KOMISJA
EUROPEJSKA

Bruksela, dnia 15.1.2024 r.
COM(2024) 7 final

SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie pierwszego przeglądu decyzji stwierdzających odpowiedni stopień ochrony, które przyjęto na podstawie art. 25 ust. 6 dyrektywy 95/46/WE

{SWD(2024) 3 final}

1. PIERWSZY PRZEGLĄD – INFORMACJE I KONTEKST

Niniejsze sprawozdanie zawiera ustalenia Komisji dotyczące pierwszego przeglądu decyzji stwierdzających odpowiedni stopień ochrony, które przyjęto na podstawie art. 25 ust. 6 dyrektywy 95/46/WE[1] (dyrektywa o ochronie danych).

W decyzjach tych Komisja stwierdziła, że jedenaście państw lub terytoriów nadal zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z Unii Europejskiej (UE)[2]: Andora[3], Argentyna[4], Guernsey[5], Izrael[6], Jersey[7], Kanada (dla podmiotów handlowych)[8], Nowa Zelandia[9], Szwajcaria[10], Urugwaj[11], Wyspy Owcze[12] i Wyspa Man[13]. W rezultacie przekazywanie danych z UE do tych państw lub terytoriów może być realizowane bez dodatkowych wymogów.

Wraz z rozpoczęciem stosowania rozporządzenia (UE) 2016/679 (RODO)[14] 25 maja 2018 r. decyzje stwierdzające odpowiedni stopień ochrony przyjęte na podstawie dyrektywy

[1] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U. L 281 z 23.11.1995, s. 31.

[2] Po włączeniu RODO do Porozumienia o Europejskim Obszarze Gospodarczym (EOG) stosuje się ono również do Norwegii, Islandii i Liechtensteinu. Odniesienia do UE w niniejszym sprawozdaniu należy rozumieć jako obejmujące również państwa EOG.

[3] Decyzja Komisji 2010/625/UE z dnia 19 października 2010 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Andorze, Dz.U. L 277 z 21.10.2010, s. 27.

[4] Decyzja Komisji 2003/490/WE z dnia 30 czerwca 2003 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Argentynie, Dz.U. L 168 z 5.7.2003, s. 19.

[5] Decyzja Komisji 2003/821/WE z dnia 21 listopada 2003 r. w sprawie właściwej ochrony danych osobowych w Guernsey, Dz.U. L 308 z 25.11.2003, s. 27.

[6] Decyzja Komisji 2011/61/UE z dnia 31 stycznia 2011 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Państwie Izrael w odniesieniu do zautomatyzowanego przetwarzania danych osobowych, Dz.U. L 27 z 1.2.2011, s. 39.

[7] Decyzja Komisji 2008/393/WE z dnia 8 maja 2008 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Jersey, Dz.U. L 138 z 28.5.2008, s. 21.

[8] Decyzja Komisji 2002/2/WE z dnia 20 grudnia 2001 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych, Dz.U. L 2 z 4.1.2002, s. 13.

[9] Decyzja wykonawcza Komisji 2013/65/UE z dnia 19 grudnia 2012 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Nowej Zelandii, Dz.U. L 28 z 30.1.2013, s. 12.

[10] Decyzja Komisji 2000/518/WE z dnia 26 lipca 2000 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Szwajcarii, Dz.U. L 215 z 25.8.2000, s. 1.

[11] Decyzja wykonawcza Komisji 2012/484/UE z dnia 21 sierpnia 2012 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych przez Wschodnią Republikę Urugwaju w odniesieniu do zautomatyzowanego przetwarzania danych osobowych, Dz.U. L 227 z 23.8.2012, s. 11.

[12] Decyzja Komisji 2010/146/UE z dnia 5 marca 2010 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie właściwej ochrony na podstawie ustawy Wysp Owczych w sprawie ochrony danych osobowych, Dz.U. L 58 z 9.3.2010, s. 17.

[13] Decyzja Komisji 2004/411/WE z dnia 28 kwietnia 2004 r. w sprawie odpowiedniej ochrony danych osobowych na Wyspie Man, Dz.U. L 151 z 30.4.2004, s. 48.

[14] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich

o ochronie danych pozostały w mocy[15]. Jednocześnie w RODO doprecyzowano, że ustalenia dotyczące odpowiedniego stopnia ochrony są „żywymi instrumentami", stanowiąc, że Komisja musi na bieżąco monitorować zmiany w państwach trzecich mogące wpłynąć na obowiązywanie istniejących decyzji stwierdzających odpowiedni stopień ochrony[16]. Ponadto art. 97 RODO zobowiązuje Komisję do okresowego przeglądu tych decyzji co cztery lata w celu ustalenia, czy państwa i terytoria, w których stwierdzono odpowiedni stopień ochrony, nadal zapewniają odpowiedni poziom ochrony danych osobowych.

Niniejszy pierwszy przegląd decyzji stwierdzających odpowiedni stopień ochrony przyjętych na podstawie poprzednich unijnych ram ochrony danych został zainicjowany w ramach szerszej oceny stosowania i funkcjonowania RODO, na temat której Komisja przedstawiła swoje ustalenia w komunikacie pt. „Ochrona danych jako filar wzmocnienia pozycji obywateli oraz podejście UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych"[17]. Zakończenie analizy tego aspektu przeglądu zostało jednak odroczone, aby uwzględnić wyrok Trybunału Sprawiedliwości w sprawie Schrems II[18], w którym Trybunał przedstawił istotne wyjaśnienia dotyczące kluczowych elementów standardu odpowiedniego stopnia ochrony, a także innych powiązanych zmian. To z kolei doprowadziło do szczegółowej wymiany informacji z odnośnymi państwami i terytoriami na temat odpowiednich aspektów ich ram prawnych, mechanizmów nadzoru i systemu egzekwowania prawa[19]. W niniejszym sprawozdaniu w pełni uwzględniono wszystkie te zmiany, zarówno w UE, jak i w odnośnych państwach trzecich i na odnośnych terytoriach.

Co ważne, ten pierwszy przegląd odbywa się w kontekście wykładniczego rozwoju technologii cyfrowych. W ostatnich dziesięcioleciach znaczenie decyzji stwierdzających odpowiedni stopień ochrony znacznie wzrosło, ponieważ przepływy danych stały się nieodłącznym elementem transformacji cyfrowej społeczeństwa i globalizacji gospodarki. Transgraniczne przekazywanie danych stało się elementem codziennego funkcjonowania europejskich przedsiębiorstw różnej wielkości we wszystkich sektorach. Bardziej niż kiedykolwiek wcześniej poszanowanie prywatności jest warunkiem stabilnych, bezpiecznych i konkurencyjnych przepływów handlowych. W tym kontekście decyzje stwierdzające

danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U. L 119 z 4.5.2016, s. 1.

[15] Zob. art. 45 ust. 9 RODO, który stanowi, że decyzje przyjęte przez Komisję na mocy art. 25 ust. 6 dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia decyzją Komisji przyjętą zgodnie z art. 45 ust. 3 lub 5.

[16] Art. 45 ust. 4 RODO. Zob. również wyrok Trybunału Sprawiedliwości UE z dnia 6 października 2015 r. w sprawie C-362/14 Maximillian Schrems/Data Protection Commissioner (Schrems I), ECLI:EU:C:2015:650, pkt 76.

[17] Przedmiotowy komunikat, opublikowany w czerwcu 2020 r., jest dostępny pod adresem: https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_pl

[18] Wyrok Trybunału Sprawiedliwości z dnia 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559.

[19] Decyzję stwierdzającą odpowiedni stopień ochrony dotyczącą Japonii przyjęto na podstawie RODO i przewidziano w niej odrębny przegląd okresowy. Pierwszy przegląd ukończono w kwietniu 2023 r., publikując sprawozdanie Komisji dla Parlamentu Europejskiego i Rady dotyczące pierwszego przeglądu funkcjonowania decyzji stwierdzającej odpowiedni stopień ochrony w Japonii, COM(2023) 275 final, dostępne pod następującym adresem: https://eur-lex.europa.eu/legal-content/pl/TXT/PDF/?uri=COM:2023:275:FIN

odpowiedni stopień ochrony odgrywają pod wieloma względami coraz istotniejszą rolę. Zapewniając ochronę przenoszonym danym, decyzje umożliwiają bezpieczny przepływ danych, z poszanowaniem praw osób fizycznych zgodnie z unijnym podejściem do transformacji cyfrowej skoncentrowanym na człowieku. Poprzez uznanie ram ochrony prywatności państw trzecich za zapewniające poziom ochrony, który jest merytorycznie równoważny poziomowi unijnemu, propagują one konwergencję między systemami ochrony prywatności opartymi na wysokich standardach ochrony. Ponadto, jak wyjaśniono w niniejszym sprawozdaniu, decyzje stwierdzające odpowiedni stopień ochrony nie są „punktem końcowym", lecz stanowią podstawę ściślejszej współpracy i dalszej konwergencji regulacyjnej między UE a partnerami o podobnych poglądach. Dzięki umożliwieniu swobodnego przepływu danych osobowych decyzje te otworzyły kanały handlowe dla podmiotów z UE, również dzięki uzupełnianiu i zwiększaniu korzyści płynących z umów handlowych, a także ułatwiły współpracę z partnerami zagranicznymi w wielu dziedzinach regulacyjnych. Zapewniając proste i kompleksowe rozwiązanie w zakresie przekazywania danych bez konieczności zapewnienia przez podmiot przekazujący dane dalszych zabezpieczeń lub uzyskania jakiegokolwiek zezwolenia, ułatwiają one, w szczególności małym i średnim przedsiębiorstwom, spełnianie międzynarodowych wymogów RODO dotyczących przekazywania danych. Ponadto dzięki wywoływanym przez siebie „efektom sieci" decyzje stwierdzające odpowiedni stopień ochrony przyjęte przez Komisję Europejską mają coraz większe znaczenie również poza UE, ponieważ umożliwiają nie tylko swobodny przepływ danych między 30 gospodarkami UE, ale także między dużo większą liczbą jurysdykcji na całym świecie[20], które uznają państwa, w odniesieniu do których wydano unijną decyzję stwierdzającą odpowiedni stopień ochrony, za „bezpieczne miejsca docelowe" na mocy ich własnych przepisów o ochronie danych.

Z wspomnianych powyżej powodów decyzje stwierdzające odpowiedni stopień ochrony stały się strategicznym elementem ogólnych stosunków UE z tymi partnerami zagranicznymi i uznaje się je za główny czynnik umożliwiający pogłębienie współpracy w wielu dziedzinach; potwierdza to również intensywny i owocny dialog z odnośnymi państwami trzecimi/terytoriami trzecimi, który stanowił podstawę niniejszego przeglądu. W związku z tym szczególnie ważne jest, aby decyzje te przetrwały próbę czasu i pozwalały reagować na zmiany i nowe wyzwania.

2. PRZEDMIOT I METODYKA PRZEGLĄDU

Decyzje stwierdzające odpowiedni stopień ochrony, które są przedmiotem niniejszego przeglądu, zostały przyjęte na podstawie unijnych ram ochrony danych, które poprzedzały RODO. Podczas gdy ostatnie decyzje opublikowano około dziesięć lat temu (np. decyzje w sprawie Nowej Zelandii i Urugwaju, obie przyjęte w 2012 r.), inne obowiązują od ponad dwudziestu lat (np. decyzja w sprawie Kanady, przyjęta w 2001 r., i w sprawie Szwajcarii, przyjęta w 2000 r.). Od tego czasu zmieniły się ramy ochrony danych we wszystkich jedenastu państwach i terytoriach, na przykład wskutek wprowadzenia reform legislacyjnych lub

[20] Należą do nich np. Argentyna, Izrael, Kolumbia, Maroko, Szwajcaria i Urugwaj.

regulacyjnych, zmian w praktyce egzekwowania przepisów przez organy ochrony danych lub w orzecznictwie.

Dokonując oceny, Komisja skoncentrowała się zatem na zmianach ram ochrony danych obowiązujących w odnośnych państwach i na odnośnych terytoriach, które to zmiany miały miejsce od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony. Oceniła ona, w jaki sposób zmiany te przyczyniły się do ukształtowania sytuacji dotyczącej ochrony danych w danym państwie lub terytorium oraz czy, biorąc pod uwagę te zmiany, poszczególne systemy nadal zapewniają odpowiedni poziom ochrony.

W tym celu w pełni uwzględniono zmiany w unijnym systemie ochrony danych, a w szczególności te, które nastąpiły wraz z rozpoczęciem stosowania RODO. W szczególności od czasu przyjęcia tych decyzji stwierdzających odpowiedni stopień ochrony norma prawna mająca zastosowanie do takich decyzji, a także elementy istotne z punktu widzenia oceny, czy system zagraniczny zapewnia odpowiedni poziom ochrony, zostały doprecyzowane w orzecznictwie Trybunału Sprawiedliwości i wytycznych przyjętych przez Grupę Roboczą Art. 29 i jej następcę, Europejską Radę Ochrony Danych[21] (EROD).

W szczególności w wyroku z dnia 6 października 2015 r. w sprawie Schrems I Trybunał Sprawiedliwości stwierdził, że o ile nie można wymagać od państwa trzeciego zapewnienia poziomu ochrony identycznego z tym gwarantowanym w UE, test odpowiedniego stopnia ochrony należy rozumieć jako wymóg zapewnienia „merytorycznie równoważnego" poziomu ochrony[22]. Trybunał doprecyzował w szczególności, że środki, z których korzysta dane państwo trzecie do zapewnienia ochrony danych osobowych, mogą różnić się od środków stosowanych w Unii, o ile w praktyce skutecznie zapewniają odpowiedni stopień ochrony[23]. Test odpowiedniego stopnia ochrony wymaga zatem przeprowadzenia kompleksowej oceny całego systemu państwa trzeciego, w tym istoty zabezpieczeń prywatności, ich rzeczywistego wdrożenia i egzekwowania.

Ponadto Trybunał wyjaśnił, że ocena Komisji nie powinna ograniczać się do ogólnych ram ochrony danych w państwie trzecim, lecz powinna również obejmować reguły dotyczące dostępu organów publicznych do danych osobowych, w szczególności do celów egzekwowania prawa i bezpieczeństwa narodowego[24]. Wykorzystując Kartę praw podstawowych jako punkt odniesienia, Trybunał zidentyfikował szereg wymogów, które przepisy te powinny spełniać, aby zachować zgodność ze standardem „merytorycznej równoważności". Na przykład prawodawstwo w tej dziedzinie powinno zawierać jasne i dokładne reguły dotyczące zakresu i sposobu stosowania rozpatrywanych środków, a także ustanawiać minimalne zabezpieczenia służące temu, aby osoby, których dane osobowe zostają dotknięte ingerencją, miały wystarczające gwarancje rzeczywistej ochrony ich danych przed ryzykiem nadużyć oraz

[21] W skład Europejskiej Rady Ochrony Danych wchodzą organy nadzorcze ds. ochrony danych z państw członkowskich oraz Europejski Inspektor Ochrony Danych.
[22] Schrems I, pkt 73, 74 i 96. Zob. również motyw 104 rozporządzenia (UE) 2016/679, w którym określono standard merytorycznej równoważności.
[23] Schrems I, pkt 74.
[24] Schrems I, pkt 90.

uzyskaniem do nich bezprawnego dostępu i ich wykorzystywaniem[25]. Ponadto powinno ono zapewniać osobom, których dane dotyczą, możliwość dostępu do drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych[26].

RODO opiera się na wyjaśnieniach udzielonych przez Trybunał Sprawiedliwości, określając szczegółowo wykaz elementów, które Komisja musi uwzględnić w swojej ocenie odpowiedniego stopnia ochrony[27]. Ponadto w wyroku w sprawie Schrems II z dnia 16 lipca 2020 r. Trybunał Sprawiedliwości rozwinął kwestię standardu „merytorycznej równoważności", w szczególności w odniesieniu zasad dotyczących dostępu do danych osobowych przez organy publiczne do celów egzekwowania prawa i bezpieczeństwa narodowego. W szczególności Trybunał wyjaśnił, że standard „merytorycznej równoważności" wymaga, aby odpowiednie ramy prawne wiążące dla organów publicznych w odnośnych państwach trzecich i na odnośnych terytoriach zawierały wymogi minimalne zapewniające, aby organy te nie mogły uzyskać dostępu do danych w sposób wykraczający poza to, co jest konieczne i proporcjonalne do osiągnięcia uzasadnionych celów, a osobom, których dane dotyczą, przysługiwały skuteczne i egzekwowalne prawa wobec takich organów[28].

Zmiany standardu odpowiedniego stopnia ochrony znajdują również odzwierciedlenie w wytycznych, które zostały pierwotnie przyjęte przez Grupę Roboczą Art. 29, a następnie zatwierdzone przez EROD[29]. Wytyczne te, a w szczególności dokument dotyczący odpowiedniego stopnia ochrony przekazywanych danych osobowych, zawierają dokładniejsze objaśnienia elementów, jakie Komisja ma obowiązek uwzględnić przy przeprowadzaniu oceny odpowiedniości, w tym przez przedstawienie przeglądu „niezbędnych gwarancji" dotyczących dostępu do danych osobowych przez organy publiczne. Ten ostatni opiera się w szczególności na orzecznictwie Europejskiego Trybunału Praw Człowieka i został zaktualizowany przez EROD, aby uwzględnić objaśnienia przedstawione przez Trybunał Sprawiedliwości w wyroku w sprawie Schrems II[30]. Co ważne, w dokumencie dotyczącym odpowiedniego stopnia ochrony przekazywanych danych osobowych również uznano, że standard „merytorycznej równoważności" nie obejmuje dokładnego odwzorowania („kopii") zasad UE, biorąc pod uwagę, że środki zapewniania porównywalnego poziomu ochrony mogą się różnić w zależności od systemu ochrony prywatności.

W związku z tym, aby ustalić, czy jedenaście decyzji stwierdzających odpowiedni stopień ochrony przyjętych na podstawie poprzednich przepisów nadal spełnia standard określony w RODO, Komisja wzięła pod uwagę nie tylko zmiany ram ochrony danych obowiązujących w odnośnych państwach i na odnośnych terytoriach, ale także zmiany w wykładni w świetle

[25] Schrems I, pkt 91.
[26] Schrems I, pkt 95.
[27] Art. 45 ust. 2 RODO.
[28] Schrems II, pkt 180–182.
[29] Odpowiedni stopień ochrony przekazywanych danych osobowych, WP 254 rev. 01, 6 lutego 2018 r. (dostępny pod adresem: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).
[30] Zob. zalecenia 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru (dostępne pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_pl).

prawa UE samego standardu odpowiedniego stopnia ochrony. Obejmuje to również ocenę ram prawnych regulujących dostęp do danych osobowych przekazywanych z UE i ich wykorzystywanie przez organy publiczne państw lub terytoriów, co do których stwierdzono, że zapewniają odpowiedni poziom ochrony na podstawie art. 25 ust. 6 dyrektywy o ochronie danych.

3. PROCES PRZEGLĄDU

Jak opisano powyżej, w przypadku każdego z odnośnych państw lub terytoriów ocena istniejących decyzji stwierdzających odpowiedni stopień ochrony obejmuje ramy ochrony danych i wszelkie zmiany w odniesieniu do tych ram prawnych, które wprowadzono od czasu przyjęcia ustalenia stwierdzającego odpowiedni stopień ochrony, a także reguły dotyczące dostępu organów publicznych do danych – w szczególności do celów egzekwowania prawa i bezpieczeństwa narodowego. W ostatnich latach służby Komisji podjęły szereg kroków w celu przeprowadzenia tej oceny w ścisłej współpracy z każdym z odnośnych państw lub terytoriów.

Aby pomóc Komisji w wypełnianiu jej obowiązków w zakresie monitorowania, każde z jedenastu państw lub terytoriów przekazało Komisji wyczerpujące informacje na temat zmian w swoim systemie ochrony danych, jakie nastąpiły od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony. Ponadto od każdego z jedenastu państw lub terytoriów Komisja uzyskała szczegółowe informacje na temat reguł dotyczących dostępu organów publicznych do danych osobowych, w szczególności do celów egzekwowania prawa i bezpieczeństwa narodowego, które mają zastosowanie w danym kraju lub na danym terytorium. Komisja gromadziła również pochodzące ze źródeł publicznych, jak również od organów nadzoru i organów ścigania oraz lokalnych ekspertów informacje na temat funkcjonowania decyzji i istotnych zmian w przepisach i praktykach każdego z odnośnych państw i terytoriów, zarówno jeżeli chodzi o przepisy o ochronie danych mające zastosowanie do podmiotów prywatnych, jak i w zakresie dostępu rządowego. Ponadto, w stosownych przypadkach, należycie uwzględniono zobowiązania międzynarodowe podjęte przez te państwa/terytoria w ramach instrumentów regionalnych lub uniwersalnych.

Na tej podstawie Komisja zaangażowała się w intensywny dialog z każdym z odnośnych państw i terytoriów. W kontekście tego dialogu wiele z tych państw i terytoriów zmodernizowało i wzmocniło swoje przepisy dotyczące prywatności poprzez kompleksowe lub częściowe reformy (np. Andora, Kanada, Wyspy Owcze, Szwajcaria, Nowa Zelandia). Było to spowodowane m.in. potrzebą zapewnienia ciągłości decyzji stwierdzających odpowiedni stopień ochrony. Niektóre z tych państw przyjęły przepisy lub wytyczne swojego organu ochrony danych w celu wprowadzenia nowych wymogów w zakresie ochrony danych (np. Izrael, Urugwaj) lub wyjaśnienia niektórych zasad ochrony prywatności (np. Argentyna, Guernsey, Izrael, Jersey, Kanada, Nowa Zelandia, Wyspa Man), w oparciu o praktykę egzekwowania prawa lub orzecznictwo. Ponadto w celu wyeliminowania istotnych różnic w poziomie ochrony wynegocjowano i uzgodniono z niektórymi z odnośnych państw i terytoriów dodatkowe zabezpieczenia dotyczące danych osobowych przekazywanych z Europy, gdy było to konieczne do zapewnienia ciągłości decyzji stwierdzającej odpowiedni

stopień ochrony. Na przykład rząd Kanady rozszerzył prawa dostępu i korekty danych osobowych przetwarzanych przez sektor publiczny na wszystkie osoby fizyczne, niezależnie od ich obywatelstwa lub miejsca zamieszkania (podczas gdy w przeszłości prawa te były dostępne wyłącznie dla obywateli Kanady, stałych rezydentów lub osób fizycznych przebywających w Kanadzie)[31]. Innym przykładem jest wprowadzenie przez rząd Izraela szczególnych zabezpieczeń w celu wzmocnienia ochrony danych osobowych przekazywanych z Europejskiego Obszaru Gospodarczego, które w szczególności tworzą nowe obowiązki w zakresie dokładności danych i zatrzymywania danych, wzmacniają prawa do informacji i usuwania danych oraz wprowadzają dodatkowe kategorie danych wrażliwych[32].

Jednocześnie służby Komisji zebrały opinie Parlamentu Europejskiego (Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych)[33], Rady (za pośrednictwem Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych)[34], EROD[35] i grupy ekspertów ds. RODO z udziałem wielu zainteresowanych stron[36] (w której skład wchodzą przedstawiciele społeczeństwa obywatelskiego, przemysłu, środowiska akademickiego oraz prawników praktyków), a także regularnie informowały te organy o postępach w ocenie.

Niniejsze sprawozdanie oraz towarzyszący mu dokument roboczy służb Komisji (SWD) są zatem wynikiem ścisłej współpracy z każdym z zainteresowanych państw i terytoriów, a także konsultacji z odpowiednimi instytucjami i organami UE oraz informacji zwrotnych od nich otrzymanych. Opierają się one na różnych źródłach, w tym na prawodawstwie, aktach regulacyjnych, orzecznictwie, decyzjach i wytycznych organów ochrony danych, sprawozdaniach (niezależnych) organów nadzoru oraz wkładzie zainteresowanych stron. Przed przyjęciem niniejszego sprawozdania wszystkie wyżej wymienione państwa i terytoria miały możliwość zweryfikowania prawdziwości informacji dostarczonych na temat ich systemu w dokumencie roboczym służb Komisji.

4. NAJWAŻNIEJSZE USTALENIA I WNIOSKI

Pierwszy przegląd wykazał, że od czasu przyjęcia decyzji stwierdzających odpowiedni stopień ochrony ramy ochrony danych obowiązujące w każdym z jedenastu państw lub terytoriów osiągnęły jeszcze większą zbieżność z ramami UE. Ponadto, w dziedzinie dostępu rządu do

[31] Sekcja 12 ustawy o prywatności, pierwsze zarządzenie w sprawie rozszerzenia ustawy o prywatności oraz drugie zarządzenie w sprawie rozszerzenia ustawy o prywatności.
[32] Rozporządzenia w sprawie ochrony prywatności (instrukcje dotyczące danych przekazywanych do Izraela z Europejskiego Obszaru Gospodarczego), 5783-2023, opublikowane w izraelskim dzienniku urzędowym (Reshumut) 7 maja 2023 r.
[33] Zob. np. rezolucja Parlamentu Europejskiego z dnia 25 marca 2021 r. w sprawie sprawozdania Komisji z oceny wdrożenia ogólnego rozporządzenia o ochronie danych po dwóch latach jego stosowania (2020/2717(RSP)), dostępne pod adresem: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_PL.html.
[34] Zob. np. stanowisko i ustalenia Rady dotyczące stosowania ogólnego rozporządzenia o ochronie danych (RODO), przyjęte 19 grudnia 2019 r., dostępne pod adresem: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/pl/pdf
[35] Zob. np. wkład EROD w ocenę RODO na podstawie art. 97, przyjęty 18 lutego 2020 r., dostępny pod adresem: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.
[36] Zob. np. sprawozdanie wielostronnej grupy ekspertów ds. oceny RODO, dostępne pod adresem: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&do=groupDetail.groupMeeting&meetingId=21356.

danych osobowych, pierwszy przegląd wykazał, że prawo tych państw lub terytoriów przewiduje odpowiednie zabezpieczenia i ograniczenia oraz zapewnia mechanizmy nadzoru i dochodzenia roszczeń w tym obszarze.

Szczegółowe ustalenia dotyczące każdego z jedenastu państw lub terytoriów przedstawiono w dokumencie roboczym służb Komisji, który towarzyszy niniejszemu sprawozdaniu. Na podstawie tych ustaleń Komisja stwierdza, że każde z jedenastu państw i terytoriów nadal zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z Unii Europejskiej w rozumieniu RODO, zgodnie z wykładnią Trybunału Sprawiedliwości. Poniżej podsumowano ustalenia dotyczące każdego z odnośnych państw i terytoriów.

4.1. Andora

Komisja z zadowoleniem przyjmuje zmiany w ramach prawnych Andory od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony, w tym zmiany legislacyjne i działania organów nadzorczych. W szczególności przyjęcie kwalifikowanej ustawy nr 29/2021 o ochronie danych osobowych, która weszła w życie w maju 2022 r., przyczyniło się do zwiększenia poziomu ochrony danych, ponieważ ustawa ta jest ściśle zgodna dostosowana do RODO pod względem struktury i głównych elementów.

W obszarze rządowego dostępu do danych osobowych organy publiczne w Andorze podlegają jasnym, precyzyjnym i dostępnym przepisom, zgodnie z którymi takie organy mogą uzyskać dostęp do danych przekazywanych z UE, a następnie je wykorzystywać do celów interesu publicznego, w szczególności do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego. Te ograniczenia i zabezpieczenia wynikają z nadrzędnych ram prawnych i zobowiązań międzynarodowych, w szczególności konstytucji Andory, europejskiej konwencji praw człowieka (EKPC) oraz Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (konwencja nr 108 i protokół zmieniający, ustanawiający zaktualizowaną konwencję nr 108+), a także ze szczegółowych przepisów o ochronie danych mających zastosowanie do przetwarzania danych osobowych w kontekście egzekwowania prawa, które zasadniczo powielają podstawowe elementy dyrektywy (UE) 2016/680[37]. Ponadto prawo andorskie przewiduje szereg szczególnych warunków i ograniczeń dotyczących dostępu organów publicznych do danych osobowych i ich wykorzystywania przez te organy oraz zapewnia mechanizmy nadzoru i dochodzenia roszczeń w tej dziedzinie.

Na podstawie ogólnych ustaleń przedstawionych w dokumencie roboczym służb Komisja stwierdza, że Andora nadal zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z UE.

[37] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

W odniesieniu do szczegółowych przepisów o ochronie danych, które mają obecnie zastosowanie do przetwarzania danych przez organy ścigania, Komisja z zadowoleniem przyjmuje wyrażony przez ustawodawcę Andory zamiar zastąpienia tych przepisów bardziej kompleksowym systemem, który zostanie jeszcze bardziej dostosowany do przepisów obowiązujących w UE. Komisja będzie ściśle monitorowała przyszły rozwój sytuacji w tej dziedzinie.

4.2. Argentyna

Komisja z zadowoleniem przyjmuje zmiany w argentyńskich ramach prawnych od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony, w tym zmiany legislacyjne, orzecznictwo i działania organów nadzorczych, które przyczyniły się do zwiększenia poziomu ochrony danych. W szczególności niezależność argentyńskiego organu nadzorczego ds. ochrony danych znacznie wzmocniono dekretem nr 746/17, w którym powierzono *Agencia de Acceso a la Información Pública* (AAIP) odpowiedzialność za nadzorowanie przestrzegania przepisów o ochronie danych. Ponadto AAIP wydała szereg wiążących rozporządzeń i opinii, w których wyjaśniono, w jaki sposób należy interpretować i stosować ramy ochrony danych w praktyce, co pomogło w aktualizowaniu przepisów o ochronie danych. Argentyna wzmocniła również swoje międzynarodowe zobowiązania w dziedzinie ochrony danych, przystępując w 2019 r. do Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych i do protokołu dodatkowego do niej, a także ratyfikując w 2023 r. protokół zmieniający ustanawiający zaktualizowaną konwencję nr 108+.

W obszarze rządowego dostępu do danych osobowych organy publiczne w Argentynie podlegają jasnym, precyzyjnym i dostępnym przepisom, zgodnie z którymi takie organy mogą uzyskać dostęp do danych przekazywanych z UE, a następnie je wykorzystywać do celów interesu publicznego, w szczególności do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego. Te ograniczenia i zabezpieczenia wynikają z nadrzędnych ram prawnych i zobowiązań międzynarodowych, w szczególności z konstytucji Argentyny, Amerykańskiej Konwencji Praw Człowieka, konwencji nr 108 i konwencji nr 108+, a także z argentyńskich przepisów o ochronie danych (ustawa nr 25.326 o ochronie danych osobowych z dnia 4 października 2000 r.), które mają również zastosowanie do przetwarzania danych osobowych przez argentyńskie organy publiczne, w tym do celów egzekwowania prawa i bezpieczeństwa narodowego. Ponadto prawo argentyńskie przewiduje szereg szczególnych warunków i ograniczeń dotyczących dostępu do danych osobowych i ich wykorzystywania do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego oraz zapewnia mechanizmy nadzoru i dochodzenia roszczeń w tej dziedzinie.

Na podstawie ogólnych ustaleń przedstawionych w dokumencie roboczym służb Komisja stwierdza, że Argentyna nadal zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z UE.

Jednocześnie Komisja zaleca usankcjonowanie w przepisach środków ochrony, które opracowano na poziomie podustawowym, w celu zwiększenia pewności prawa i skonsolidowania tych wymogów. Projekt ustawy o ochronie danych, który niedawno

przedstawiono w argentyńskim Kongresie, może stanowić okazję do skodyfikowania takich zmian, a tym samym dalszego wzmocnienia argentyńskich ram ochrony prywatności. Komisja będzie ściśle monitorowała przyszły rozwój sytuacji w tej dziedzinie.

4.3. Kanada

Komisja z zadowoleniem przyjmuje zmiany w kanadyjskich ramach prawnych od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony, w tym szereg zmian legislacyjnych, orzecznictwo i działania organów nadzorczych, które przyczyniły się do zwiększenia poziomu ochrony danych. W szczególności wzmocniono dodatkowo ustawę o ochronie danych osobowych i dokumentach elektronicznych (PIPEDA), wprowadzając różne zmiany (np. dotyczące warunków ważnej zgody i powiadomień o naruszeniu ochrony danych). Kluczowe wymogi ochrony danych (np. dotyczące przetwarzania danych wrażliwych) zostały natomiast doprecyzowane w orzecznictwie, a także w wytycznych wydanych przez kanadyjski federalny organ ochrony danych – Urząd Komisarza ds. Prywatności. Jednocześnie Komisja zaleca usankcjonowanie w przepisach niektórych środków ochrony, które opracowano na poziomie podustawowym, w celu zwiększenia pewności prawa i skonsolidowania tych wymogów. Trwająca reforma legislacyjna PIPEDA może w szczególności stanowić okazję do skodyfikowania takich zmian, a tym samym dalszego wzmocnienia kanadyjskich ram ochrony prywatności. Komisja będzie ściśle monitorowała przyszły rozwój sytuacji w tej dziedzinie.

W obszarze rządowego dostępu do danych osobowych organy publiczne w Kanadzie podlegają jasnym, precyzyjnym i dostępnym przepisom, zgodnie z którymi takie organy mogą uzyskać dostęp do danych przekazywanych z UE, a następnie je wykorzystywać do celów interesu publicznego, w szczególności do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego. Te ograniczenia i zabezpieczenia wynikają z nadrzędnych ram konstytucyjnych (kanadyjskiej karty praw i wolności), orzecznictwa, szczegółowych przepisów regulujących dostęp do danych, a także przepisów o ochronie danych (tj. ustawy o prywatności i podobnych przepisów na szczeblu prowincji), które mają również zastosowanie do przetwarzania danych osobowych przez kanadyjskie organy publiczne, w tym do celów egzekwowania prawa i bezpieczeństwa narodowego. Ponadto kanadyjski system prawny zapewnia skuteczne mechanizmy nadzoru i dochodzenia roszczeń w tej dziedzinie, w tym poprzez niedawne rozszerzenie praw osób, których dane dotyczą, oraz możliwości dochodzenia roszczeń przez obywateli lub rezydentów spoza Kanady.

Na podstawie ogólnych ustaleń przedstawionych w dokumencie roboczym służb Komisja stwierdza, że Kanada nadal zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z UE odbiorcom podlegającym przepisom PIPEDA. Jak wspomniano powyżej, PIPEDA jest obecnie przedmiotem reformy legislacyjnej, która mogłaby jeszcze bardziej wzmocnić ochronę prywatności, w tym w obszarach istotnych dla stwierdzenia odpowiedniego stopnia ochrony.

4.4. Wyspy Owcze

Komisja z zadowoleniem przyjmuje zmiany w ramach prawnych Wysp Owczych od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony, w tym zmiany legislacyjne,

orzecznictwo i działania organów nadzorczych, które przyczyniły się do zwiększenia poziomu ochrony danych. W szczególności Wyspy Owcze znacznie zmodernizowały swoje ramy ochrony danych, przyjmując ustawę o ochronie danych, która weszła w życie w 2021 r. i zapewniła ścisłe dostosowanie systemu Wysp Owczych do RODO.

W obszarze rządowego dostępu do danych osobowych organy publiczne na Wyspach Owczych podlegają jasnym, precyzyjnym i dostępnym przepisom, zgodnie z którymi takie organy mogą uzyskać dostęp do danych przekazywanych z UE, a następnie je wykorzystywać do celów interesu publicznego, w szczególności do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego. Te ograniczenia i zabezpieczenia wynikają z nadrzędnych ram prawnych i zobowiązań międzynarodowych, w szczególności z ram konstytucyjnych i EKPC, a także ze szczegółowych przepisów regulujących dostęp rządu do danych i przepisów o ochronie danych, które mają zastosowanie do przetwarzania danych osobowych do celów egzekwowania prawa w sprawach karnych (ustawa o przetwarzaniu danych osobowych przez organy ścigania, która weszła w życie na Wyspach Owczych w 2022 r. i która transponuje przepisy przyjęte przez Danię w celu wdrożenia dyrektywy (UE) 2016/680 na Wyspach Owczych) oraz do celów bezpieczeństwa narodowego (są one zawarte w ustawie o Służbie Bezpieczeństwa i Wywiadu). Ponadto w tej dziedzinie dostępne są skuteczne mechanizmy nadzoru i dochodzenia roszczeń.

Na podstawie ogólnych ustaleń przedstawionych w dokumencie roboczym służb Komisja stwierdza, że Wyspy Owcze nadal zapewniają odpowiedni poziom ochrony danych osobowych przekazywanych z UE.

4.5. Guernsey

Komisja z zadowoleniem przyjmuje zmiany w ramach prawnych Guernsey od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony, w tym zmiany legislacyjne i działania organów nadzorczych, które przyczyniły się do zwiększenia poziomu ochrony danych. W szczególności państwo to znacznie zmodernizowało swoje ramy ochrony danych, przyjmując ustawę o ochronie danych dla Baliwatu Guernsey z 2017 r., która obowiązuje od 2019 r. i zapewnia ścisłe dostosowanie systemu Guernsey do RODO.

W obszarze rządowego dostępu do danych osobowych organy publiczne na Guernsey podlegają jasnym, precyzyjnym i dostępnym przepisom, zgodnie z którymi takie organy mogą uzyskać dostęp do danych przekazywanych z UE, a następnie je wykorzystywać do celów interesu publicznego, w szczególności do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego. Te ograniczenia i zabezpieczenia wynikają z nadrzędnych ram prawnych i zobowiązań międzynarodowych, w szczególności EKPC i konwencji nr 108, a także z przepisów Guernsey o ochronie danych, w tym przepisów szczegółowych dotyczących przetwarzania danych osobowych w kontekście egzekwowania prawa ustanowionych w zarządzeniu o ochronie danych (egzekwowanie prawa i sprawy powiązane) dla Bailiwatu Guernsey z 2018 r. Ponadto prawo Guernsey przewiduje szereg szczególnych warunków i ograniczeń dotyczących dostępu do danych osobowych i ich wykorzystywania do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego oraz zapewnia mechanizmy nadzoru i dochodzenia roszczeń w tej dziedzinie.

Na podstawie ogólnych ustaleń przedstawionych w dokumencie roboczym służb Komisja stwierdza, że Guernsey nadal zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z UE.

4.6. Wyspa Man

Komisja z zadowoleniem przyjmuje zmiany w ramach prawnych Wyspy Man od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony, w tym zmiany legislacyjne i działania organów nadzorczych, które przyczyniły się do zwiększenia poziomu ochrony danych. W szczególności Wyspa Man przyjęła w 2018 r. nowe przepisy (ustawa o ochronie danych z 2018 r., uzupełniona zarządzeniem z 2018 r. o ochronie danych (stosowanie RODO)), które włączają większość przepisów zawartych w unijnych ramach ochrony danych do porządku prawnego Wyspy Man, wprowadzając jednocześnie jedynie niewielkie zmiany w konkretnych aspektach, w szczególności w celu dostosowania ram do kontekstu lokalnego.

W obszarze rządowego dostępu do danych osobowych organy publiczne na Wyspie Man podlegają jasnym, precyzyjnym i dostępnym przepisom, zgodnie z którymi takie organy mogą uzyskać dostęp do danych przekazywanych z UE, a następnie je wykorzystywać do celów interesu publicznego, w szczególności do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego. Te ograniczenia i zabezpieczenia wynikają z nadrzędnych ram prawnych i zobowiązań międzynarodowych, w szczególności EKPC i konwencji nr 108, a także z przepisów Wyspy Man o ochronie danych, w tym przepisów szczegółowych dotyczących przetwarzania danych osobowych w kontekście egzekwowania prawa ustanowionych w zarządzeniu o ochronie danych (stosowanie dyrektywy o ochronie danych w sprawach karnych) z 2018 r. i w rozporządzeniach wykonawczych do dyrektywy o ochronie danych w sprawach karnych przyjętych w 2018 r. Ponadto prawo Wyspy Man przewiduje szereg szczególnych ograniczeń dotyczących dostępu do danych osobowych i ich wykorzystywania do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego oraz zapewnia mechanizmy nadzoru i dochodzenia roszczeń w tej dziedzinie.

Na podstawie ogólnych ustaleń przedstawionych w dokumencie roboczym służb Komisja stwierdza, że Wyspa Man nadal zapewniają odpowiedni poziom ochrony danych osobowych przekazywanych z UE.

4.7. Izrael

Komisja z zadowoleniem przyjmuje zmiany w ramach prawnych Szwajcarii od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony, w tym zmiany legislacyjne, orzecznictwo i działania organów nadzorczych, które przyczyniły się do zwiększenia poziomu ochrony danych. W szczególności Izrael wprowadził szczególne zabezpieczenia w celu wzmocnienia ochrony danych osobowych przekazywanych z Europejskiego Obszaru Gospodarczego poprzez przyjęcie rozporządzeń w sprawie ochrony prywatności (instrukcje dotyczące danych przekazywanych do Izraela z Europejskiego Obszaru Gospodarczego), 5783-2023. Izrael wzmocnił również wymogi dotyczące bezpieczeństwa danych, przyjmując rozporządzenia w sprawie ochrony prywatności (bezpieczeństwa danych), 5777-2017, i zwiększył niezależność swojego organu nadzorczego ds. ochrony danych w wiążącej rezolucji rządowej.

W obszarze rządowego dostępu do danych osobowych organy publiczne w Izraelu podlegają jasnym, precyzyjnym i dostępnym przepisom, zgodnie z którymi takie organy mogą uzyskać dostęp do danych przekazywanych z UE, a następnie je wykorzystywać do celów interesu publicznego, w szczególności do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego. Te ograniczenia i zabezpieczenia wynikają z nadrzędnych ram prawnych, w szczególności izraelskiej ustawy zasadniczej, a także z ustawy o ochronie prywatności, 5741–1981, i rozporządzeń przyjętych na jej podstawie, które mają zastosowanie do przetwarzania danych osobowych przez izraelskie organy publiczne, w tym do celów egzekwowania prawa i bezpieczeństwa narodowego. Ponadto prawo izraelskie przewiduje szereg szczególnych ograniczeń dotyczących dostępu do danych osobowych i ich wykorzystywania do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego oraz zapewnia mechanizmy nadzoru i dochodzenia roszczeń w tej dziedzinie.

Opierając się na ogólnych ustaleniach przedstawionych w dokumencie roboczym służb Komisji, można stwierdzić, że Izrael nadal zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z UE.

Jednocześnie Komisja zaleca usankcjonowanie w przepisach środków ochrony, które opracowano na poziomie podustawowym i w orzecznictwie, w celu zwiększenia pewności prawa i ugruntowania tych wymogów. Projekt ustawy o ochronie prywatności (poprawka nr 14), 5722–2022, który niedawno przedstawiono w izraelskim parlamencie, stanowi ważną okazję do skonsolidowania i kodyfikacji takich zmian, a tym samym dalszego wzmocnienia ram ochrony prywatności Izraela. Komisja będzie ściśle monitorowała przyszły rozwój sytuacji w tej dziedzinie.

4.8. Jersey

Komisja z zadowoleniem przyjmuje zmiany w ramach prawnych Szwajcarii od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony, w tym zmiany legislacyjne, orzecznictwo i działania organów nadzorczych, które przyczyniły się do zwiększenia poziomu ochrony danych. W szczególności państwo to znacznie zmodernizowało swoje ramy ochrony danych, przyjmując ustawę o ochronie danych dla Jersey z 2018 r. oraz ustawę o organie ochrony danych dla Jersey z 2018 r., które weszły w życie w 2018 r. i zapewniają ścisłe dostosowanie systemu Jersey do RODO.

W obszarze rządowego dostępu do danych osobowych organy publiczne na Jersey podlegają jasnym, precyzyjnym i dostępnym przepisom, zgodnie z którymi takie organy mogą uzyskać dostęp do danych przekazywanych z UE, a następnie je wykorzystywać do celów interesu publicznego, w szczególności do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego. Te ograniczenia i zabezpieczenia wynikają z nadrzędnych ram prawnych i zobowiązań międzynarodowych, w szczególności EKPC i konwencji nr 108, a także z przepisów Jersey o ochronie danych, w tym przepisów szczegółowych dotyczących przetwarzania danych osobowych w kontekście egzekwowania prawa ustanowionych w ustawie o ochronie danych dla Jersey z 2018 r., zmienionej załącznikiem 1 do tej ustawy. Ponadto prawo Jersey przewiduje szereg szczególnych ograniczeń dotyczących dostępu do danych osobowych i ich wykorzystywania do celów egzekwowania prawa w sprawach karnych

i bezpieczeństwa narodowego oraz zapewnia mechanizmy nadzoru i dochodzenia roszczeń w tej dziedzinie.

Na podstawie ogólnych ustaleń przedstawionych w dokumencie roboczym służb Komisja stwierdza, że Jersey nadal zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z UE.

4.9. Nowa Zelandia

Komisja z zadowoleniem przyjmuje zmiany w ramach prawnych Nowej Zelandii od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony, w tym zmiany legislacyjne, orzecznictwo i działania organów nadzorczych, które przyczyniły się do zwiększenia poziomu ochrony danych. W szczególności system ochrony danych przeszedł kompleksową reformę wraz z przyjęciem ustawy o prywatności z 2020 r., która przyczyniła się do dalszego zwiększenia zbieżności z unijnymi ramami ochrony danych, w szczególności w odniesieniu do przepisów dotyczących międzynarodowego przekazywania danych osobowych oraz uprawnień organu ochrony danych (Urzędu Komisarza ds. Prywatności).

W obszarze rządowego dostępu do danych osobowych organy publiczne w Nowej Zelandii podlegają jasnym, precyzyjnym i dostępnym przepisom, zgodnie z którymi takie organy mogą uzyskać dostęp do danych przekazywanych z UE, a następnie je wykorzystywać do celów interesu publicznego, w szczególności do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego. Te ograniczenia i zabezpieczenia wynikają z nadrzędnych ram konstytucyjnych (np. ustawy o karcie praw) i orzecznictwa, a także z przepisów szczególnych regulujących dostęp rządu do danych oraz z przepisów ustawy o ochronie prywatności, które mają również zastosowanie do przetwarzania danych osobowych przez organy ścigania i organy bezpieczeństwa narodowego. Ponadto w nowozelandzkim systemie prawnym przewidziano różne mechanizmy nadzoru i dochodzenia roszczeń w tej dziedzinie.

Na podstawie ogólnych ustaleń przedstawionych w dokumencie roboczym służb Komisja stwierdza, że Nowa Zelandia nadal zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z UE. Komisja z zadowoleniem przyjmuje również niedawne przedstawienie w parlamencie przez rząd Nowej Zelandii projektu ustawy zmieniającej ustawę o ochronie prywatności z 2020 r. w celu dalszego wzmocnienia obowiązujących wymogów dotyczących przejrzystości. Komisja będzie ściśle monitorowała przyszły rozwój sytuacji w tej dziedzinie.

4.10. Szwajcaria

Komisja z zadowoleniem przyjmuje zmiany w ramach prawnych Szwajcarii od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony, w tym zmiany legislacyjne, orzecznictwo i działania organów nadzorczych, które przyczyniły się do zwiększenia poziomu ochrony danych. Chodzi w szczególności o zaktualizowaną ustawę federalną o ochronie danych, która przyczyniła się do dalszego zbliżenia z unijnymi ramami ochrony danych, zwłaszcza w odniesieniu do ochrony danych wrażliwych i przepisów dotyczących międzynarodowego przekazywania danych. Szwajcaria wzmocniła również swoje międzynarodowe zobowiązania w dziedzinie ochrony danych, ratyfikując we wrześniu 2023 r. konwencję nr 108+.

W obszarze rządowego dostępu do danych osobowych organy publiczne w Szwajcarii podlegają jasnym, precyzyjnym i dostępnym przepisom, zgodnie z którymi takie organy mogą uzyskać dostęp do danych przekazywanych z UE, a następnie je wykorzystywać do celów interesu publicznego, w szczególności do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego. Te ograniczenia i zabezpieczenia wynikają z nadrzędnych ram prawnych i zobowiązań międzynarodowych, w szczególności ze szwajcarskiej konstytucji federalnej, EKPC i konwencji nr 108+, a także ze szwajcarskich przepisów o ochronie danych, w tym z federalnej ustawy o ochronie danych i szczegółowych przepisów o ochronie danych, które mają zastosowanie do egzekwowania prawa w sprawach karnych (np. przepisów zawartych w kodeksie postępowania karnego) i organów bezpieczeństwa narodowego (np. przepisów zawartych w ustawie o służbach wywiadowczych). Ponadto prawo szwajcarskie przewiduje szereg szczególnych ograniczeń dotyczących dostępu do danych osobowych i ich wykorzystywania do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego oraz zapewnia mechanizmy nadzoru i dochodzenia roszczeń w tej dziedzinie.

Na podstawie ogólnych ustaleń przedstawionych w dokumencie roboczym służb Komisja stwierdza, że Szwajcaria nadal zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z UE.

4.11. Urugwaj

Komisja z zadowoleniem przyjmuje zmiany w urugwajskich ramach prawnych od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony, w tym szereg zmian legislacyjnych, orzecznictwo i działania organów nadzorczych, które przyczyniły się do zwiększenia poziomu ochrony danych. W szczególności Urugwaj zaktualizował i wzmocnił swoją ustawę nr 18.331 o ochronie danych osobowych i o środku zaskarżenia „Habeas Data" z 2008 r. w drodze zmian legislacyjnych wprowadzonych w latach 2018 i 2020, które przewidywały rozszerzenie terytorialnego zakresu stosowania przepisów o ochronie danych, wprowadzenie nowych wymogów w zakresie rozliczalności (takich jak oceny skutków, uwzględnianie ochrony danych w fazie projektowania i domyślna ochrona danych, powiadamianie o naruszeniu ochrony danych i wyznaczanie inspektorów ochrony danych) oraz wprowadzenie dodatkowych środków ochrony danych biometrycznych. Urugwaj wzmocnił również swoje międzynarodowe zobowiązania w dziedzinie ochrony danych, przystępując do konwencji nr 108 w 2019 r. oraz ratyfikując konwencję nr 108+ w 2021 r.

W obszarze rządowego dostępu do danych osobowych organy publiczne w Urugwaju podlegają jasnym, precyzyjnym i dostępnym przepisom, zgodnie z którymi takie organy mogą uzyskać dostęp do danych przekazywanych z UE, a następnie je wykorzystywać do celów interesu publicznego, w szczególności do celów egzekwowania prawa w sprawach karnych i bezpieczeństwa narodowego. Te ograniczenia i zabezpieczenia wynikają z nadrzędnych ram prawnych i zobowiązań międzynarodowych, w szczególności z konstytucji Urugwaju, Amerykańskiej Konwencji Praw Człowieka, konwencji nr 108 i konwencji nr 108+, a także z przepisów o ochronie danych zawartych w ustawie nr 18.331 o ochronie danych osobowych i o środku zaskarżenia „Habeas Data", które mają zastosowanie do przetwarzania danych osobowych przez organy publiczne w Urugwaju, w szczególności do celów egzekwowania

prawa i bezpieczeństwa narodowego. Ponadto prawo urugwajskie przewiduje szereg szczególnych warunków i ograniczeń dotyczących dostępu organów publicznych do danych osobowych i ich wykorzystywania przez te organy oraz zapewnia mechanizmy nadzoru i dochodzenia roszczeń w tej dziedzinie.

Na podstawie ogólnych ustaleń dokonanych w ramach niniejszego pierwszego przeglądu Komisja stwierdza, że Urugwaj nadal zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z UE.

5. MONITOROWANIE I WSPÓŁPRACA W PRZYSZŁOŚCI

Komisja uznaje i zdecydowanie docenia doskonałą współpracę z właściwymi organami w każdym z państw i terytoriów, których dotyczy niniejszy przegląd. Komisja będzie nadal uważnie monitorować rozwój sytuacji w zakresie ram ochrony oraz rzeczywistą praktykę odnośnych państw i terytoriów. W przypadku zmian w odpowiednim państwie lub terytorium, które mogłyby negatywnie wpłynąć na poziom ochrony danych uznany za odpowiedni, Komisja w razie potrzeby skorzysta ze swoich uprawnień przewidzianych w art. 45 ust. 5 RODO w celu zawieszenia, zmiany lub cofnięcia decyzji stwierdzającej odpowiedni stopień ochrony.

Niniejszy przegląd potwierdza, że przyjęcie decyzji stwierdzającej odpowiedni stopień ochrony nie jest „punktem końcowym", lecz stanowi okazję do dalszego pogłębienia dialogu i współpracy z partnerami międzynarodowymi o zbieżnych poglądach w zakresie przepływów danych i kwestii cyfrowych w ogólniejszym ujęciu. W związku z tym Komisja liczy na przyszłą wymianę informacji z właściwymi organami w celu dalszego zacieśnienia współpracy na szczeblu międzynarodowym w zakresie propagowania bezpiecznego i swobodnego przepływu danych, w tym poprzez wzmocnioną współpracę w zakresie egzekwowania prawa. Aby pogłębić ten dialog i wspierać wymianę informacji i doświadczeń, w 2024 r. Komisja zamierza zorganizować posiedzenie wysokiego szczebla, w którym wezmą udział przedstawiciele UE i wszystkich państw objętych decyzjami stwierdzającymi odpowiedni stopień ochrony.