, acesta asigură condiții de concurență echitabile pentru toate întreprinderile care operează pe piața UE, indiferent de locul unde sunt stabilite, și asigură libera circulație a datelor în interiorul UE, întărind, prin urmare, piața internă.

RGPD este o componentă importantă a abordării centrate pe factorul uman a tehnologiei și un punct de reper pentru utilizarea tehnologiei digitale în cadrul dublei tranziții, verzi și digitale, care caracterizează elaborarea politicilor UE. Acest lucru a fost subliniat mai recent în Cartea albă privind inteligența artificială[3] și în Comunicarea intitulată „O strategie europeană privind datele”[4] (denumită în continuare „strategia privind datele”) din februarie 2020.

Într-o economie din ce în ce mai dependentă de prelucrarea datelor, inclusiv a celor cu caracter personal, RGPD este un instrument esențial care garantează că persoanele au un control mai bun asupra datelor cu caracter personal și că datele sunt prelucrate într-

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

[2] În urma încorporării sale în Acordul privind Spațiul Economic European (SEE), regulamentul se aplică și Norvegiei, Islandei și Liechtensteinului.

[3] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy.

un scop legitim, într-un mod legal, echitabil și transparent. În același timp, RGPD ajută la promovarea inovării fiabile, în special prin abordarea sa bazată pe riscuri și prin principii cum ar fi protejarea vieții private începând cu momentul conceperii și în mod implicit. Comisia a propus completarea cadrului legislativ privind protecția datelor și viața privată[5] prin Regulamentul privind viața privată și comunicațiile electronice[6], care este destinat să înlocuiască actuala Directivă asupra confidențialității și comunicațiilor electronice[7]. Această propunere este examinată în prezent de colegiuitori și este foarte important să se asigure adoptarea sa rapidă.

În contextul priorităților-cheie ale Comisiei privind „o Europă pregătită pentru era digitală”[8] și „Pactul verde european”[9], pot fi dezvoltate noi inițiative care să capaciteze cetățenii să joace un rol mai activ în tranziția digitală și în valorificarea utilizării instrumentelor digitale pentru a crea o societate neutră din punct de vedere climatic și pentru o dezvoltare mai durabilă. RGPD stabilește un cadru pentru aceste inițiative și garantează că ele sunt concepute pentru a capacita efectiv cetățenii.

Strategia europeană privind datele[10] face apel la crearea unui „spațiu european unic al datelor” – o piață unică veritabilă pentru date – precum și a zece spații sectoriale comune europene ale datelor, relevante pentru dubla tranziție verde și digitală[11]. Pentru toate aceste priorități, este esențial să existe un cadru clar și funcțional pentru schimbul de date în condiții de siguranță și o disponibilitate sporită a datelor. Strategia privind datele a anunțat, totodată, intenția Comisiei de a analiza, în acte legislative viitoare, modalități prin care să se permită utilizarea datelor deținute în bazele de date publice în scopuri de cercetare științifică, într-o manieră conformă cu RGPD. Spațiile datelor urmează să fie sprijinite prin agregarea serviciilor în cloud la nivel european, furnizându-se astfel servicii de prelucrare a datelor și de infrastructură de tip cloud conforme cu RGPD. RGPD asigură un nivel ridicat de protecție a datelor cu caracter personal și acordă un rol central persoanelor fizice în toate aceste spații ale datelor, oferind în același timp flexibilitatea necesară pentru a permite abordări diferite.

Cu siguranță, necesitatea de a asigura un anumit nivel de încredere și cererea pentru protecția datelor cu caracter personal nu se limitează la UE. Cetățeni din întreaga

---

[5] Acest cadru legislativ include, de asemenea, Directiva privind protecția datelor în materie de asigurare a respectării legii (Directiva 2016/680) și Regulamentul privind protecția datelor pentru instituțiile și organele UE (Regulamentul 2018/1725).

[6] Propunere de regulament al Parlamentului European și al Consiliului privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice și de abrogare a Directivei 2002/58/CE (Regulamentul privind viața privată și comunicațiile electronice) - COM/2017/010 final - 2017/03 (COD).

[7] Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), JO L 201, 31.7.2002, p. 37.

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_ro.

[9] Comunicarea Comisiei către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor „Pactul verde european” COM(2019) 640 final.

[10] Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor „O strategie europeană privind datele”, COM/2020/66 final.

[11] Aceste zece spații sectoriale comune europene ale datelor se referă la: sănătate, producția industrială, energie, mobilitate, agricultură, date financiare, administrația publică, un spațiu comun european al datelor privind competențele în materie de date, un spațiu al datelor privind Pactul verde european, precum și la Cloudul european pentru știința deschisă.

lume apreciază din ce în ce mai mult confidențialitatea și securitatea propriilor date. După cum arată un sondaj recent la nivel mondial[12], aceștia consideră protecția datelor cu caracter personal ca fiind un factor important care influențează deciziile lor de cumpărare și comportamentul lor online. Un număr din ce în ce mai mare de întreprinderi a răspuns acestei solicitări de respectare a vieții private, în special prin aplicarea, în mod voluntar, a unora dintre drepturile și garanțiile prevăzute în RGPD și în cazul clienților lor din afara UE. Totodată, multe întreprinderi promovează respectarea datelor cu caracter personal ca factor de diferențiere din punct de vedere concurențial și ca atu comercial pe piața mondială, prin oferirea de produse și servicii inovatoare, cu soluții noi privind respectarea vieții private sau securitatea datelor. De asemenea, capacitatea sporită a actorilor din sectorul public și privat de a colecta și a prelucra datele la o scară largă ridică întrebări importante și complexe, care plasează din ce în ce mai des viața privată în centrul dezbaterii publice în diferite părți ale lumii.

Adoptarea RGPD a determinat și alte țări, din numeroase regiuni ale lumii, să urmeze exemplul Uniunii Europene. Se conturează o tendință cu adevărat mondială, care se manifestă din Chile până în Coreea de Sud, din Brazilia până în Japonia, din Kenya până în India și din California până în Indonezia. Asumarea de către UE a rolului de lider în domeniul protecției datelor arată că aceasta poate acționa ca un model în materie de stabilire a standardelor la nivel mondial pentru reglementarea economiei digitale, această poziționare fiind salutată de voci importante ale comunității internaționale, cum ar fi secretarul general al ONU, António Guterres, care a remarcat modul în care RGPD „*a stabilit un exemplu* […] *care inspiră măsuri similare și în alte țări*” și „*a îndemânat UE și statele sale membre să continue să joace un rol de lider în vederea conturării erei digitale și să se situeze în avangarda inovării și a reglementării tehnologice*”.[13]

Actuala criză provocată de pandemia de COVID-19 oferă o imagine foarte sugestivă a acestei globalizări a dezbaterii privind viața privată, atât în timpul crizei și cât ulterior, pe măsură ce lumea încearcă să iasă din criză. În UE, mai multe state membre au luat măsuri de urgență pentru a proteja sănătatea publică. RGPD menționează clar că orice restricție trebuie să respecte esența drepturilor și libertăților fundamentale și să fie o măsură necesară și proporțională într-o societate democratică pentru a proteja un interes public, cum ar fi sănătatea publică. Odată cu eliminarea treptată a măsurilor de limitare a răspândirii, factorii de decizie trebuie să răspundă așteptărilor cetățenilor de a beneficia de soluții digitale de încredere, care să respecte drepturile la viața privată și la protecția datelor cu caracter personal.

În numeroase țări, măsurile integrate de protecție a vieții private, cum ar fi înscrierea voluntară a utilizatorilor, minimizarea datelor și securitatea acestora, precum și excluderea geolocalizării, sunt considerate esențiale pentru a asigura fiabilitatea și

---

[12] A se vedea, de exemplu, Studiul Cisco privind viața privată a consumatorilor din 2019 (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). Conform acestui studiu, care a vizat 2 600 de consumatori din întreaga lume, un număr semnificativ de consumatori a luat deja măsuri pentru a-și proteja viața privată, de exemplu, schimbând întreprinderile sau furnizorii din cauza politicilor lor privind datele sau a practicilor acestora în materie de schimb de date.

[13] Alocuțiunea secretarului general al ONU în Senatul italian, 18 decembrie 2019 (disponibilă la adresa: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

acceptarea socială a soluțiilor bazate pe date care vizează monitorizarea și limitarea răspândirii virusului, calibrarea contramăsurilor de politici publice, acordarea de asistență pacienților sau punerea în aplicare a strategiilor de ieșire. În UE, cadrul legislativ privind protecția datelor și a vieții private[14] s-a dovedit a fi un instrument suficient de flexibil pentru a permite dezvoltarea de soluții practice (de exemplu, aplicațiile de depistare a contacților), asigurând în același timp un nivel ridicat de protecție a datelor cu caracter personal. În acest context, la 16 aprilie 2020, Comisia a publicat orientări în domeniul protecției datelor privind aplicațiile care sprijină combaterea pandemiei[15].

Protejarea datelor cu caracter personal este, de asemenea, esențială pentru prevenirea manipulării alegerilor făcute de cetățeni, în special prin adresarea de conținut personalizat alegătorilor, bazată pe prelucrarea ilegală a datelor cu caracter personal, pentru evitarea interferențelor în procesele democratice și menținerea unei dezbateri deschise, a corectitudinii și a transparenței, care sunt esențiale într-o democrație. Din acest motiv, în septembrie 2018, Comisia a publicat orientări privind aplicarea legislației Uniunii în materie de protecție a datelor în contextul alegerilor[16].

Pentru prezenta evaluare și revizuire, Comisia a luat în considerare contribuțiile Consiliului[17], ale Parlamentului European[18], ale Comitetului european pentru protecția datelor (denumit în continuare „comitetul”)[19] și ale autorităților individuale pentru protecția datelor[20], ale Grupului multipartit de experți[21] și ale altor părți interesate, inclusiv prin feedbackul acordat cu privire la foaia de parcurs[22].

---

[14] Acest cadru cuprinde, pe lângă RGPD, și Directiva asupra confidențialității și comunicațiilor electronice (Directiva 2002/58/CE), care prevede, printre altele, norme privind accesarea și stocarea informațiilor pe terminalul utilizatorului.

[15] Comunicare a Comisiei - Orientări în domeniul protecției datelor privind aplicațiile care sprijină combaterea pandemiei de COVID-19 (2020/C 124 I/01 - C/2020/2523 - JO C 124I, 17.4.2020, p. 1). La 16 aprilie 2020, statele membre ale UE, sprijinite de Comisie, au elaborat un set de instrumente al UE pentru utilizarea aplicațiilor mobile de depistare a contacților și de avertizare ca răspuns la pandemia de COVID-19. Acesta face parte dintr-o abordare coordonată comună pentru a sprijini ridicarea treptată a măsurilor de limitare a mișcării persoanelor. (https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf).

[16] Orientările Comisiei privind aplicarea legislației Uniunii în materie de protecție a datelor în contextul alegerilor. Contribuția Comisiei Europene la reuniunea liderilor din 19-20 septembrie 2018 de la Salzburg (COM/2018/638 final).

[17] Poziția Consiliului și constatările privind aplicarea Regulamentului general privind protecția datelor (RGPD): https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/ro/pdf.

[18] Scrisoarea Comisiei LIBE a Parlamentului European din 21 februarie 2020 către comisarul Reynders, Ref.: IPOL-COM-LIBE D (2020)6525.

[19] Contribuția comitetului la evaluarea RGPD în conformitate cu articolul 97, adoptată la 18 februarie 2020: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en.

[20] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en.

[21] Grupul multipartit de experți privind regulamentul, instituit de Comisie, cuprinde reprezentanți ai societății civile și ai mediului de afaceri, ai mediului universitar și practicieni: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537.

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation/feedback?p_id=7669437.

În general, se consideră că, după doi ani de când a început să se aplice, RGPD și-a atins cu succes obiectivele de a asigura o protecție mai bună a drepturilor persoanelor fizice la protecția datelor cu caracter personal și de a garanta libera circulație a datelor cu caracter personal în cadrul UE[23]. Cu toate acestea, au fost identificate și câteva domenii care ar putea fi îmbunătățite în viitor. La fel ca majoritatea părților interesate și a autorităților pentru protecția datelor, Comisia este de părere că, în această etapă, ar fi prematur să se tragă concluzii definitive cu privire la aplicarea RGPD. Dobândirea unei experiențe mai ample în aplicarea RGPD în anii următori va fi utilă pentru cele mai multe dintre problemele identificate de către statele membre și părțile interesate. Totuși, prezentul raport scoate în evidență provocările întâlnite până acum în aplicarea RGPD și prezintă posibile modalități de a le aborda.

Fără a aduce atingere accentului pus pe cele două aspecte evidențiate la articolul 97 alineatul (2) din RGPD, și anume transferurile internaționale și mecanismele de cooperare și coerență, prezenta evaluare și revizuire are o sferă mai largă, abordând și aspecte care au fost ridicate de diferiți actori în ultimii doi ani.

2 PRINCIPALELE CONSTATĂRI

Aplicarea RGPD și funcționarea mecanismelor de cooperare și coerență

RGPD a instituit un sistem de guvernanță inovator, bazat pe autorități independente pentru protecția datelor în statele membre și pe cooperarea dintre acestea în cazurile transfrontaliere și în cadrul Comitetului european pentru protecția datelor (denumit în continuare „comitetul”). Opinia generală este că autoritățile pentru protecția datelor au utilizat în mod echilibrat competențele lor corective consolidate, inclusiv avertizările și mustrările, amenzile și limitările temporare sau definitive în materie de prelucrare[24]. Comisia constată că autoritățile au aplicat amenzi administrative cuprinse între câteva mii de euro și câteva milioane, în funcție de gravitatea încălcărilor. Alte sancțiuni, cum ar fi interzicerea prelucrării, pot avea un efect de descurajare similar, dacă nu chiar mai important, decât amenzile. Obiectivul final al RGPD este schimbarea culturii și a comportamentului tuturor actorilor implicați, în beneficiul persoanelor fizice. Informații mai detaliate privind utilizarea competențelor corective de către autoritățile pentru protecția datelor sunt prezentate în documentul de lucru al serviciilor Comisiei care însoțește prezentul document.

Deși este încă prematur să se evalueze pe deplin funcționarea noilor mecanisme de cooperare și coerență, autoritățile pentru protecția datelor au dezvoltat cooperarea prin mecanismul ghișeului unic[25] și printr-o largă utilizare a asistenței reciproce[26]. Mecanismul ghișeului unic, care este un element-cheie al pieței interne, este utilizat pentru a lua decizii în numeroase cazuri transfrontaliere[27]. Sunt în curs de adoptare decizii importante cu o dimensiune transfrontalieră care vor face obiectul mecanismului ghișeului unic. Aceste decizii, care implică deseori mari companii

[23] A se vedea, de exemplu, poziția și constatările Consiliului, precum și contribuția comitetului.
[24] A se vedea punctul 2.1 din documentul de lucru al serviciilor Comisiei.
[25] Dacă o întreprindere prelucrează date la nivel transfrontalier, autoritatea competentă pentru protecția datelor este cea din statul membru în care întreprinderea își are sediul principal.
[26] A se vedea punctul 2.2 din documentul de lucru al serviciilor Comisiei.
[27] Între 25 mai 2018 și 31 decembrie 2019, au fost prezentate prin procedura ghișeului unic 141 de proiecte de decizie, iar pentru 79 dintre acestea s-au emis decizii finale.

multinaționale din domeniul tehnologiei informației, vor avea un impact substanțial asupra drepturilor persoanelor în multe state membre.

Cu toate acestea, dezvoltarea unei veritabile culturi europene comune în ceea ce privește protecția datelor între autoritățile pentru protecția datelor reprezintă un proces continuu. Autoritățile pentru protecția datelor nu au recurs încă la toate instrumentele pe care le oferă RGPD, cum ar fi operațiunile comune care ar putea duce la investigații comune. Uneori, găsirea unei abordări comune a însemnat identificarea celui mai mic numitor comun și, ca urmare, au fost pierdute oportunități de a promova un grad mai înalt de armonizare[28].

Sunt necesare progrese suplimentare pentru a eficientiza și a armoniza gestionarea cazurilor transfrontaliere în întreaga UE, inclusiv din punct de vedere procedural, de exemplu, în ceea ce privește aspecte cum ar fi procedurile de soluționare a plângerilor, criteriile de admisibilitate a plângerilor, durata procedurilor din cauza diferitelor intervale de timp sau a absenței termenelor în dreptul procesual administrativ național, momentul în cadrul procedurii în care se acordă dreptul de a fi audiat sau informarea și implicarea reclamanților în timpul procedurii. Procesul de reflecție lansat de comitet în legătură cu acest aspect este binevenit, iar Comisia participă la aceste discuții[29].

Activitățile și orientările comitetului sunt de o importanță esențială pentru dezvoltarea consecventă în viitor a schimburilor dintre comitet și părțile interesate[30]. Până la sfârșitul anului 2019, comitetul adoptase 67 de documente, inclusiv 10 noi orientări[31] și 43 de avize[32]. În general, părțile interesate salută orientările comitetului și solicită orientări suplimentare cu privire la conceptele-cheie ale RGPD, dar indică, de asemenea, neconcordanțe între orientările naționale și cele ale comitetului. Ele subliniază necesitatea unor sfaturi mai practice, în special a unor exemple mai concrete, precum și necesitatea ca autoritățile pentru protecția datelor să dețină resursele umane, tehnice și financiare necesare pentru a-și îndeplini efectiv sarcinile.

Comisia a subliniat constant obligația statelor membre de a aloca suficiente resurse umane, financiare și tehnice autorităților naționale pentru protecția datelor[33]. Majoritatea autorităților au beneficiat de o creștere a numărului de personal și a bugetului între 2016 și 2019[34], autoritățile irlandeze, neerlandeze, islandeze,

---

[28] De exemplu, listele naționale ale tipurilor de operațiuni de prelucrare care necesită evaluarea impactului asupra protecției datelor în conformitate cu articolul 35 din RGPD ar fi putut fi mai bine armonizate.

[29] A se vedea punctul 2.2 din documentul de lucru al serviciilor Comisiei.

[30] În special reprezentanții mediului de afaceri și ai societății civile. A se vedea punctul 2.3 din documentul de lucru al serviciilor Comisiei.

[31] Acestea completează cele 10 orientări care au fost adoptate de Grupul de lucru instituit prin articolul 29 în perioada prealabilă intrării în vigoare a regulamentului și care au fost aprobate de comitet. Comitetul a adoptat, de asemenea, 4 orientări suplimentare între luna ianuarie și sfârșitul lunii mai 2020 și a actualizat o orientare existentă.

[32] 42 dintre aceste avize au fost adoptate în temeiul articolului 64 din RGPD, iar un aviz a fost adoptat în temeiul articolului 70 alineatul (1) litera (s) din RGPD și a vizat decizia privind caracterul adecvat al nivelului de protecție cu privire la Japonia.

[33] Comunicare a Comisiei către Parlamentul European și Consiliu, Normele privind protecția datelor, factor favorizant al încrederii în UE și în afara acesteia – bilanț – COM(2019) 374 final, 24.7.2019.

[34] S-a înregistrat o creștere globală de 42 % în ceea ce privește personalul și de 49 % în ceea ce privește bugetul la nivelul tuturor autorităților naționale pentru protecția datelor din SEE, luate împreună, între 2016 și 2019.

luxemburgheze și finlandeze beneficiind de cele mai mari creșteri relative în ceea ce privește personalul. Având în vedere că cele mai mari companii multinaționale din domeniul tehnologiei informației își au sediul în Irlanda și în Luxemburg, autoritățile pentru protecția datelor ale acestor țări acționează ca autorități principale în multe cazuri transfrontaliere importante și ar putea avea nevoie de resurse mai mari comparativ cu populația țărilor lor. Cu toate acestea, situația este încă inegală între statele membre și nesatisfăcătoare în ansamblu. Autoritățile pentru protecția datelor joacă un rol esențial pentru a garanta că RGPD este pus în aplicare la nivel național și că mecanismele de cooperare și coerență din cadrul comitetului funcționează efectiv, în special mecanismul ghișeului unic pentru cazurile transfrontaliere. Prin urmare, statele membre sunt invitate să pună la dispoziția autorităților menționate suficiente resurse, în conformitate cu dispozițiile RGPD[35].

Normele sunt armonizate, dar persistă un anumit grad de fragmentare și abordări divergente

Comisia monitorizează punerea în aplicare a RGPD în legislația națională. La data prezentului raport, toate statele membre, cu excepția Sloveniei, adoptaseră noua legislație sau își adaptaseră legislația națională privind protecția datelor. Slovenia[36] a fost invitată să furnizeze clarificări Comisiei cu privire la finalizarea acestui proces[37].

RGPD asigură o abordare coerentă a normelor de protecție a datelor în întreaga UE. Cu toate acestea, RGPD le impune statelor membre obligația de a legifera în anumite domenii[38] și le acordă posibilitatea de a detalia mai mult dispozițiile RGPD în alte domenii[39]. Ca urmare, există încă un anumit grad de fragmentare, care se datorează în special utilizării pe scară largă a clauzelor de specificare facultative. De exemplu, diferența dintre statele membre în ceea ce privește vârsta consimțământului copiilor în raport cu serviciile societății informaționale creează incertitudine pentru copii și părinții lor în ceea ce privește aplicarea drepturilor lor în materie de protecție în cadrul pieței unice. Această fragmentare creează, de asemenea, provocări în ceea ce privește desfășurarea de activități comerciale transfrontaliere și inovarea, în special în legătură cu noile evoluții tehnologice și soluții de securitate cibernetică. Pentru a se asigura funcționarea eficace a pieței interne și pentru a se evita impunerea unor sarcini inutile asupra întreprinderilor, este de asemenea esențial ca legislația națională să nu depășească limitele stabilite de RGPD și să nu introducă cerințe suplimentare atunci când nu există astfel de limite.

O provocare specifică pentru legislația națională o reprezintă reconcilierea dintre dreptul la protecția datelor cu caracter personal și libertatea de exprimare și informare, precum și echilibrarea corespunzătoare a acestor drepturi. În ceea ce privește ordinea precedenței, în unele legislații naționale primează libertatea de exprimare, în timp ce în altele protecția datelor cu caracter personal este prioritară, aplicarea normelor de protecție a datelor fiind exceptată numai în anumite situații, cum ar fi în cazul în care

[35] A se vedea punctul 2.4 din documentul de lucru al serviciilor Comisiei.
[36] Cel mai recent, printr-o scrisoare a comisarului Reynders din martie 2020.
[37] Trebuie menționat că autoritatea națională pentru protecția datelor din Slovenia este înființată pe baza legii privind protecția datelor în vigoare și supraveghează aplicarea RGPD în statul membru respectiv.
[38] A se vedea punctul 3.1 din documentul de lucru al serviciilor Comisiei.
[39] A se vedea punctul 3.2 din documentul de lucru al serviciilor Comisiei.

este vorba despre o persoană publică. În sfârșit, alte state membre prevăd stabilirea de către legiuitor a unui anumit echilibru și/sau a unei evaluări de la caz la caz în ceea ce privește derogările de la anumite dispoziții ale RGPD.

Comisia va continua evaluarea legislației naționale. Reconcilierea trebuie să fie prevăzută în lege, să respecte esența drepturilor fundamentale respective și să fie proporțională și necesară[40]. Normele de protecție a datelor (precum și interpretarea și aplicarea lor) nu ar trebui să afecteze exercitarea libertății de exprimare și de informare, de exemplu, prin efecte de intimidare sau prin exercitarea de presiuni asupra jurnaliștilor ca să își dezvăluie sursele. Echilibrarea acestor două drepturi în legislația națională ar trebui să țină cont de jurisprudența Curții de Justiție și a Curții Europene a Drepturilor Omului[41].

Legislația statelor membre urmărește abordări diferite atunci când pune în aplicare derogări de la interdicția generală de prelucrare a categoriilor speciale de date cu caracter personal, în ceea ce privește nivelul specificării și al garanțiilor, inclusiv în scopuri legate de sănătate și de cercetare. Pentru a aborda această problemă, Comisia realizează, într-o primă etapă, o cartografiere a diferitelor abordări ale statelor membre[42] și, într-o etapă următoare, va sprijini stabilirea unui cod (a unor coduri) de conduită care să contribuie la o abordare mai coerentă în acest domeniu și să faciliteze prelucrarea transfrontalieră a datelor cu caracter personal[43]. În plus, viitoarele orientări ale comitetului în ceea ce privește utilizarea datelor cu caracter personal în domeniul cercetării științifice vor contribui la o abordare armonizată. Comisia va furniza contribuții comitetului, în special în ceea ce privește cercetarea în domeniul sănătății, inclusiv sub formă de întrebări și analize concrete cu privire la scenarii specifice, pe care le-a primit de la comunitatea de cercetare.

[40] Articolul 52 alineatul (1) din Cartă.
[41] A se vedea punctul 3.1 din documentul de lucru al serviciilor Comisiei. Reconcilierea dintre dreptul la protecția datelor cu caracter personal și libertatea de exprimare și informare.
[42] Comisia a lansat un studiu privind „Evaluarea normelor statelor membre referitoare la datele privind sănătatea din perspectiva RGPD”, Chafea/2018/Health/03, contractul specific nr. 2019 70 01.
[43] A se vedea acțiunile anunțate în strategia europeană privind datele, pagina 30.

Capacitarea persoanelor fizice pentru a-și controla datele

Potrivit unui sondaj privind drepturile fundamentale[44], 69 % din populația UE în vârstă de peste 16 ani a auzit de RGPD, iar 71 % din cetățenii UE știu despre existența autorității lor naționale pentru protecția datelor.

Persoanele fizice sunt din ce în ce mai conștiente de drepturile lor: drepturile de acces, de rectificare, de ștergere și de portabilitate a datelor lor cu caracter personal, dreptul de a se opune prelucrării, precum și o transparență sporită. RGPD a consolidat drepturile procedurale, incluzând dreptul de a depune o plângere la o autoritate pentru protecția datelor, inclusiv prin acțiuni de reprezentare, precum și dreptul la o cale de atac judiciară. Persoanele fizice invocă din ce în ce mai des aceste drepturi, dar este necesar să se faciliteze exercitarea și deplina aplicare a acestora. Exercițiile de reflecție efectuate sub conducerea comitetului vor clarifica și facilita în continuare exercitarea drepturilor individuale și se preconizează că, odată adoptată, Directiva privind acțiunile de reprezentare propusă[45] le va permite persoanelor fizice să introducă acțiuni colective în toate statele membre și va reduce costurile acțiunilor transfrontaliere.

Dreptul la portabilitatea datelor are un potențial clar, neutilizat încă pe deplin, de a plasa persoanele fizice în centrul economiei bazate pe date, permițându-le să facă transferul între furnizori de servicii diferiți, să combine servicii diferite, să utilizeze alte servicii inovatoare și să aleagă serviciile care sunt cele mai favorabile protecției datelor. Acest lucru va încuraja, în mod indirect, concurența și va sprijini inovarea. Deblocarea acestui potențial este una dintre prioritățile Comisiei, în special deoarece, odată cu utilizarea mai frecventă a dispozitivelor bazate pe internetul obiectelor, din ce în ce mai multe date sunt generate de către consumatori, care riscă să se confrunte cu practici neloiale și cu efecte de blocare. Portabilitatea ar putea aduce beneficii semnificative în ceea ce privește sănătatea și bunăstarea, reducerea amprentei ecologice și accesul la servicii publice și private, o productivitate mai mare în industria prelucrătoare și creșterea calității și a siguranței produselor.

Strategia privind datele a subliniat necesitatea de a aborda dificultățile precum lipsa unor standarde care să permită furnizarea de date într-un format care poate fi citit automat, pentru a spori utilizarea efectivă a dreptului la portabilitatea datelor, în prezent limitat la câteva sectoare (de exemplu, sectorul bancar și al telecomunicațiilor). Acest lucru s-ar putea realiza în special prin proiectarea de instrumente adecvate și prin formate și interfețe standardizate[46]. De asemenea, această utilizare sporită ar putea să fie realizată în special prin impunerea obligativității interfețelor tehnice și a formatelor care pot fi citite automat ce permit portabilitatea datelor în timp real. Utilizarea sporită a dreptului la portabilitate ar putea, printre altele, să faciliteze utilizarea de către persoanele fizice a datelor proprii pentru binele public (de exemplu, pentru a favoriza cercetarea în sectorul sănătății), dacă doresc

[44] Agenția pentru Drepturi Fundamentale a Uniunii Europene (FRA) (2020): Sondaj privind drepturile fundamentale 2019. Protecția datelor și tehnologia: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection.

[45] Propunerea de directivă privind acțiunile de reprezentare pentru protecția intereselor colective ale consumatorilor [COM/2018/0184 final - 2018/089 (COD)], odată adoptată, va consolida cadrul pentru acțiunile de reprezentare și în domeniul protecției datelor.

[46] Aceste instrumente ar putea include instrumente de gestionare a consimțământului și aplicații de gestionare a informațiilor personale.

acest lucru („altruismul în materie de date”). În vederea pregătirii pachetului legislativ privind serviciile digitale[47], Comisia va examina mai pe larg rolul datelor și al practicilor legate de date în ecosistemul platformelor.

[47] https://ec.europa.eu/commission/presscorner/detail/ro/ip_20_962.

Oportunități și provocări pentru organizații, în special pentru întreprinderile mici și mijlocii

RGPD, împreună cu Regulamentul privind libera circulație a datelor fără caracter personal[48], le oferă oportunități întreprinderilor prin promovarea concurenței și a inovării, asigurând fluxul liber de date în cadrul UE și creând condiții de concurență egale cu cele de care beneficiază întreprinderile stabilite în afara UE[49]. Dreptul la portabilitate și numărul tot mai mare de persoane care caută soluții mai favorabile vieții private au potențialul de a reduce barierele la intrare pentru întreprinderi și de a oferi posibilități de creștere bazate pe încredere și inovare. Unele părți interesate raportează că aplicarea RGPD reprezintă o provocare mai ales pentru întreprinderile mici și mijlocii (IMM-uri). Conform abordării bazate pe riscuri, nu ar fi adecvat să se prevadă derogări în funcție de dimensiunea operatorilor, întrucât dimensiunea nu constituie, în sine, un indicator al riscurilor pe care le poate crea pentru persoanele fizice prelucrarea datelor cu caracter personal. Mai multe autorități de protecție a datelor au pus la dispoziție instrumente practice pentru a facilita punerea în aplicare a RGPD de către IMM-uri care desfășoară activități de prelucrare cu risc scăzut. Ar trebui ca aceste eforturi să fie accelerate și extinse, de preferință în cadrul unei abordări europene comune, astfel încât să nu se creeze bariere în calea pieței unice.

Autoritățile pentru protecția datelor au luat o serie de măsuri pentru a ajuta IMM-urile să respecte RGPD, de exemplu, prin furnizarea de modele de contracte de prelucrare și de evidențe ale activităților de prelucrare, de seminare și de linii de asistență telefonică pentru consultare. Unele dintre aceste inițiative au beneficiat de fonduri din partea UE[50]. Ar trebui luate în considerare și alte activități pentru a facilita aplicarea RGPD de către IMM-uri.

RGPD pune la dispoziția tuturor tipurilor de întreprinderi și organizații un set de instrumente care să le ajute să demonstreze conformitatea, cum ar fi coduri de conduită, mecanisme de certificare și clauze contractuale standard. Acest set de instrumente ar trebui să fie utilizat pe deplin. IMM-urile subliniază în special importanța și utilitatea codurilor de conduită, care sunt adaptate situației lor și care nu implică costuri disproporționate. În ceea ce privește schemele de certificare, securitatea (inclusiv securitatea cibernetică) și protecția datelor începând cu momentul conceperii sunt elemente-cheie care trebuie luate în considerare în cadrul RGPD și care ar beneficia de o abordare comună și ambițioasă în întreaga UE. În prezent, Comisia lucrează la elaborarea unor clauze contractuale standard între operatori și

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

[49] A se vedea punctul 5 din documentul de lucru al serviciilor Comisiei. A se vedea, de asemenea, COM/2019/250 final - Orientări referitoare la Regulamentul privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană, care explică regulile ce reglementează prelucrarea seturilor de date mixte, compuse atât din date cu caracter personal, cât și din date fără caracter personal, facilitând prelucrarea practică de către întreprinderi, inclusiv IMM-uri.

[50] Comisia a oferit sprijin financiar prin granturi organizate în trei etape, în valoare totală de 5 milioane EUR, cele mai recente două astfel de etape vizând în special sprijinirea autorităților naționale pentru protecția datelor în eforturile lor de a interacționa cu persoanele fizice și cu IMM-urile: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en. În 2020 vor mai fi alocați încă 1 milion EUR.

persoanele împuternicite de către operatori[51], pornind de la eforturile în curs privind modernizarea clauzelor contractuale standard pentru transferurile internaționale[52].

Aplicarea RGPD în cazul noilor tehnologii

Întrucât a fost conceput într-un mod neutru din punct de vedere tehnologic, RGPD are la bază principii și este, prin urmare, proiectat pentru a acoperi noile tehnologii pe măsură ce acestea se dezvoltă.

RGPD este considerat un instrument esențial și flexibil al cărui obiectiv este de a se asigura că dezvoltarea noilor tehnologii respectă drepturile fundamentale. Protecția datelor și cadrul legislativ privind viața privată și-au dovedit importanța și flexibilitatea în cursul crizei cauzate de pandemia de COVID-19, în special în ceea ce privește proiectarea aplicațiilor de depistare a contacților și a altor soluții tehnologice pentru combaterea pandemiei. Viitoarele provocări vizează clarificarea modului în care principiile consacrate se pot aplica tehnologiilor specifice, cum ar fi inteligența artificială, tehnologia blockchain, internetul obiectelor sau recunoașterea facială, care necesită o monitorizare continuă. Cartea albă a Comisiei privind inteligența artificială[53], de exemplu, a deschis o dezbatere publică cu privire la circumstanțele specifice, după caz, care ar putea justifica folosirea inteligenței artificiale pentru identificarea la distanță a datelor biometrice (cum ar fi recunoașterea facială) în locuri publice, precum și cu privire la garanții comune. În acest sens, autoritățile pentru protecția datelor ar trebui să fie pregătite să sprijine procesele de proiectare tehnică în etapa inițială.

Mai mult, aplicarea fermă și eficace a RGPD în ceea ce privește platformele digitale de mari dimensiuni și companiile integrate, inclusiv în domenii precum publicitatea online și adresarea de conținut personalizat, reprezintă un element esențial pentru protejarea persoanelor.

Elaborarea unui set de instrumente modern pentru transferul internațional de date

RGPD oferă un set de instrumente modernizat pentru a facilita transferul de date cu caracter personal din UE către o țară terță sau o organizație internațională, asigurându-se în același timp faptul că datele continuă să beneficieze de un nivel ridicat de protecție. În ultimii doi ani, Comisia și-a intensificat activitatea pentru a valorifica întregul potențial al instrumentelor disponibile în cadrul RGPD.

Acest lucru a inclus colaborarea activă cu partenerii-cheie în vederea luării unei „decizii privind caracterul adecvat”. Efectul unei astfel de decizii este de a permite fluxul sigur și liber de date cu caracter personal către țara terță în cauză, fără a fi necesar ca exportatorul de date să ofere garanții suplimentare sau să obțină o autorizație. În special, deciziile reciproce privind caracterul adecvat între UE și Japonia, care au intrat în vigoare în februarie 2019, au creat cel mai mare spațiu de fluxuri gratuite și sigure de date din lume. Mai mult, procesul de evaluare a caracterului adecvat cu Republica Coreea se află într-un stadiu avansat și sunt în curs discuții preliminare și cu alți parteneri importanți din Asia și America Latină.

[51] În temeiul articolului 28 din RGPD.
[52] În temeiul articolului 46 din RGPD.
[53] Cartea albă „Inteligența artificială - O abordare europeană axată pe excelență și încredere” - COM/2020/65 final.

Caracterul adecvat joacă, de asemenea, un rol important în contextul relațiilor viitoare cu Regatul Unit, dacă sunt îndeplinite condițiile relevante. Acesta constituie un factor favorizant pentru comerț, inclusiv pentru comerțul digital, și o precondiție esențială pentru o cooperare strânsă și ambițioasă în domeniul aplicării legii și al securității. Mai mult, un grad ridicat de convergență în domeniul protecției datelor reprezintă un element important pentru asigurarea unor condiții de concurență egale între două economii atât de bine integrate. În conformitate cu Declarația politică de stabilire a cadrului viitoarelor relații dintre Uniunea Europeană și Regatul Unit, Comisia efectuează în prezent o evaluare a caracterului adecvat atât în temeiul RGPD, cât și al Directivei privind protecția datelor în materie de asigurare a respectării legii[54].

În cadrul primei evaluări a RGPD, Comisia are obligația să revizuiască deciziile privind caracterul adecvat adoptate în conformitate cu normele anterioare[55]. Serviciile Comisiei s-au implicat într-un dialog intens cu fiecare dintre cele 11 țări și teritorii terțe vizate[56] pentru a evalua modul în care sistemele lor de protecție a datelor au evoluat de la adoptarea deciziei privind caracterul adecvat și a determina dacă acestea respectă standardele stabilite în RGPD. Necesitatea de a asigura continuitatea acestor decizii, ca instrument esențial pentru cooperarea comercială și internațională, reprezintă unul dintre factorii care au determinat mai multe astfel de țări și teritorii să își modernizeze și să își consolideze legile privind viața privată. Cu unele dintre aceste țări și teritorii sunt discutate garanții suplimentare pentru a rezolva diferențele relevante în materie de protecție. Cu toate acestea, având în vedere că este posibil ca, printr-o hotărâre pronunțată la 16 iulie, Curtea de Justiție să ofere clarificări care ar putea fi relevante pentru anumite elemente ale standardului privind caracterul adecvat, Comisia va elabora un raport separat cu privire la evaluarea deciziilor privind caracterul adecvat existente după ce Curtea de Justiție își va fi pronunțat hotărârea în cauza respectivă[57].

Pe lângă activitatea privind caracterul adecvat, Comisia lucrează la o modernizare completă a clauzelor contractuale standard, pentru a le actualiza în conformitate cu noile cerințe introduse de RGPD. Scopul este de a reflecta mai bine realitățile operațiunilor de prelucrare în economia digitală modernă și de a lua în considerare eventuala necesitate, inclusiv în lumina jurisprudenței viitoare a Curții de Justiție, de a clarifica anumite măsuri de protecție[58]. Aceste clauze reprezintă, de departe, mecanismul de transfer de date utilizat cel mai des, mii de întreprinderi din UE

---

[54] Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, JO L 119, 4.5.2016, p. 89.

[55] Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, JO L 281, 23.11.1995, p. 31.

[56] Aceste țări și teritorii sunt: Andorra, Argentina, Canada, Insulele Feroe, Guernsey, Jersey, Insula Man, Israel, Noua Zeelandă, Elveția și Uruguay.

[57] A se vedea cauza C-311/18, Data Protection Commissioner/Facebook Ireland Limited, Maximillian Schrems („Schrems II”), care se referă la o trimitere preliminară privind așa-numitele clauze contractuale standard. Cu toate acestea, este posibil ca și anumite elemente ale standardului privind caracterul adecvat să fie clarificate de Curte.

[58] A se vedea cauza Schrems II.

bazându-se pe ele în scopul de a le oferi o gamă largă de servicii clienților, furnizorilor, partenerilor și angajaților lor.

Comitetul a jucat, de asemenea, un rol activ în dezvoltarea aspectelor internaționale ale RGPD. Este vorba, printre altele, de actualizarea orientărilor privind mecanismele existente de transfer, cum ar fi normele corporative obligatorii și așa-numitele „derogări", precum și de dezvoltarea infrastructurii juridice pentru utilizarea noilor instrumente introduse de RGPD, și anume, codurile de conduită și certificarea.

Pentru a le permite părților interesate să utilizeze pe deplin setul de instrumente de transfer prevăzute în RGPD, este important ca comitetul să își intensifice activitatea în curs cu privire la diferitele mecanisme de transfer, inclusiv prin simplificarea în continuare a procesului de aprobare pentru normele corporative obligatorii, prin finalizarea orientărilor privind codurile de conduită și certificare ca instrumente de transfer și prin clarificarea interacțiunii dintre normele privind transferurile internaționale de date (capitolul V) și domeniul de aplicare teritorial al RGPD (articolul 3).

Un alt aspect important al dimensiunii internaționale a normelor UE de protecție a datelor este domeniul de aplicare teritorial extins al RGPD, care acoperă și activitățile de prelucrare ale operatorilor străini care desfășoară activități pe piața UE. Pentru a se asigura respectarea efectivă a RGPD și a se crea condiții de concurență cu adevărat echitabile, este esențial ca această extindere să fie reflectată în mod adecvat în acțiunile de aplicare a legii ale autorităților pentru protecția datelor. Acestea ar trebui, în special, să implice, după caz, reprezentantul din Uniunea Europeană al operatorului sau al persoanei împuternicite de către operator, care poate fi abordat pe lângă sau în locul întreprinderii cu sediul în afara UE. Această abordare ar trebui să fie aplicată cu mai multă rigurozitate, pentru a transmite un mesaj clar că lipsa unui sediu în UE nu scutește operatorii străini de responsabilitățile care le revin în temeiul RGPD.

Promovarea convergenței și a cooperării internaționale în domeniul protecției datelor

RGPD s-a dovedit deja a fi un punct de referință esențial la nivel internațional și a acționat ca un catalizator pentru multe țări din întreaga lume, care au luat astfel în considerare introducerea unor norme moderne privind viața privată. Această tendință către o convergență globală este o evoluție pozitivă care aduce noi oportunități de a proteja mai bine persoanele fizice din UE atunci când datele lor sunt transferate în străinătate, facilitând, în același timp, fluxurile de date.

Pornind de la această tendință, Comisia și-a intensificat dialogurile purtate într-o serie de forumuri bilaterale, regionale și multilaterale pentru a încuraja o cultură globală a respectării vieții private și a dezvolta elemente de convergență între sisteme diferite de protecție a vieții private. În eforturile sale, Comisia s-a bazat și va continua să se bazeze pe sprijinul activ al Serviciului European de Acțiune Externă, al rețelei de delegații UE din țările terțe și al misiunilor pe lângă organizațiile internaționale. Acest lucru a permis, de asemenea, o mai mare consecvență și complementaritate între diferite aspecte ale dimensiunii externe a politicilor UE - de la comerț la noul parteneriat UE-Africa. Totodată, G20 și G7 au recunoscut recent contribuția protecției

datelor la încrederea în economia digitală și în fluxurile de date, în special prin conceptul de „Data Free Flow with Trust”, propus inițial de președinția japoneză a G20[59]. Strategia privind datele evidențiază intenția Comisiei de a continua să promoveze schimbul de date cu parteneri fiabili, combătând în același timp abuzurile, cum ar fi accesul disproporționat al autorităților publice (străine) la datele cu caracter personal.

Comisia promovează convergența standardelor de protecție a datelor la nivel internațional, ca modalitate de a facilita fluxurile de date și, prin urmare, comerțul, dar este hotărâtă să abordeze, în același timp, și protecționismul digital, astfel cum a fost evidențiat recent în Strategia privind datele[60]. În acest scop, Comisia a elaborat dispoziții specifice privind fluxurile de date și protecția datelor în acordurile comerciale[61], pe care le înscrie sistematic pe agenda negocierilor bilaterale - cel mai recent cu Australia, Noua Zeelandă și Regatul Unit - și multilaterale, cum ar fi actualele discuții privind comerțul electronic din cadrul OMC[62]. Aceste dispoziții orizontale exclud restricțiile nejustificate, precum cerințele de localizare forțată a datelor, păstrând în același timp autonomia în materie de reglementare a părților, pentru a proteja dreptul fundamental la protecția datelor.

Sinergiile dintre comerț și instrumentele de protecție a datelor ar trebui să fie analizate în continuare, pentru a se asigura fluxuri internaționale libere și sigure de date, care sunt esențiale pentru operațiunile comerciale, pentru competitivitate și pentru creșterea întreprinderilor europene, inclusiv a IMM-urilor, într-o economie din ce în ce mai digitalizată.

În mod similar, este important să se asigure faptul că, atunci când societăților care desfășoară activități pe piața europeană li se solicită, pe baza unei cereri legitime, să comunice date în scopul aplicării legii, acestea pot face acest lucru fără să se confrunte cu conflicte de legi și cu respectarea deplină a drepturilor fundamentale ale UE. Pentru a îmbunătăți aceste transferuri, Comisia se angajează să dezvolte cadre juridice adecvate cu partenerii săi internaționali pentru a evita conflictele de legi și a sprijini formele de cooperare eficace, în special prin asigurarea garanțiilor necesare pentru protecția datelor, contribuind astfel la combaterea cu mai multă eficacitate a criminalității.

În sfârșit, într-un moment în care problemele legate de respectarea vieții private sau incidentele de securitate a datelor pot afecta simultan un număr mare de persoane din mai multe jurisdicții, cooperarea „pe teren” dintre autoritățile de reglementare europene și internaționale ar trebui să fie consolidată în continuare. În mod concret, este necesar să se elaboreze instrumente juridice adecvate pentru forme mai strânse de

---

[59] A se vedea, de exemplu, textul Declarației liderilor G20 de la Osaka: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[60] Strategia privind datele, p. 23.

[61] A se vedea textul dispozițiilor orizontale privind fluxurile transfrontaliere de date și protecția datelor cu caracter personal (în acordurile comerciale și de investiții ale UE): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

[62] 84 de membri ai OMC sunt implicați în prezent în negocieri plurilaterale privind comerțul electronic, în urma unei inițiative de declarație comună, adoptată de miniștri la 25 ianuarie 2019 la Davos. În cadrul acestui proces, UE a prezentat, la data de 3 mai 2019, o propunere de text referitoare la normele și obligațiile viitoare privind comerțul electronic. Propunerea include dispoziții orizontale privind fluxurile de date și protecția datelor cu caracter personal: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

cooperare și asistență reciprocă, inclusiv prin permiterea schimburilor de informații necesare în contextul anchetelor. Tot în acest spirit, Comisia va înființa o „Academie de protecție a datelor”, o platformă prin intermediul căreia autoritățile pentru protecția datelor din UE și străine ar face schimb de cunoștințe, de experiență și de bune practici pentru a facilita și a sprijini cooperarea dintre autoritățile de aplicare a legii din domeniul protecției vieții private.

3 CALEA DE URMAT

Pentru a beneficia de întregul potențial al RGPD, este important să existe o abordare armonizată și o cultură europeană comună de protecție a datelor, precum și să se promoveze o gestionare mai eficientă și mai armonizată a cazurilor transfrontaliere. Această abordare este așteptată de cetățeni și de întreprinderi și constituie un obiectiv esențial al reformei normelor UE de protecție a datelor. Este la fel de important să se garanteze că toate instrumentele disponibile în RGPD sunt utilizate pe deplin pentru a se asigura o aplicare eficientă, în beneficiul persoanelor fizice și al întreprinderilor.

Comisia va continua schimburile bilaterale cu statele membre în ceea ce privește punerea în aplicare a RGPD și, dacă este necesar, va continua să utilizeze toate instrumentele de care dispune pentru a promova respectarea de către statele membre a obligațiilor care le revin în cadrul RGPD.

Având în vedere evaluarea continuă a legislației naționale, perioada scurtă de experiență practică de când RGPD a devenit aplicabil, precum și faptul că legislația specifică acestui sector este încă în curs de revizuire în multe state membre, este prematur să se tragă concluzii definitive cu privire la nivelul de fragmentare existent. În ceea ce privește eventualul conflict de legi rezultat în urma punerii în aplicare de către statele membre a unor clauze de specificare, este necesar mai întâi să se înțeleagă mai bine consecințele asupra operatorilor și asupra persoanelor împuternicite de către operatori[63].

În cadrul monitorizării acestor aspecte, jurisprudența relevantă a instanțelor naționale și a Curții de Justiție contribuie la o interpretare consecventă a normelor de protecție a datelor. Instanțele naționale au emis recent hotărâri care invalidează anumite dispoziții din legile naționale care se abat de la prevederile RGPD[64].

În ceea ce privește dimensiunea internațională, Comisia va continua să se concentreze pe promovarea convergenței normelor de protecție a datelor ca modalitate de a asigura fluxuri de date sigure. Sunt incluse aici diferite forme de activități „în amonte”, de exemplu, în contextul reformelor în curs pentru adoptarea de acte legislative noi sau actualizate privind protecția datelor ori al promovării conceptului de „Data Free Flow with Trust” în forumurile multilaterale. Acest demers acoperă, de asemenea, diverse dialoguri privind caracterul adecvat și modernizarea, precum și extinderea setului de instrumente privind transferul de care dispunem, prin actualizarea clauzelor contractuale standard și prin punerea bazelor pentru mecanismele de certificare. La acestea se adaugă negocierile internaționale, de exemplu în domeniul accesului

[63] Cf. poziția și constatările Consiliului privind aplicarea RGPD.
[64] Acest lucru s-a întâmplat în Germania și în Spania, precum și în Austria, unde a fost acoperită o lacună existentă în legislația națională.

transfrontalier la probe electronice, pentru a se asigura că transferurile de date se vor desfășura cu garanții adecvate de protecție a datelor. În cele din urmă, prin participarea la negocieri cu privire la cooperarea internațională și acordarea de asistență reciprocă între autoritățile pentru protecția datelor, Comisia va depune eforturi pentru a transfera convergența din teorie în practică.

Pe baza acestei evaluări a aplicării RGPD din luna mai 2018 până în prezent, acțiunile enumerate mai jos au fost identificate ca fiind necesare pentru a sprijini aplicarea regulamentului. Comisia va monitoriza punerea lor în aplicare, inclusiv în perspectiva următorului raport de evaluare din 2024.

Punerea în aplicare și completarea cadrului juridic

Statele membre ar trebui:

- să finalizeze alinierea legislației lor sectoriale la RGPD;
- să ia în considerare limitarea utilizării clauzelor de specificare susceptibile să cauzeze o fragmentare și să pună în pericol libera circulație a datelor în cadrul UE;
- să evalueze dacă legislația națională de punere în aplicare a RGPD se situează, în toate privințele, în limitele prevăzute de legislația statului membru.

Comisia:

- va continua schimburile bilaterale cu statele membre cu privire conformitatea legislației naționale cu RGPD, inclusiv în ceea ce privește independența și resursele autorităților naționale pentru protecția datelor; va utiliza toate instrumentele de care dispune, inclusiv procedurile de constatare a încălcării obligațiilor, pentru a se asigura că statele membre respectă RGPD;
- va susține în continuare schimbul de opinii și de practici naționale între statele membre pe teme care fac obiectul unei specificări suplimentare la nivel național, astfel încât să se reducă gradul de fragmentare a pieței unice, cum ar fi prelucrarea datelor cu caracter personal referitoare la sănătate și în contextul cercetării, sau pentru care trebuie asigurat un echilibru cu alte drepturi, cum ar fi libertatea de exprimare;
- va sprijini o aplicare consecventă a cadrului de protecție a datelor în raport cu noile tehnologii, pentru a sprijini inovațiile și evoluțiile tehnologice;
- va utiliza Grupul de experți al statelor membre privind RGPD (înființat în etapa de tranziție, înainte de intrarea în vigoare a RGPD) pentru a facilita discuțiile și schimbul de experiență între statele membre și cu Comisia;
- va analiza dacă, în lumina unor experiențe ulterioare și a jurisprudenței relevante, ar putea fi oportună propunerea în viitor a unor eventuale modificări direcționate ale anumitor dispoziții din RGPD, în special în ceea ce privește evidențele activităților de prelucrare ale IMM-urilor a căror activitate principală nu este prelucrarea datelor cu caracter personal (risc redus)[65],

[65] Articolul 30 alineatul (5) din RGPD.

precum și posibila armonizare a vârstei de la care copii își pot da consimțământul în ceea ce privește serviciile societății informaționale.

Utilizarea întregului potențial al noului sistem de guvernanță

Comitetul și autoritățile pentru protecția datelor sunt invitate:

- să instituie modalități de lucru eficiente între autoritățile pentru protecția datelor privind funcționarea mecanismelor de cooperare și coerență, inclusiv privind aspectele procedurale, pornind de la experiența propriilor membri și prin intensificarea implicării secretariatului;
- să sprijine armonizarea în ceea ce privește aplicarea și asigurarea respectării RGPD, recurgând la toate mijloacele disponibile, inclusiv prin clarificarea în continuare a conceptelor-cheie ale RGPD, și asigurându-se că orientările naționale sunt pe deplin conforme cu orientările adoptate de comitet;
- să încurajeze utilizarea tuturor instrumentelor prevăzute în RGPD pentru a se asigura că acesta este aplicat în mod consecvent;
- să intensifice cooperarea dintre autoritățile pentru protecția datelor, de exemplu, prin efectuarea de anchete comune.

Comisia:

- va continua să monitorizeze îndeaproape independența efectivă și deplină a autorităților naționale pentru protecția datelor;
- va încuraja cooperarea dintre autoritățile de reglementare (în special în domenii precum concurența, comunicațiile electronice, securitatea rețelelor și a sistemelor informatice și politica de protecție a consumatorilor);
- va sprijini procesul de reflecție din cadrul comitetului cu privire la procedurile aplicate de autoritățile naționale pentru protecția datelor, pentru a îmbunătăți cooperarea privind cazurile transfrontaliere.

Statele membre:

- vor aloca suficiente resurse autorităților pentru protecția datelor, astfel încât acestea să își poată îndeplini sarcinile.

Sprijinirea părților interesate

Comitetul și autoritățile pentru protecția datelor sunt invitate:

- să adopte orientări suplimentare care să fie practice, ușor de înțeles și care să ofere răspunsuri clare și să evite ambiguitățile cu privire la problemele legate de aplicarea RGPD, de exemplu cu privire la prelucrarea datelor copiilor și drepturile persoanelor vizate, inclusiv exercitarea dreptului de acces și a dreptului la ștergerea datelor, cu consultarea părților interesate care sunt implicate în acest proces;
- să revizuiască orientările atunci când sunt necesare clarificări suplimentare având în vedere experiența dobândită și evoluțiile înregistrate, inclusiv în jurisprudența Curții de Justiție;

- să elaboreze instrumente practice, de exemplu formulare armonizate pentru încălcările securității datelor și evidențe simplificate ale activităților de prelucrare, pentru a ajuta IMM-urile cu risc scăzut să își îndeplinească obligațiile.

Comisia:

- va furniza clauze contractuale standard atât pentru transferurile internaționale, cât și pentru relația dintre operator și persoana împuternicită de către operator;
- va furniza instrumente care să clarifice/să sprijine aplicarea normelor de protecție în cazul copiilor[66];
- în conformitate cu strategia privind datele, va analiza mijloacele practice de a facilita utilizarea sporită a dreptului la portabilitate de către persoanele fizice, de exemplu, oferindu-le mai mult control asupra entităților care pot accesa și utiliza datele generate automat;
- va sprijini standardizarea/certificarea, în special cu privire la aspecte de securitate cibernetică, prin cooperarea dintre Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), autoritățile pentru protecția datelor și comitet;
- dacă este cazul, se va prevala de dreptul său de a solicita comitetului să elaboreze orientări și avize cu privire la probleme specifice care prezintă importanță pentru părțile interesate;
- atunci când este necesar, va elabora orientări, respectând pe deplin rolul comitetului;
- va sprijini activitățile autorităților de protecție a datelor care facilitează punerea în aplicare de către IMM-uri a obligațiilor impuse prin RGPD, prin acordarea de sprijin financiar, în special pentru orientări practice și instrumente digitale care pot fi reproduse și în alte state membre.

Încurajarea inovării

Comisia:

- va monitoriza aplicarea RGPD în cazul noilor tehnologii, ținând cont și de eventualele inițiative viitoare adoptate în domeniul inteligenței artificiale și în cadrul strategiei privind datele;
- va încuraja, inclusiv prin sprijin financiar, elaborarea codurilor de conduită ale UE în domeniul sănătății și al cercetării;
- va urmări îndeaproape dezvoltarea și utilizarea aplicațiilor în contextul pandemiei de COVID-19.

[66] Proiect al Comisiei privind instrumentele de identificare a vârstei – proiect-pilot pentru demonstrarea unei infrastructuri tehnice interoperabile pentru protecția copiilor, inclusiv verificarea vârstei și acordul părinților. Se preconizează că acesta va sprijini punerea în aplicare a mecanismelor de protecție a copiilor bazate pe legislația UE în vigoare care prezintă relevanță pentru protecția copiilor în mediul online.

Comitetul este invitat:

- să elaboreze orientări privind aplicarea RGPD în domeniul cercetării științifice, al inteligenței artificiale, al tehnologiei blockchain și al altor eventuale evoluții tehnologice;
- să revizuiască orientările atunci când sunt necesare clarificări suplimentare ca urmare a evoluțiilor tehnologice.

Dezvoltarea în continuare a setului de instrumente pentru transferurile de date

Comisia:

- va continua dialogurile privind caracterul adecvat cu țările terțe interesate, în conformitate cu strategia prezentată în Comunicarea sa din 2017 intitulată „Schimbul de date cu caracter personal și protecția acestora într-o lume globalizată”, inclusiv, după caz, prin acoperirea transferurilor de date către autoritățile de aplicare a legislației în materie penală (în conformitate cu Directiva privind protecția datelor în materie de asigurare a respectării legii) și către alte autorități publice; este inclusă aici și finalizarea, cât mai curând posibil, a procesului de evaluare a caracterului adecvat cu Republica Coreea;
- va finaliza evaluarea în curs a deciziilor existente privind caracterul adecvat și va informa Parlamentul European și Consiliul;
- va finaliza activitatea de modernizare a clauzelor contractuale standard, în vederea actualizării acestora în funcție de RGPD, acoperind toate scenariile de transfer relevante și reflectând mai bine practicile comerciale moderne.

Comitetul este invitat:

- să clarifice în continuare interacțiunea dintre normele privind transferurile internaționale de date (capitolul V) și domeniul de aplicare teritorial al RGPD (articolul 3);
- să asigure respectarea efectivă a legii de către operatorii cu sediul în țări terțe care intră în domeniul de aplicare teritorial al RGPD, inclusiv în ceea ce privește numirea unui reprezentant, dacă este cazul (articolul 27);
- să simplifice evaluarea și eventuala aprobare a normelor corporative obligatorii, cu scopul de a accelera procesul;
- să finalizeze activitatea privind arhitectura, procedurile și criteriile de evaluare pentru codurile de conduită și mecanismele de certificare ca instrumente pentru transferurile de date.

Promovarea convergenței și dezvoltarea cooperării internaționale

Comisia:

- va sprijini procesele de reformă în curs din țările terțe cu privire la normele noi sau modernizate de protecție a datelor, prin schimburi de experiență și de bune practici;

- se va implica în relațiile cu partenerii africani pentru a promova convergența normativă și pentru a sprijini consolidarea capacității autorităților de supraveghere în cadrul capitolului digital al noului parteneriat UE-Africa;
- va evalua modul în care ar putea fi facilitată cooperarea dintre operatorii privați și autoritățile de aplicare a legii, inclusiv prin negocierea unor cadre bilaterale și multilaterale pentru transferurile de date în contextul accesului autorităților străine de aplicare a legii în materie penală la probele electronice, pentru a se evita conflictele de legi, asigurându-se în același timp garanții adecvate pentru protecția datelor;
- se va implica în relațiile cu organizații regionale și internaționale, cum ar fi OCDE, ASEAN sau G20, pentru a promova fluxurile de date de încredere bazate pe standarde ridicate de protecție a datelor, inclusiv în contextul inițiativei „Data Flow with Trust initiative”;
- va înființa o „Academie de protecție a datelor” pentru a facilita și a sprijini schimburile dintre autoritățile de reglementare europene și internaționale;
- va promova cooperarea internațională în materie de aplicare între autoritățile de supraveghere, inclusiv prin negocierea unor acorduri de cooperare și asistență reciprocă.