Consiliul
Uniunii Europene

Bruxelles, 22 ianuarie 2024
(OR. en)

5454/24

DATAPROTECT 23
JAI 62
RELEX 42

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Destinatar:	Dna Thérèse BLANCHET, Secretară Generală a Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2024) 7 final
Subiect:	RAPORT AL COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU privind prima revizuire a funcționării deciziilor privind caracterul adecvat al nivelului de protecție care au fost adoptate în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE

În anexă, se pune la dispoziția delegațiilor documentul COM(2024) 7 final.

Anexă: COM(2024) 7 final

COMISIA
EUROPEANĂ

Bruxelles, 15.1.2024
COM(2024) 7 final

RAPORT AL COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

privind prima revizuire a funcționării deciziilor privind caracterul adecvat al nivelului de protecție care au fost adoptate în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE

{SWD(2024) 3 final}

1. PRIMA REVIZUIRE – ISTORIC ȘI CONTEXT

Prezentul raport cuprinde constatările Comisiei referitoare la prima revizuire a deciziilor privind caracterul adecvat al nivelului de protecție care au fost adoptate în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE[1] (Directiva privind protecția datelor).

În aceste decizii, Comisia a stabilit că 11 țări sau teritorii asigură un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniunea Europeană (UE)[2]: Andorra[3], Argentina[4], Canada (pentru operatorii comerciali)[5], Insulele Feroe[6], Guernsey[7], Insula Man[8], Israel[9], Jersey[10], Noua Zeelandă[11], Elveția[12] și Uruguay[13]. Prin urmare, transferurile de date din UE către aceste țări sau teritorii pot avea loc fără impunerea unor cerințe suplimentare.

Odată cu intrarea în vigoare a Regulamentului (UE) 2016/679[14] (RGPD) la 25 mai 2018, deciziile privind caracterul adecvat adoptate în temeiul Directivei privind protecția datelor au

[1] 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.

[2] În urma încorporării sale în Acordul privind Spațiul Economic European (SEE), RGPD se aplică și Norvegiei, Islandei și Liechtensteinului. Trimiterile la UE din prezentul raport trebuie înțelese ca incluzând și statele SEE.

[3] Decizia 2010/625/UE a Comisiei din 19 octombrie 2010 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind nivelul adecvat de protecție a datelor cu caracter personal în Andorra, JO L 277, 21.10.2010, p. 27.

[4] Decizia 2003/490/CE a Comisiei din 30 iunie 2003 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind nivelul adecvat de protecție a datelor cu caracter personal în Andorra, JO L 168, 5.7.2003, p. 19.

[5] Decizia 2002/2/CE a Comisiei din 20 decembrie 2001 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției datelor cu caracter personal asigurat prin legea canadiană referitoare la protecția informațiilor cu caracter personal și documentele electronice (Personal Information Protection and Electronic Documents Act), JO L 2, 4.1.2002, p. 13.

[6] Decizia 2010/146/UE a Comisiei din 5 martie 2010 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind nivelul de protecție adecvat asigurat de Legea feroeză privind prelucrarea datelor cu caracter personal, JO L 58, 9.3.2010, p. 17.

[7] Decizia 2003/821/CE a Comisiei din 21 noiembrie 2003 privind nivelul adecvat de protecție a datelor cu caracter personal în Guernsey, JO L 308, 25.11.2003, p. 27.

[8] Decizia 2004/411/CE a Comisiei din 28 aprilie 2004 de constatare a nivelului adecvat de protecție a datelor cu caracter personal pe Insula Man, JO L 151, 30.4.2004, p. 48.

[9] Decizia 2011/61/UE a Comisiei din 31 ianuarie 2011 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind nivelul de protecție adecvat asigurat de Statul Israel privind prelucrarea automată a datelor cu caracter personal, JO L 27, 1.2.2011, p. 39.

[10] Decizia 2008/393/CE a Comisiei din 8 mai 2008 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind nivelul de protecție adecvat a datelor cu caracter personal în Jersey, JO L 138, 28.5.2008, p. 21.

[11] Decizia de punere în aplicare 2013/65/UE a Comisiei din 19 decembrie 2012 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind nivelul adecvat de protecție a datelor cu caracter personal asigurat de Noua Zeelandă, JO L 28, 30.1.2013, p. 12.

[12] Decizia 2000/518/CE a Comisiei din 26 iulie 2000 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind protecția adecvată a datelor cu caracter personal în Elveția, JO L 215, 25.8.2000, p. 1.

[13] Decizia de punere în aplicare 2012/484/UE a Comisiei din 21 august 2012 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind nivelul de protecție adecvat asigurat de Republica Orientală a Uruguayului privind prelucrarea automată a datelor cu caracter personal, JO L 227, 23.8.2012, p. 11.

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

rămas în vigoare[15]. În același timp, RGPD a clarificat faptul că constatările privind caracterul adecvat al nivelului de protecție sunt „instrumente vii”, stipulând obligația Comisiei de a monitoriza în permanență evoluțiile din țările terțe care ar putea afecta funcționarea deciziilor existente privind caracterul adecvat al nivelului de protecție[16]. În plus, articolul 97 din RGPD impune Comisiei să revizuiască periodic aceste decizii, o dată la patru ani, pentru a stabili dacă țările și teritoriile în privința cărora s-a constatat caracterul adecvat asigură în continuare un nivel adecvat de protecție a datelor cu caracter personal.

Această primă revizuire a deciziilor privind caracterul adecvat al nivelului de protecție adoptate în temeiul fostului cadru al UE privind protecția datelor a fost inițiată ca parte a unei evaluări mai ample a aplicării și funcționării RGPD, cu privire la care Comisia și-a prezentat constatările în Comunicarea sa intitulată „Protecția datelor ca pilon al capacitării cetățenilor și al abordării UE privind tranziția digitală - doi ani de aplicare a Regulamentului general privind protecția datelor”[17]. Cu toate acestea, finalizarea acestui aspect al reexaminării a fost amânată pentru a se ține seama de hotărârea Curții de Justiție în cauza Schrems II[18], în care Curtea a oferit clarificări importante cu privire la elementele-cheie ale standardului privind nivelul de adecvare, precum și la alte evoluții conexe. La rândul său, acest lucru a condus la schimburi detaliate cu țările și teritoriile în cauză cu privire la aspectele relevante ale cadrului juridic, ale mecanismelor de supraveghere și ale sistemului lor de asigurare a respectării legii[19]. Prezentul raport ține seama pe deplin de toate aceste evoluții, atât în UE, cât și în țările și teritoriile terțe în cauză.

Este important de remarcat faptul că această primă revizuire are loc în contextul dezvoltării exponențiale a tehnologiilor digitale. În ultimele decenii, importanța deciziilor privind caracterul adecvat al nivelului de protecție a crescut considerabil, întrucât fluxurile de date au devenit un element integrant al transformării digitale a societății și al globalizării economiei. Transferul de date la nivel transfrontalier a devenit parte a operațiunilor zilnice ale întreprinderilor europene de toate dimensiunile, în toate sectoarele. Mai mult ca niciodată, respectarea vieții private este o condiție pentru fluxuri comerciale stabile, sigure și competitive. În acest context, deciziile privind caracterul adecvat al nivelului de protecție joacă un rol din ce în ce mai important, în multe privințe. Prin asigurarea faptului că protecția

[15] A se vedea articolul 45 alineatul (9) din RGPD, care prevede că deciziile adoptate de Comisie în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE rămân în vigoare până când sunt modificate, înlocuite sau abrogate de o decizie a Comisiei adoptată în conformitate cu articolul 45 alineatul (3) sau (5).

[16] Articolul 45 alineatul (4) din RGPD. A se vedea și hotărârea Curții de Justiție a UE din 6 octombrie 2015 în cauza C-362/14, Maximillian Schrems/Data Protection Commissioner (hotărârea în cauza Schrems I), ECLI:EU:C:2015:650, punctul 76.

[17] Comunicarea a fost publicată în iunie 2020 și este disponibilă la următoarea adresă: https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en.

[18] Hotărârea Curții de Justiție a UE din 16 iulie 2020 în cauza C-311/18, Data Protection Commissioner/Facebook Ireland Ltd. și Maximilian Schrems (hotărârea în cauza Schrems II), ECLI:EU:C:2020:559.

[19] Decizia privind caracterul adecvat al nivelului de protecție în ceea ce privește Japonia a fost adoptată pe baza RGPD și prevede o revizuire periodică separată. Prima revizuire s-a încheiat în aprilie 2023 cu Raportul Comisiei către Parlamentul European și Consiliu referitor la prima revizuire a funcționării deciziei privind caracterul adecvat al nivelului de protecție asigurat de Japonia, COM(2023) 275 final, document disponibil la următorul link https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=COM:2023:275:FIN.

însoțește datele, aceste decizii permit fluxuri de date sigure, respectând drepturile persoanelor, în conformitate cu abordarea UE centrată pe factorul uman a transformării digitale. Prin recunoașterea cadrului de protecție a vieții private al unei țări terțe care oferă un nivel de protecție în esență echivalent cu cel al UE, acestea promovează convergența între sistemele de protecție a vieții private bazate pe standarde ridicate de protecție. În plus, astfel cum se explică în prezentul raport, în loc să fie un „punct final", deciziile privind caracterul adecvat al nivelului de protecție au pus bazele unei cooperări mai strânse și ale unei convergențe sporite în materie de reglementare între UE și partenerii care împărtășesc aceeași viziune. 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, precum și prin facilitarea cooperării cu partenerii străini într-o gamă largă de domenii de reglementare. Prin furnizarea unei soluții simple și cuprinzătoare pentru transferurile de date, fără a fi necesar ca exportatorul de date să ofere garanții suplimentare sau să obțină vreo autorizație, acestea facilitează respectarea, în special de către întreprinderile mici și mijlocii, a cerințelor privind transferurile internaționale prevăzute în RGPD. În final, 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 nu numai libera circulație a datelor în cele 30 de economii ale UE, ci și în multe alte jurisdicții din întreaga lume[20] 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.

Din toate aceste motive, astfel cum s-a confirmat, de asemenea, prin dialogul intens și fructuos cu țările/teritoriile terțe în cauză care stă la baza prezentei revizuiri, deciziile privind caracterul adecvat al nivelului de protecție au devenit o componentă strategică a relației globale a UE cu acești parteneri străini și sunt recunoscute ca fiind un catalizator major pentru aprofundarea cooperării într-o gamă largă de domenii. Prin urmare, este deosebit de important ca aceste decizii să poată trece testul timpului și să poată aborda noile evoluții și provocări.

2. OBIECTUL ȘI METODOLOGIA REVIZUIRII

Deciziile privind caracterul adecvat al nivelului de protecție care fac obiectul acestei revizuiri au fost adoptate în temeiul cadrului UE privind protecția datelor care a precedat RGPD. În timp ce cele mai recente decizii datează de aproximativ un deceniu (de exemplu, deciziile privind Noua Zeelandă și Uruguay, ambele adoptate în 2012), altele sunt în vigoare de peste douăzeci de ani (de exemplu, decizia privind Canada, adoptată în 2001, și decizia privind Elveția, adoptată în 2000). De atunci, cadrele de protecție a datelor din toate cele unsprezece țări și teritorii au evoluat, de exemplu prin reforme legislative sau de reglementare, prin evoluții în ceea ce privește practicile de asigurare a respectării legii ale autorităților de protecție a datelor sau prin jurisprudență.

Prin urmare, în efectuarea evaluării sale, Comisia s-a axat pe evoluțiile cadrelor de protecție a datelor din țările și teritoriile relevante care au avut loc de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție. Comisia a evaluat modul în care aceste evoluții au

[20] Cum ar fi, de exemplu, Argentina, Columbia, Israel, Maroc, Elveția și Uruguay.

modelat în continuare peisajul protecției datelor din țara sau teritoriul relevant(ă) și dacă, având în vedere aceste evoluții, diferitele regimuri continuă să asigure un nivel adecvat de protecție.

În acest scop, a fost luată pe deplin în considerare evoluția propriului regim al UE de protecție a datelor, în special odată cu intrarea în vigoare a RGPD. În special, de la adoptarea acestor decizii privind caracterul adecvat al nivelului de protecție, standardul juridic aplicabil unor astfel de decizii, precum și elementele relevante pentru a evalua dacă un sistem străin asigură un nivel adecvat de protecție au fost clarificate suplimentar prin jurisprudența Curții de Justiție și prin orientările adoptate de Grupul de lucru „Articolul 29" și de succesorul acestuia, Comitetul european pentru protecția datelor[21] (CEPD).

În special, în hotărârea sa din 6 octombrie 2015 în cauza Schrems I, Curtea de Justiție a stabilit că, deși nu se poate impune ca o țară terță să asigure un nivel de protecție identic cu cel garantat în UE, testul privind caracterul adecvat trebuie înțeles ca impunând un nivel de protecție „în esență echivalent"[22]. În special, Curtea a clarificat că mijloacele la care țara terță în cauză recurge pentru protecția datelor cu caracter personal pot fi diferite de cele puse în aplicare în Uniune, cu condiția ca acestea să se dovedească în practică efective în scopul de a asigura un nivel de protecție adecvat[23]. Prin urmare, testul privind caracterul adecvat necesită o evaluare cuprinzătoare a sistemului țării terțe în ansamblu, inclusiv a fondului protecției vieții private, a punerii în aplicare eficace și a asigurării respectării acestora.

În plus, Curtea a clarificat faptul că evaluarea Comisiei nu ar trebui să se limiteze la cadrul general de protecție a datelor din țara terță, ci ar trebui să includă și normele care reglementează accesul autorităților publice la datele cu caracter personal, în special în scopul asigurării respectării legii și al securității naționale[24]. Utilizând Carta drepturilor fundamentale ca punct de referință, Curtea a identificat mai multe cerințe pe care aceste norme ar trebui să le respecte pentru a îndeplini standardul privind nivelul de protecție „în esență echivalent". De exemplu, legislația din acest domeniu ar trebui să prevadă norme clare și precise care să reglementeze domeniul de aplicare și aplicarea unei măsuri și să impună garanții minime, astfel încât persoanele ale căror date cu caracter personal sunt vizate să dispună de garanții suficiente care să permită protejarea efectivă a datelor lor împotriva riscurilor de abuz, precum și împotriva oricărei accesări și a oricărei utilizări ilicite a acestor date[25]. Aceasta ar trebui, de asemenea, să ofere persoanelor fizice posibilitatea de a exercita căi legale pentru a avea acces la datele cu caracter personal care le privesc sau pentru a obține rectificarea sau ștergerea unor astfel de date[26].

RGPD s-a bazat pe clarificările furnizate de Curtea de Justiție prin stabilirea unui catalog detaliat de elemente pe care Comisia trebuie să le ia în considerare într-o evaluare a

[21] Comitetul european pentru protecția datelor reunește autoritățile de supraveghere a protecției datelor din statele membre și Autoritatea Europeană pentru Protecția Datelor.
[22] Hotărârea în cauza Schrems I, punctele 73, 74 și 96. A se vedea și considerentul 104 din Regulamentul (UE) 2016/679, care se referă la standardul privind nivelul de protecție echivalent în esență.
[23] Hotărârea în cauza Schrems I, punctul 74.
[24] Hotărârea în cauza Schrems I, punctul 90.
[25] Hotărârea în cauza Schrems I, punctul 91.
[26] Hotărârea în cauza Schrems I, punctul 95.

caracterului adecvat al nivelului de protecție[27]. În plus, în hotărârea în cauza Schrems II din 16 iulie 2020, Curtea de Justiție a detaliat standardul privind nivelul de protecție „în esență echivalent", 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. În special, aceasta a clarificat faptul că, potrivit standardului privind nivelul de protecție „în esență echivalent", cadrele juridice relevante cu caracter obligatoriu pentru autoritățile publice din țările și teritoriile terțe în cauză trebuie să includă garanții minime care să garanteze că aceste autorități nu pot accesa date dincolo de ceea ce este necesar și proporțional pentru a urmări obiective legitime, iar persoanele vizate se bucură de drepturi efective și opozabile împotriva acestor autorități[28].

Evoluția standardului privind caracterul adecvat al nivelului de protecție se reflectă și în orientările care au fost adoptate inițial de Grupul de lucru „Articolul 29" și apoi aprobate de CEPD[29]. Aceste orientări, în special așa-numitele „criterii de referință privind caracterul adecvat al nivelului de protecție", clarifică și mai mult elementele pe care Comisia trebuie să le ia în considerare atunci când efectuează o evaluare a caracterului adecvat al nivelului de protecție, inclusiv prin furnizarea unei imagini de ansamblu asupra „garanțiilor esențiale" pentru accesul autorităților publice la datele cu caracter personal. Aceasta din urmă se bazează în special pe jurisprudența Curții Europene a Drepturilor Omului și a fost actualizată de CEPD pentru a ține seama de clarificările furnizate de Curtea de Justiție în hotărârea în cauza Schrems II[30]. Este important de remarcat faptul că criteriile de referință privind caracterul adecvat al nivelului de protecție recunosc, de asemenea, că standardul privind nivelul de protecție „în esență echivalent" nu implică o reproducere punct cu punct („fotocopie") a normelor UE, având în vedere că mijloacele de asigurare a unui nivel comparabil de protecție pot varia între diferitele sisteme de protecție a vieții private, reflectând adesea tradiții juridice diferite.

Prin urmare, pentru a stabili dacă cele 11 decizii privind caracterul adecvat al nivelului de protecție adoptate în temeiul normelor anterioare continuă să respecte standardul stabilit de RGPD, Comisia a luat în considerare nu numai evoluția cadrelor de protecție a datelor în țările și teritoriile în cauză, ci și evoluția interpretării în temeiul dreptului UE a standardului privind caracterul adecvat al nivelului de protecție în sine. Aceasta include, de asemenea, o evaluare a cadrului juridic care reglementează accesul la datele cu caracter personal transferate din UE și utilizarea acestora de către autoritățile publice ale țărilor sau teritoriilor despre care s-a constatat că oferă un nivel adecvat de protecție în temeiul articolului 25 alineatul (6) din Directiva privind protecția datelor.

[27] Articolul 45 alineatul (2) din RGPD.
[28] Hotărârea în cauza Schrems II, punctele 180-182.
[29]Criterii de referință privind caracterul adecvat al nivelului de protecție, WP 254 rev. 01, 6 februarie 2018 (document disponibil la adresa: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).
[30] Recomandările 02/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere (document disponibil la adresa: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_ro).

3. PROCESUL DE REVIZUIRE

Astfel cum s-a descris mai sus, pentru fiecare dintre țările sau teritoriile în cauză, evaluarea deciziilor existente privind caracterul adecvat al nivelului de protecție acoperă cadrul de protecție a datelor și orice evoluții în ceea ce privește cadrul juridic respectiv de la adoptarea constatării privind caracterul adecvat al nivelului de protecție, precum și normele care reglementează accesul autorităților publice la date – în special în scopul asigurării respectării legii și al securității naționale. În ultimii ani, serviciile Comisiei au luat mai multe măsuri pentru a efectua această evaluare, în strânsă cooperare cu fiecare dintre țările sau teritoriile relevante.

Pentru a sprijini Comisia în îndeplinirea obligațiilor sale de monitorizare, fiecare dintre cele 11 țări sau teritorii a furnizat Comisiei informații cuprinzătoare cu privire la evoluțiile regimului său de protecție a datelor de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție. În plus, Comisia a solicitat, de la fiecare dintre cele 11 țări sau teritorii, informații detaliate cu privire la normele privind accesul autorităților publice la datele cu caracter personal, în special în scopul asigurării respectării legii și al securității naționale care se aplică în țara sau teritoriul relevant(ă). De asemenea, Comisia a solicitat informații din surse publice, de la autoritățile de supraveghere și de aplicare a legii, precum și de la experți locali cu privire la funcționarea deciziilor și la evoluțiile relevante ale legislației și practicilor din fiecare dintre țările și teritoriile în cauză, atât în ceea ce privește normele de protecție a datelor aplicabile operatorilor privați, cât și în ceea ce privește accesul autorităților publice. În cele din urmă, după caz, s-a ținut seama în mod corespunzător de angajamentele internaționale asumate de aceste țări/teritorii în temeiul instrumentelor regionale sau universale.

Pe această bază, Comisia a purtat un dialog intens cu fiecare dintre țările și teritoriile în cauză. În contextul acestui dialog, multe dintre aceste țări și teritorii și-au modernizat și consolidat legislația privind protecția vieții private prin reforme cuprinzătoare sau parțiale (de exemplu, Andorra, Canada, Insulele Feroe, Elveția, Noua Zeelandă), determinate, printre altele, de necesitatea de a asigura continuitatea deciziilor privind caracterul adecvat al nivelului de protecție. Unele dintre aceste țări au adoptat reglementări și/sau orientări din partea autorității lor pentru protecția datelor pentru a introduce noi cerințe de protecție a datelor (de exemplu, Israel, Uruguay) sau pentru a clarifica anumite norme privind viața privată (de exemplu, Argentina, Canada, Guernsey, Jersey, Insula Man, Israel, Noua Zeelandă), pe baza practicilor de asigurare a respectării legii sau pe baza jurisprudenței. În plus, pentru a aborda diferențele relevante în ceea ce privește nivelul de protecție, atunci când au fost necesare pentru a asigura continuitatea deciziei privind caracterul adecvat, garanții suplimentare au fost negociate și convenite cu unele dintre țările și teritoriile în cauză pentru datele cu caracter personal transferate din Europa. De exemplu, guvernul canadian a extins drepturile de acces și de corectare în ceea ce privește datele cu caracter personal prelucrate de sectorul public la toate persoanele, indiferent de cetățenia sau locul lor de reședință (în timp ce, în trecut, aceste drepturi erau disponibile numai pentru cetățenii canadieni, rezidenții permanenți sau

persoanele fizice prezente în Canada)[31]. Ca un alt exemplu, guvernul israelian a introdus garanții specifice pentru a consolida protecția datelor cu caracter personal transferate din Spațiul Economic European, care creează, în special, noi obligații în domeniul exactității și păstrării datelor, consolidează drepturile la informare și ștergere și introduc categorii suplimentare de date sensibile[32].

În paralel, serviciile Comisiei au colectat opiniile și au informat periodic Parlamentul European (Comisia pentru libertăți civile, justiție și afaceri interne)[33], Consiliul (prin intermediul Grupului de lucru pentru protecția datelor)[34], CEPD[35] și Grupul multipartit de experți privind RGPD[36] (care include reprezentanți ai societății civile, ai industriei, ai mediului academic și ai practicienilor din domeniul dreptului) cu privire la progresele înregistrate în cadrul evaluării.

Prezentul raport și documentul de lucru al serviciilor Comisiei (SWD) care îl însoțește sunt, prin urmare, rezultatul cooperării strânse cu fiecare dintre țările și teritoriile vizate, precum și al consultărilor cu instituțiile și organismele relevante ale UE și al feedbackului primit din partea acestora. Aceste documente se bazează pe o varietate de surse, inclusiv legislație, acte de reglementare, jurisprudență, decizii și orientări din partea autorităților pentru protecția datelor, rapoarte ale organismelor de supraveghere (independente) și contribuții ale părților interesate. Înainte de adoptarea prezentului raport, tuturor țărilor și teritoriilor menționate anterior li s-a oferit posibilitatea de a verifica exactitatea factuală a informațiilor prezentate cu privire la sistemul lor în documentul de lucru al serviciilor Comisiei.

4. REZULTATE ȘI CONCLUZII PRINCIPALE

Prima revizuire a demonstrat că, de la adoptarea deciziilor privind caracterul adecvat al nivelului de protecție, cadrele de protecție a datelor în vigoare în fiecare dintre cele 11 țări sau teritorii au continuat convergența cu cadrul UE. În plus, în ceea ce privește accesul autorităților publice la datele cu caracter personal, prima revizuire a arătat că legislația acestor țări sau teritorii impune garanții și limitări adecvate și oferă mecanisme de supraveghere și de reparații în acest domeniu.

---

[31] Secțiunea 12 din Legea privind viața privată, Ordinul de extindere a Legii privind viața privată nr. 1 și Ordinul de extindere a Legii privind viața privată nr. 2.

[32] Regulamentul privind protecția vieții private (Instrucțiuni pentru datele care au fost transferate în Israel din Spațiul Economic European), 5783-2023, publicat în Monitorul Oficial al Israelului (*Reshumut*) la 7 mai 2023.

[33] A se vedea, de exemplu, Rezoluția Parlamentului European din 25 martie 2021 referitoare la raportul de evaluare al Comisiei privind punerea în aplicare a Regulamentului general privind protecția datelor, la doi ani de la aplicarea acestuia [2020/2717(RSP)], document disponibil la adresa următoare: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_RO.html.

[34] A se vedea, de exemplu, Poziția Consiliului și constatările privind aplicarea Regulamentului general privind protecția datelor (RGPD), adoptate la 19 decembrie 2019, document disponibil la adresa următoare: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/ro/pdf.

[35] A se vedea, de exemplu, contribuția CEPD la evaluarea RGPD în temeiul articolului 97, adoptată la 18 februarie 2020, document disponibil la adresa următoare: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.

[36] A se vedea, de exemplu, raportul Grupului multipartit de experți privind evaluarea RGPD, document disponibil la adresa următoare: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=ro&do=groupDetail.groupMeeting&meetingId=21356.

Constatările detaliate privind fiecare dintre cele 11 țări sau teritorii sunt prezentate în documentul de lucru al serviciilor Comisiei care însoțește prezentul raport. Pe baza acestor constatări, Comisia concluzionează că fiecare dintre cele 11 țări și teritorii continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniunea Europeană în sensul RGPD, astfel cum a fost interpretat de Curtea de Justiție. Constatările pentru fiecare dintre țările și teritoriile care asigură un nivel adecvat de protecție sunt rezumate mai jos.

4.1. Andorra

Comisia salută evoluțiile cadrului juridic din Andorra înregistrate de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție, inclusiv modificările legislative și activitățile organismelor de supraveghere. În special, adoptarea Legii calificate nr. 29/2021 privind protecția datelor cu caracter personal, care a intrat în vigoare în mai 2022, a contribuit la creșterea nivelului de protecție a datelor, întrucât legea este aliniată îndeaproape la RGPD în ceea ce privește structura și componentele sale principale.

În ceea ce privește accesul autorităților publice la datele cu caracter personal, autoritățile publice din Andorra se supun unor norme clare, precise și accesibile, în temeiul cărora aceste autorități pot accesa și utiliza ulterior datele transferate din UE în scopuri de interes public, în special în scopul asigurării respectării dreptului penal și al securității naționale. Aceste limitări și garanții decurg din cadrul juridic general și din angajamentele internaționale, în special din Constituția Andorrei, din Convenția europeană a drepturilor omului (CEDO) și din Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108 și Protocolul de modificare, care creează Convenția 108+ modernizată), precum și din normele specifice de protecție a datelor care se aplică prelucrării datelor cu caracter personal în contextul asigurării respectării legii, care reproduc, în esență, elementele de bază ale Directivei (UE) 2016/680[37]. În plus, legislația din Andorra impune o serie de condiții și limitări specifice privind accesul la datele cu caracter personal și utilizarea acestora de către autoritățile publice și prevede mecanisme de supraveghere și de reparații în acest domeniu.

Pe baza constatărilor generale prezentate în documentul de lucru al serviciilor Comisiei, Comisia concluzionează că Andorra continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE.

În ceea ce privește normele specifice de protecție a datelor care se aplică în prezent prelucrării datelor de către autoritățile de aplicare a legii, Comisia salută intenția legiuitorului din Andorra de a înlocui aceste norme cu un regim mai cuprinzător, care va fi aliniat și mai mult la normele care se aplică în UE. Comisia va monitoriza îndeaproape evoluțiile viitoare în acest domeniu.

4.2. Argentina

[37] 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.

Comisia salută evoluțiile cadrului juridic din Argentina de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție, inclusiv modificările legislative, jurisprudența și activitățile organismelor de supraveghere, care au contribuit la creșterea nivelului de protecție a datelor. În special, independența autorității argentiniene de supraveghere a protecției datelor a fost consolidată în mod semnificativ prin Decretul nr. 746/17, care a încredințat către *Agencia de Acceso a la Información Pública* (AAIP) responsabilitatea de a supraveghea respectarea legislației privind protecția datelor. În plus, AAIP a emis o serie de regulamente și avize obligatorii care clarifică modul în care cadrul de protecție a datelor trebuie interpretat și aplicat în practică, contribuind astfel la actualizarea legislației privind protecția datelor. Argentina și-a consolidat, de asemenea, angajamentele internaționale în domeniul protecției datelor prin aderarea în 2019 la Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal și la protocolul adițional la aceasta, precum și prin ratificarea în 2023 a Protocolului de modificare care a creat Convenția 108+ modernizată.

În ceea ce privește accesul autorităților publice la datele cu caracter personal, autoritățile publice din Argentina se supun unor norme clare, precise și accesibile, în temeiul cărora aceste autorități pot accesa și utiliza ulterior datele transferate din UE în scopuri de interes public, în special în scopul asigurării respectării dreptului penal și al securității naționale. Aceste limitări și garanții decurg din cadrul juridic general și din angajamentele internaționale, în special Constituția Argentinei, Convenția americană privind drepturile omului, Convenția 108 și Convenția 108+, precum și din normele argentiniene privind protecția datelor (Legea nr. 25.326 privind protecția datelor cu caracter personal din 4 octombrie 2000) care se aplică și prelucrării datelor cu caracter personal de către autoritățile publice argentiniene, inclusiv în scopul asigurării respectării legii și al securității naționale. În plus, legislația argentiniană impune o serie de condiții și limitări specifice privind accesul la datele cu caracter personal și utilizarea acestora în scopul asigurării respectării dreptului penal și al securității naționale și prevede mecanisme de supraveghere și de reparații în acest domeniu.

Pe baza constatărilor generale prezentate în documentul de lucru al serviciilor Comisiei, Comisia concluzionează că Argentina continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE.

În același timp, Comisia recomandă consacrarea în legislație a măsurilor de protecție care au fost dezvoltate la nivel sublegislativ pentru a spori securitatea juridică și a consolida aceste cerințe. Proiectul de lege privind protecția datelor, care a fost introdus recent în Congresul argentinian, ar putea oferi ocazia de a codifica aceste evoluții și, prin urmare, de a consolida și mai mult cadrul argentinian privind protecția vieții private. Comisia va monitoriza îndeaproape evoluțiile viitoare în acest domeniu.

4.3. Canada

Comisia salută evoluțiile cadrului juridic din Canada de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție, inclusiv cele câteva modificări legislative, jurisprudența și activitățile organismelor de supraveghere, care au contribuit la creșterea

nivelului de protecție a datelor. În special, Legea privind protecția informațiilor cu caracter personal și documentele electronice (PIPEDA) a fost consolidată în continuare prin diferite modificări (de exemplu, cu privire la condițiile pentru consimțământul valabil și notificările privind încălcarea securității datelor), în timp ce cerințele-cheie privind protecția datelor (de exemplu, privind prelucrarea datelor sensibile) au fost clarificate suplimentar prin jurisprudență, precum și prin orientări emise de autoritatea federală canadiană pentru protecția datelor, Oficiul Comisarului pentru protecția vieții private. În același timp, Comisia recomandă consacrarea în legislație a unora dintre măsurile de protecție care au fost dezvoltate la nivel sublegislativ pentru a spori securitatea juridică și pentru a consolida aceste cerințe. Reforma legislativă în curs a PIPEDA ar putea oferi, în special, o oportunitate de a codifica astfel de evoluții și, prin urmare, de a consolida și mai mult cadrul canadian privind protecția vieții private. Comisia va monitoriza îndeaproape evoluțiile viitoare în acest domeniu.

În ceea ce privește accesului autorităților publice la datele cu caracter personal, autoritățile publice din Canada se supun unor norme clare, precise și accesibile în temeiul cărora aceste autorități pot accesa și utiliza ulterior datele transferate din UE în scopuri de interes public, în special în scopul asigurării respectării dreptului penal și al securității naționale. Aceste limitări și garanții decurg din cadrul constituțional general (Carta canadiană a drepturilor și libertăților), din jurisprudență, din legislația specifică care reglementează accesul la date, precum și din normele privind protecția datelor (și anume Legea privind viața privată și legile similare le la nivelul provinciilor) care se aplică și prelucrării datelor cu caracter personal de către autoritățile publice canadiene, inclusiv în scopul asigurării respectării legii și al securității naționale. În plus, sistemul juridic canadian oferă mecanisme eficace de supraveghere și de reparații în acest domeniu, inclusiv printr-o extindere recentă a drepturilor persoanelor vizate și a posibilităților de reparații pentru resortisanții sau rezidenții din afara Canadei.

Pe baza constatărilor generale prezentate în documentul de lucru al serviciilor Comisiei, Comisia concluzionează că Canada continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE către destinatari care fac obiectul PIPEDA. Astfel cum s-a menționat mai sus, PIPEDA face în prezent obiectul unei reforme legislative care ar putea consolida și mai mult măsurile de protecție a vieții private, inclusiv în domenii relevante pentru constatarea caracterului adecvat al nivelului de protecție.

4.4. Insulele Feroe

Comisia salută evoluțiile cadrului juridic din Insulele Feroe de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție, inclusiv modificările legislative, jurisprudența și activitățile organismelor de supraveghere, care au contribuit la creșterea nivelului de protecție a datelor. În special, Insulele Feroe și-au modernizat în mod semnificativ cadrul de protecție a datelor prin adoptarea Legii privind protecția datelor, care a intrat în vigoare în 2021 și a aliniat îndeaproape regimul din Insulele Feroe la RGPD.

În ceea ce privește accesul autorităților publice la datele cu caracter personal, autoritățile publice din Insulele Feroe se supun unor norme clare, precise și accesibile în temeiul cărora

aceste autorități pot accesa și utiliza ulterior datele transferate din UE în scopuri de interes public, în special în scopul asigurării respectării dreptului penal și al securității naționale. Aceste limitări și garanții decurg din cadrul juridic general și din angajamentele internaționale, în special cadrul constituțional și Convenția europeană a drepturilor omului, precum și din legile specifice care reglementează accesul autorităților publice la date și normele de protecție a datelor care se aplică prelucrării datelor cu caracter personal în scopul asigurării respectării dreptului penal [Legea privind prelucrarea datelor cu caracter personal de către autoritățile de aplicare a legii, care a fost instituită în Insulele Feroe în 2022 și care transpune legislația adoptată de Danemarca în vederea punerii în aplicare a Directivei (UE) 2016/680 în Insulele Feroe] și în scopuri legate de securitatea națională (cuprinse în Legea privind securitatea și serviciile de informații). În plus, în acest domeniu sunt disponibile mecanisme efective de supraveghere și de reparații.

Pe baza constatărilor generale prezentate în documentul de lucru al serviciilor Comisiei, Comisia concluzionează că Insulele Feroe continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE.

4.5. Guernsey

Comisia salută evoluțiile cadrului juridic din Guernsey de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție, inclusiv modificările legislative și activitățile organismelor de supraveghere, care au contribuit la creșterea nivelului de protecție a datelor. În special, Guernsey și-a modernizat în mod semnificativ cadrul de protecție a datelor prin adoptarea Legii din 2017 privind protecția datelor (Domeniul Guernsey), care se aplică din 2019 și aliniază îndeaproape regimul din Guernsey la RGPD.

În ceea ce privește accesul autorităților publice la datele cu caracter personal, autoritățile publice din Guernsey se supun unor norme clare, precise și accesibile în temeiul cărora aceste autorități pot accesa și utiliza ulterior datele transferate din UE în scopuri de interes public, în special în scopul asigurării respectării dreptului penal și al securității naționale. Aceste limitări și garanții decurg din cadrul juridic general și din angajamentele internaționale, în special Convenția europeană a drepturilor omului și Convenția 108, precum și din normele de protecție a datelor din Guernsey, inclusiv din dispozițiile specifice privind prelucrarea datelor cu caracter personal în contextul asigurării respectării legii prevăzute în Ordonanța din 2018 privind protecția datelor (asigurarea respectării legii și aspecte conexe) (Domeniul Guernsey). În plus, legislația din Guernsey impune o serie de condiții și limitări specifice privind accesul la datele cu caracter personal și utilizarea acestora în scopul asigurării respectării dreptului penal și al securității naționale și prevede mecanisme de supraveghere și de reparații în acest domeniu.

Pe baza constatărilor generale prezentate în documentul de lucru al serviciilor Comisiei, Comisia concluzionează că Guernsey continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE.

4.6. Insula Man

Comisia salută evoluțiile cadrului juridic din Insula Man de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție, inclusiv modificările legislative și activitățile organismelor de supraveghere, care au contribuit la creșterea nivelului de protecție a datelor. În special, Insula Man a adoptat o nouă legislație în 2018 [Legea privind protecția datelor din 2018, completată de Ordinul din 2018 privind protecția datelor (aplicarea RGPD)], care încorporează majoritatea dispozițiilor cadrului UE privind protecția datelor în ordinea juridică din Insula Man, efectuând, în același timp, doar ajustări minore cu privire la aspecte specifice, în special pentru a adapta cadrul la contextul local.

În ceea ce privește accesul autorităților publice la datele cu caracter personal, autoritățile publice din Insula Man se supun unor norme clare, precise și accesibile în temeiul cărora aceste autorități pot accesa și utiliza ulterior datele transferate din UE în scopuri de interes public, în special în scopul asigurării respectării dreptului penal și al securității naționale. Aceste limitări și garanții decurg din cadrul juridic general și din angajamentele internaționale, în special Convenția europeană a drepturilor omului și Convenția 108, precum și din normele din Insula Man privind protecția datelor, inclusiv din dispozițiile specifice privind prelucrarea datelor cu caracter personal în contextul asigurării respectării legii prevăzute în Ordinul din 2018 privind protecția datelor (aplicarea LED) și în Regulamentul de punere în aplicare a LED din 2018. În plus, legislația din Insula Man impune o serie de limitări specifice privind accesul la datele cu caracter personal și utilizarea acestora în scopul asigurării respectării dreptului penal și al securității naționale și prevede mecanisme de supraveghere și de reparații în acest domeniu.

Pe baza constatărilor generale prezentate în documentul de lucru al serviciilor Comisiei, Comisia concluzionează că Insula Man continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE.

4.7. Israel

Comisia salută evoluțiile cadrului juridic din Israel de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție, inclusiv modificările legislative, jurisprudența și activitățile organismelor de supraveghere, care au contribuit la creșterea nivelului de protecție a datelor. În special, Israel a introdus garanții specifice pentru a consolida protecția datelor cu caracter personal transferate din Spațiul Economic European prin adoptarea Regulamentului privind protecția vieții private (Instrucțiuni pentru datele care au fost transferate în Israel din Spațiul Economic European), 5783-2023. De asemenea, Israel a consolidat cerințele privind securitatea datelor prin adoptarea Regulamentului privind protecția vieții private (securitatea datelor), 5777-2017, și a consolidat independența autorității sale de supraveghere a protecției datelor printr-o rezoluție guvernamentală cu caracter obligatoriu.

În ceea ce privește accesul autorităților publice la datele cu caracter personal, autoritățile publice din Israel se supun unor norme clare, precise și accesibile în temeiul cărora aceste autorități pot accesa și utiliza ulterior datele transferate din UE în scopuri de interes public, în special în scopul asigurării respectării dreptului penal și al securității naționale. Aceste limitări și garanții decurg din cadrul juridic general, în special din Legea fundamentală a Israelului, precum și din Legea privind protecția vieții private 5741-1981 și din regulamentele adoptate

în temeiul acesteia, care se aplică prelucrării datelor cu caracter personal de către autoritățile publice israeliene, inclusiv în scopul asigurării respectării legii și al securității naționale. În plus, legislația din Israel impune o serie de limitări specifice privind accesul la datele cu caracter personal și utilizarea acestora în scopul asigurării respectării dreptului penal și al securității naționale și prevede mecanisme de supraveghere și de reparații în acest domeniu.

Pe baza constatărilor generale prezentate în documentul de lucru al serviciilor Comisiei, Comisia concluzionează că Israel continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE.

În același timp, Comisia recomandă consacrarea în legislație a măsurilor de protecție care au fost dezvoltate la nivel sublegislativ și prin jurisprudență pentru a spori securitatea juridică și pentru a consolida aceste cerințe. Proiectul de lege privind protecția vieții private (amendamentul nr. 14), 5722-2022, care a fost introdus recent în parlamentul israelian, oferă o oportunitate importantă de a consolida și codifica aceste evoluții și, prin urmare, de a consolida și mai mult cadrul israelian privind protecția vieții private. Comisia va monitoriza îndeaproape evoluțiile viitoare în acest domeniu.

4.8. Jersey

Comisia salută evoluțiile cadrului juridic din Jersey de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție, inclusiv modificările legislative, jurisprudența și activitățile organismelor de supraveghere, care au contribuit la creșterea nivelului de protecție a datelor. În special, Jersey și-a modernizat în mod semnificativ cadrul de protecție a datelor prin adoptarea Legii din 2018 privind protecția datelor (Jersey) și a Legii din 2018 privind Autoritatea pentru Protecția Datelor (Jersey), care au intrat în vigoare în 2018, și a aliniat îndeaproape regimul din Jersey la RGPD.

În ceea ce privește accesul autorităților publice la datele cu caracter personal, autoritățile publice din Jersey se supun unor norme clare, precise și accesibile în temeiul cărora aceste autorități pot accesa și utiliza ulterior datele transferate din UE în scopuri de interes public, în special în scopul asigurării respectării dreptului penal și al securității naționale. Aceste limitări și garanții decurg din cadrul juridic general și din angajamentele internaționale, în special Convenția europeană a drepturilor omului și Convenția 108, precum și din normele de protecție a datelor din Jersey, inclusiv din dispozițiile specifice privind prelucrarea datelor cu caracter personal în contextul asigurării respectării legii prevăzute în Legea din 2018 privind protecția datelor (Jersey), astfel cum a fost modificată prin anexa 1 la legea respectivă. În plus, legislația din Jersey impune o serie de limitări specifice privind accesul la datele cu caracter personal și utilizarea acestora în scopul asigurării respectării dreptului penal și al securității naționale și prevede mecanisme de supraveghere și de reparații în acest domeniu.

Pe baza constatărilor generale prezentate în documentul de lucru al serviciilor Comisiei, Comisia concluzionează că Jersey continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE.

4.9. Noua Zeelandă

Comisia salută evoluțiile cadrului juridic din Noua Zeelandă de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție, inclusiv modificările legislative, jurisprudența și activitățile organismelor de supraveghere, care au contribuit la creșterea nivelului de protecție a datelor. În special, regimul de protecție a datelor a făcut obiectul unei reforme cuprinzătoare odată cu adoptarea Legii privind protecția vieții private din 2020, care a sporit și mai mult convergența cu cadrul UE privind protecția datelor, în special în ceea ce privește normele pentru transferurile internaționale de date cu caracter personal și competențele autorității pentru protecția datelor (Biroul Comisarului pentru protecția vieții private).

În ceea ce privește accesul autorităților publice la datele cu caracter personal, autoritățile publice din Noua Zeelandă se supun unor norme clare, precise și accesibile în temeiul cărora aceste autorități pot accesa și utiliza ulterior datele transferate din UE în scopuri de interes public, în special în scopul asigurării respectării dreptului penal și al securității naționale. Aceste limitări și garanții decurg din cadrul constituțional general (de exemplu, Legea privind Carta drepturilor) și din jurisprudență, precum și din legile specifice care reglementează accesul administrației publice la date și din dispozițiile Legii privind protecția vieții private care se aplică și prelucrării datelor cu caracter personal de către autoritățile de aplicare a dreptului penal și de securitate națională. În plus, sistemul juridic al Noii Zeelande prevede diferite mecanisme de supraveghere și de reparații în acest domeniu.

Pe baza constatărilor generale prezentate în documentul de lucru al serviciilor Comisiei, Comisia concluzionează că Noua Zeelandă continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE. Comisia salută, de asemenea, recenta introducere de către guvernul Noii Zeelande în fața Parlamentului a unui proiect de lege de modificare a Legii privind protecția vieții private din 2020 pentru a consolida și mai mult cerințele existente în materie de transparență. Comisia va monitoriza îndeaproape evoluțiile viitoare în acest domeniu.

4.10. Elveția

Comisia salută evoluțiile cadrului juridic din Elveția de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție, inclusiv modificările legislative, jurisprudența și activitățile organismelor de supraveghere, care au contribuit la creșterea nivelului de protecție a datelor. În special, Legea federală modernizată privind protecția datelor, care a sporit și mai mult convergența cu cadrul UE privind protecția datelor, în special în ceea ce privește protecția datelor sensibile și normele privind transferurile internaționale de date. De asemenea, Elveția și-a consolidat angajamentele internaționale în domeniul protecției datelor prin ratificarea Convenției 108+ în septembrie 2023.

În ceea ce privește accesul autorităților publice la datele cu caracter personal, autoritățile publice din Elveția se supun unor norme clare, precise și accesibile în temeiul cărora aceste autorități pot accesa și utiliza ulterior datele transferate din UE în scopuri de interes public, în special în scopul asigurării respectării dreptului penal și al securității naționale. Aceste limitări și garanții decurg din cadrul juridic general și din angajamentele internaționale, în special Constituția federală a Elveției, Convenția europeană a drepturilor omului și Convenția 108+, precum și din normele elvețiene privind protecția datelor, inclusiv Legea federală privind

protecția datelor și normele specifice de protecție a datelor care se aplică autorităților de aplicare a dreptului penal (de exemplu, Codul de procedură penală) și autorităților de securitate națională (de exemplu, Legea privind serviciile de informații). În plus, legislația elvețiană impune o serie de limitări specifice privind accesul la datele cu caracter personal și utilizarea acestora în scopul asigurării respectării dreptului penal și al securității naționale și prevede mecanisme de supraveghere și de reparații în acest domeniu.

Pe baza constatărilor generale prezentate în documentul de lucru al serviciilor Comisiei, Comisia concluzionează că Elveția continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE.

4.11. Uruguay

Comisia salută evoluțiile cadrului juridic din Uruguay de la adoptarea deciziei privind caracterul adecvat al nivelului de protecție, inclusiv cele câteva modificări legislative, jurisprudența și activitățile organismelor de supraveghere, care au contribuit la creșterea nivelului de protecție a datelor. În special, Uruguay și-a modernizat și consolidat Legea nr. 18.331 privind protecția datelor cu caracter personal și acțiunile de tip „habeas data" din 2008 prin modificări legislative în 2018 și 2020, care au extins domeniul de aplicare teritorial al legislației privind protecția datelor, au creat noi cerințe în materie de răspundere (cum ar fi evaluările impactului, protecția datelor începând cu momentul conceperii și în mod implicit, notificarea încălcării securității datelor și numirea responsabililor cu protecția datelor) și au introdus măsuri suplimentare de protecție pentru datele biometrice. De asemenea, Uruguay și-a consolidat angajamentele internaționale în domeniul protecției datelor prin aderarea la Convenția 108 în 2019 și prin ratificarea Convenției 108+ în 2021.

În ceea ce privește accesul autorităților publice la datele cu caracter personal, autoritățile publice din Uruguay se supun unor norme clare, precise și accesibile în temeiul cărora aceste autorități pot accesa și utiliza ulterior datele transferate din UE în scopuri de interes public, în special în scopul asigurării respectării dreptului penal și al securității naționale. Aceste limitări și garanții decurg din cadrul juridic general și din angajamentele internaționale, în special Constituția statului Uruguay, Convenția americană privind drepturile omului, Convenția 108 și Convenția 108+, precum și din normele de protecție a datelor din Legea 18.331 privind protecția datelor cu caracter personal și acțiunile de tip „habeas data" care se aplică prelucrării datelor cu caracter personal de către autoritățile publice din Uruguay, în special în scopul asigurării respectării legii și al securității naționale. În plus, legislația din Uruguay impune o serie de condiții și limitări specifice privind accesul la datele cu caracter personal și utilizarea acestora de către autoritățile publice și prevede mecanisme de supraveghere și de reparații în acest domeniu.

Pe baza constatărilor generale formulate în cadrul acestei prime revizuiri, Comisia concluzionează că Uruguay continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate din UE.

5. MONITORIZAREA ȘI COOPERAREA VIITOARE

Comisia recunoaște și apreciază foarte mult cooperarea excelentă cu autoritățile competente din fiecare dintre țările și teritoriile vizate în cadrul acestei revizuiri. Comisia va continua să monitorizeze îndeaproape evoluțiile cadrelor de protecție și practicile efective ale țărilor și teritoriilor în cauză. În cazul unor evoluții dintr-o țară sau un teritoriu care are un nivel adecvat de protecție care ar afecta în mod negativ nivelul de protecție a datelor considerat adecvat, Comisia va recurge, dacă este necesar, la competențele care îi revin în temeiul articolului 45 alineatul (5) din RGPD pentru a suspenda, modifica sau retrage o decizie privind caracterul adecvat al nivelului de protecție.

Prezenta revizuire confirmă faptul că adoptarea unei decizii privind caracterul adecvat al nivelului de protecție nu este un „punct final”, ci oferă o oportunitate de a intensifica și mai mult dialogul și cooperarea cu parteneri internaționali care împărtășesc aceeași viziune în ceea ce privește fluxurile de date și aspectele digitale în general. În acest sens, Comisia așteaptă cu interes viitoarele schimburi cu autoritățile relevante pentru a consolida în continuare cooperarea la nivel internațional în ceea ce privește promovarea fluxurilor de date sigure și libere, inclusiv prin consolidarea cooperării în materie de asigurare a respectării legii. Pentru a intensifica acest dialog și a promova schimbul de informații și de experiență, Comisia intenționează să organizeze o reuniune la nivel înalt în 2024, care să reunească reprezentanți ai UE și ai tuturor țărilor care beneficiază de o decizie privind caracterul adecvat al nivelului de protecție.