DECYZJA WYKONAWCZA KOMISJI (UE) 2023/1795

z dnia 10 lipca 2023 r.

na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE–USA

(notyfikowana jako dokument nr C(2023) 4745)

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając 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 danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) ([1]), w szczególności jego art. 45 ust. 3,

a także mając na uwadze, co następuje:

1. WPROWADZENIE

(1) W rozporządzeniu (UE) 2016/679 ([2]) określono zasady dotyczące przekazywania danych osobowych przez administratorów lub podmioty przetwarzające w Unii do państw trzecich i organizacji międzynarodowych w zakresie, w jakim takie przekazywanie wchodzi w zakres stosowania rozporządzenia. Zasady dotyczące międzynarodowego przekazywania danych określono w rozdziale V tego rozporządzenia. Chociaż przepływ danych osobowych do państw spoza Unii Europejskiej oraz z takich państw jest niezbędnym warunkiem rozwoju handlu transgranicznego i współpracy międzynarodowej, przekazywanie danych osobowych państwom trzecim i organizacjom międzynarodowym nie może obniżać stopnia ochrony zapewnianego tym danym w Unii ([3]).

(2) Zgodnie z art. 45 ust. 3 rozporządzenia (UE) 2016/679 Komisja może w drodze aktu wykonawczego przyjąć decyzję stwierdzającą, że państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim zapewniają odpowiedni stopień ochrony. Przy spełnieniu tego warunku przekazywanie danych osobowych do państwa trzeciego może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia, jak przewidziano w art. 45 ust. 1 i motywie 103 rozporządzenia (UE) 2016/679.

(3) Jak określono w art. 45 ust. 2 rozporządzenia (UE) 2016/679, przy przyjmowaniu decyzji stwierdzającej odpowiedni stopień ochrony należy opierać się na wszechstronnej analizie porządku prawnego państwa trzeciego, obejmującej zarówno jego przepisy dotyczące podmiotów odbierających dane, jak i ograniczenia oraz zabezpieczenia w zakresie dostępu organów publicznych do danych osobowych. W swojej ocenie Komisja musi ustalić, czy dane państwo trzecie daje gwarancje zapewniające stopień ochrony „zasadniczo odpowiadający" stopniowi ochrony zapewnianemu w Unii (motyw 104 rozporządzenia (UE) 2016/679). To, czy tak jest w istocie, należy oceniać w świetle przepisów Unii, w szczególności rozporządzenia (UE) 2016/679, a także orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (Trybunał Sprawiedliwości) ([4]).

([1]) Dz.U. L 119 z 4.5.2016, s. 1.
([2]) Dla ułatwienia, wykaz skrótów stosowanych w niniejszej decyzji znajduje się w załączniku VIII.
([3]) Zob. motyw 101 rozporządzenia (UE) 2016/679.
([4]) Zob. niedawna sprawa C-311/18, Facebook Ireland i Schrems (Schrems II), ECLI:EU:C:2020:559.

(4) Jak wyjaśnił Trybunał Sprawiedliwości w swoim wyroku z dnia 6 października 2015 r. w sprawie C-362/14, Maximillian Schrems/Data Protection Commissioner ([5]) (Schrems), nie oznacza to konieczności stwierdzenia identycznego stopnia ochrony. W szczególności 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 ([6]). Odpowiedni standard ochrony nie wymaga zatem dokładnego powielenia przepisów unijnych. Przy określaniu odpowiedniości chodzi raczej o stwierdzenie, czy biorąc pod uwagę istotę prawa do prywatności oraz jego skuteczne wprowadzenie w życie, egzekwowanie i nadzór nad jego przestrzeganiem, dany zagraniczny system zapewnia jako całość wymagany stopień ochrony ([7]). Ponadto zgodnie z tym wyrokiem przy stosowaniu tego standardu Komisja powinna w szczególności ocenić, czy ramy prawne danego państwa trzeciego zawierają reguły służące do ograniczenia ingerencji w prawa podstawowe osób, których dane zostały przekazane z Unii, których to ingerencji organy państwowe tego kraju mogłyby dokonywać przy okazji dążenia do realizacji uzasadnionego prawem celu, takiego jak bezpieczeństwo narodowe, oraz czy zapewniają skuteczną ochronę prawną przed ingerencjami tego rodzaju ([8]). Wytyczne w tym zakresie zawiera również dokument w sprawie odpowiedniego stopnia ochrony Europejskiej Rady Ochrony Danych, który ma na celu dalsze wyjaśnienie tego standardu ([9]).

(5) Standard obowiązujący w odniesieniu do takiej ingerencji w podstawowe prawa do prywatności i ochrony danych został doprecyzowany przez Trybunał Sprawiedliwości w wyroku z dnia 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Limited i Maximillian Schrems (Schrems II), w którym unieważniono decyzję wykonawczą Komisji (UE) 2016/1250 ([10]) w sprawie dawnych ram dotyczących transatlantyckich przepływów danych, Tarczy Prywatności UE–USA (Tarcza Prywatności). Trybunał Sprawiedliwości uznał, że ograniczenia ochrony danych osobowych, które wynikają z wewnętrznych regulacji Stanów Zjednoczonych dotyczących dostępu i wykorzystywania przez organy amerykańskich władz publicznych takich przekazywanych z Unii do Stanów Zjednoczonych danych do celów ochrony bezpieczeństwa narodowego nie stanowią uregulowania tych ograniczeń w sposób odpowiadający wymogom merytorycznie równoważnym tym ustanowionym w prawie Unii w odniesieniu do konieczności i proporcjonalności takich ingerencji w prawo do ochrony danych ([11]). Trybunał Sprawiedliwości uznał również, że nie było możliwości podniesienia środka odwoławczego przed organem oferującego osobom, których dane są przekazywane do Stanów Zjednoczonych, zabezpieczenia merytorycznie równoważne tym wymaganym w art. 47 karty dotyczącym prawa do skutecznego środka odwoławczego ([12]).

(6) W następstwie wyroku w sprawie Schrems II Komisja rozpoczęła rozmowy z rządem Stanów Zjednoczonych w celu ewentualnego przyjęcia nowej decyzji stwierdzającej odpowiedni stopień ochrony, która spełniałaby wymogi określone w art. 45 ust. 2 rozporządzenia (UE) 2016/679, zgodnie z wykładnią Trybunału Sprawiedliwości. W wyniku przeprowadzonych rozmów Stany Zjednoczone przyjęły w dniu 7 października 2022 r. rozporządzenie wykonawcze 14086 w sprawie wzmocnienia zabezpieczeń na potrzeby amerykańskich działań w zakresie rozpoznania radioelektronicznego (rozporządzenie wykonawcze 14086), które jest uzupełnione zarządzeniem w sprawie Sądu Odwoławczego ds. Ochrony Danych wydanym przez prokuratora generalnego USA (zarządzenie prokuratora generalnego) ([13]). Zaktualizowano ponadto ramy ochrony danych UE–USA (DPF UE–USA lub DPF) – ramy mające zastosowanie do podmiotów komercyjnych przetwarzających dane przekazywane z Unii na podstawie niniejszej decyzji.

(7) Komisja uważnie przeanalizowała prawo i praktykę Stanów Zjednoczonych, w tym rozporządzenie wykonawcze 14086 i zarządzenie prokuratora generalnego. W oparciu o ustalenia przedstawione w motywach 9–200 Komisja stwierdza, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych zgodnie z DPF UE–USA przez administratora lub podmiot przetwarzający w Unii ([14]) certyfikowanym podmiotom w Stanach Zjednoczonych.

([5]) Sprawa C-362/14, Maximilian Schrems/Data Protection Commissioner (Schrems), ECLI:EU:C:2015:650, pkt 73.

([6]) Wyrok w sprawie Schrems, pkt 74.

([7]) Zob. komunikat Komisji do Parlamentu Europejskiego i Rady „Wymiana i ochrona danych osobowych w zglobalizowanym świecie" z dnia 10 stycznia 2017 r., COM(2017) 7, pkt 3.1, s. 6–7.

([8]) Wyrok w sprawie Schrems, pkt 88–89.

([9]) Europejska Rada Ochrony Danych, dokument w sprawie odpowiedniego stopnia ochrony, WP 254 rev.01, dokument dostępny pod adresem: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

([10]) Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA (Dz.U. L 207 z 1.8.2016, s. 1).

([11]) Schrems II, pkt 185.

([12]) Schrems II, pkt 197.

([13]) Tytuł 28 część 302 kodeksu przepisów federalnych.

([14]) Niniejsza decyzja ma znaczenie dla EOG. W Porozumieniu o Europejskim Obszarze Gospodarczym (Porozumienie EOG) przewidziano rozszerzenie rynku wewnętrznego Unii Europejskiej na trzy państwa EOG – Islandię, Liechtenstein i Norwegię. Decyzja Wspólnego Komitetu włączająca rozporządzenie (UE) 2016/679 do załącznika XI do Porozumienia EOG została przyjęta przez Wspólny Komitet EOG w dniu 6 lipca 2018 r. i weszła w życie w dniu 20 lipca 2018 r. Rozporządzenie jest zatem objęte tym porozumieniem. Do celów niniejszej decyzji odniesienia do UE i państw członkowskich UE należy zatem rozumieć jako obejmujące również państwa EOG.

(8) Niniejsza decyzja skutkuje tym, że przekazywanie danych osobowych przez administratorów i podmioty przetwarzające w Unii ([15]) certyfikowanym podmiotom w Stanach Zjednoczonych może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia. Nie ma ona wpływu na bezpośrednie stosowanie rozporządzenia (UE) 2016/679 w odniesieniu do takich podmiotów, jeżeli spełnione są warunki dotyczące terytorialnego zakresu stosowania tego rozporządzenia, określone w jego art. 3.

2. **RAMY OCHRONY DANYCH UE–USA**

2.1. **Zakres podmiotowy i przedmiotowy**

2.1.1. ***Podmioty certyfikowane***

(9) DPF UE–USA opierają się na systemie certyfikacji, zgodnie z którym amerykańskie podmioty zobowiązują się przestrzegać zbioru zasad ochrony prywatności – „zasad ramowych ochrony danych UE–USA", w tym zasad uzupełniających (zwanych dalej łącznie: „zasadami") – wydanych przez Departament Handlu Stanów Zjednoczonych (DoC) i zawartych w załączniku I do niniejszej decyzji ([16]). Aby kwalifikować się do certyfikacji zgodnie z DPF UE–USA, podmiot musi respektować uprawnienia Federalnej Komisji Handlu (FTC) lub Departamentu Transportu Stanów Zjednoczonych (DoT) w zakresie prowadzenia dochodzeń i egzekwowania prawa ([17]). Zasady mają zastosowanie niezwłocznie po certyfikacji. Jak wyjaśniono szczegółowo w motywach 48–52, podmioty objęte DPF UE–USA są zobowiązane do corocznego dokonywania ponownej certyfikacji potwierdzającej ich zobowiązanie do przestrzegania zasad ([18]).

2.1.2. ***Definicja danych osobowych i pojęć administratora i „przedstawiciela"***

(10) Ochrona zapewniana zgodnie z DPF UE–USA ma zastosowanie do wszystkich danych osobowych, które zostały przekazane z Unii do podmiotów w USA, które przyjęły zasady w drodze certyfikacji w DoC, z wyjątkiem danych gromadzonych w celu ich publikacji w prasie, radiu lub telewizji albo w innej formie publicznego rozpowszechnienia materiału dziennikarskiego oraz informacji w uprzednio opublikowanym materiale rozpowszechnionym z archiwów środków masowego przekazu ([19]). Takich danych nie można zatem przekazywać na podstawie DPF UE–USA.

(11) W zasadach dane osobowe zdefiniowano w taki sam sposób jak w rozporządzeniu (UE) 2016/679, tj. jako „dane dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, wchodzące w zakres RODO, otrzymane z UE przez podmiot w Stanach Zjednoczonych i zapisane w dowolnej formie" ([20]). W związku z tym obejmują one również spseudonimizowane (lub „kodowane za pomocą klucza") dane badawcze (również w przypadku, gdy klucz nie jest udostępniany amerykańskiemu podmiotowi otrzymującemu dane) ([21]). Podobnie pojęcie „przetwarzania" jest zdefiniowane jako „każda operacja lub każdy zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych środków, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, dostosowanie lub modyfikacja, odzyskiwanie, przeszukiwanie, wykorzystywanie, ujawnianie lub rozpowszechnianie, a także usuwanie lub niszczenie" ([22]).

(12) DPF UE–USA mają zastosowanie do podmiotów w USA, które kwalifikują się jako administratorzy (tj. jako osoba fizyczna lub podmiot, które samodzielnie lub wspólnie z innymi podmiotami określają cele i sposoby przetwarzania danych osobowych) ([23]) lub podmioty przetwarzające dane (tj. przedstawiciele działający w imieniu administratora) ([24]). Amerykańskie podmioty przetwarzające muszą być zobowiązane umownie do działania wyłącznie zgodnie z instrukcjami unijnego administratora i do wspomagania tego administratora w udzielaniu odpowiedzi osobom

([15]) Niniejsza decyzja nie ma wpływu na wymogi rozporządzenia (UE) 2016/679, które mają zastosowanie do podmiotów (administratorów i podmiotów przetwarzających) w Unii przekazujących dane, na przykład w zakresie ograniczenia celu, minimalizacji danych, przejrzystości i bezpieczeństwa danych (zob. także art. 44 rozporządzenia (UE) 2016/679).

([16]) Zob. w tym zakresie Schrems, pkt 81, w którym Trybunał Sprawiedliwości potwierdził, że system samocertyfikacji może zapewnić odpowiedni poziom ochrony.

([17]) Załącznik I sekcja I pkt 2. FTC posiada szeroką właściwość w obszarze związanym z handlem, z pewnymi wyjątkami, np. w odniesieniu do banków, linii lotniczych, zakładów ubezpieczeń i wspólnej działalności transportowej dostawców usług telekomunikacyjnych (chociaż orzeczenie amerykańskiego sądu apelacyjnego dla dziewiątego okręgu z dnia 26 lutego 2018 r. w sprawie FTC/AT i T potwierdziło, że FTC ma właściwość w obszarze niewspólnej działalności transportowej takich podmiotów). Zob. także załącznik IV przypis 2. DoT jest właściwy do egzekwowania przestrzegania przepisów przez linie lotnicze i agentów sprzedaży biletów (w odniesieniu do transportu lotniczego), zob. załącznik V, sekcja A.

([18]) Załącznik I sekcja III pkt 6.

([19]) Załącznik I sekcja III pkt 2.

([20]) Załącznik I sekcja I pkt 8 lit. a).

([21]) Załącznik I sekcja III pkt 14 lit. g).

([22]) Załącznik I sekcja I pkt 8 lit. b).

([23]) Załącznik I sekcja I pkt 8 lit. c).

([24]) Zob. np. załącznik I sekcja II pkt 2 lit. b) i sekcja II pkt 3 lit. b) i pkt 7 lit. d), w których wyjaśniono, że przedstawiciele działają w imieniu administratora danych, zgodnie z jego instrukcjami i szczególnymi zobowiązaniami umownymi.

fizycznym, które korzystają ze swoich praw wynikających z zasad ([25]). W przypadku dalszego przetwarzania podmiot przetwarzający musi ponadto zawrzeć umowę z podmiotem dokonującym dalszego przetwarzania, gwarantującą taki sam stopień ochrony jak stopień zapewniany przez zasady oraz musi podjąć działania w celu zapewnienia prawidłowego wykonania tej umowy ([26]).

2.2. **Zasady ramowe ochrony danych UE–USA**

2.2.1. ***Ograniczenie celu i wybór***

(13) Dane osobowe powinno się przetwarzać zgodnie z prawem i rzetelnie. Powinny być zbierane w określonym celu, a następnie wykorzystywane tylko w takim zakresie, w jakim nie jest to niezgodne z celem przetwarzania.

(14) W DPF UE–USA zapewniają to różne zasady. Po pierwsze, zgodnie z *zasadą integralności danych i ograniczenia celu* oraz z art. 5 ust. 1 lit. b) rozporządzenia (UE) 2016/679, podmiot nie może przetwarzać danych osobowych w sposób niezgodny z celem, dla którego były one pierwotnie gromadzone lub na który osoba, której dane dotyczą, wyraziła następnie zgodę ([27]).

(15) Po drugie, zanim dojdzie do wykorzystania danych osobowych w nowym (zmienionym) celu, który jest znacząco różny od pierwotnego celu, ale nadal z nim zgodny, lub do ujawnienia ich stronie trzeciej, podmiot musi zapewnić osobom, których dane dotyczą, możliwość wyrażenia sprzeciwu (klauzula *opt-out*), zgodnie z *zasadą wyboru* ([28]), za pomocą jasnego, jednoznacznego i łatwo dostępnego mechanizmu. Co ważne, zasada ta nie zastępuje wyraźnego zakazu przetwarzania danych w sposób niezgodny z zasadami ([29]).

([25]) Załącznik I sekcja III pkt 10 lit. a). Zob. również wytyczne przygotowane przez DoC w porozumieniu z Europejską Radą Ochrony Danych w ramach Tarczy Prywatności, w których wyjaśniono obowiązki amerykańskich podmiotów przetwarzających otrzymujących dane osobowe z Unii zgodnie z przedmiotowymi ramami. Ponieważ przepisy te nie uległy zmianie, wytyczne/FAQ pozostają aktualne w ramach DPF UE-USA (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) Załącznik I sekcja II pkt 3 lit. b).

([27]) Załącznik I sekcja II pkt 5 lit. a). Dopuszczalne cele mogą obejmować audyt, zapobieganie oszustwom lub inne cele zgodne z oczekiwaniami, jakie może mieć racjonalna osoba pod względem gromadzenia danych (zob. załącznik I przypis 6).

([28]) Załącznik I sekcja II pkt 2 lit. a). Nie dotyczy to sytuacji, w których podmiot przekazuje dane osobowe podmiotowi przetwarzającemu działającemu w jego imieniu i zgodnie z jego instrukcjami (załącznik I sekcja II pkt 2 lit. b)). W takim przypadku podmiot musi jednak zawrzeć umowę i zapewnić zgodność z zasadą *odpowiedzialności za dalsze przekazywanie*, opisaną szczegółowo w motywie 43. *Zasada wyboru* (jak również *zasada powiadomienia*) może zostać ponadto ograniczona, gdy dane osobowe są przetwarzane w kontekście badania due diligence (w ramach potencjalnego połączenia lub przejęcia) lub audytów, tak długo oraz w takim zakresie, w jakim jest to konieczne do spełnienia wymogów ustawowych lub wymogów interesu publicznego, lub w takim zakresie i tak długo, jak stosowanie tych zasad naruszałoby prawnie uzasadnione interesy podmiotu w szczególnym kontekście dochodzeń lub badań due diligence (załącznik I sekcja III pkt 4). Zasada uzupełniająca 15 (załącznik I sekcja III pkt 15 lit. a i b) przewiduje również wyjątek od zasady wyboru (jak również od zasad powiadomienia i odpowiedzialności za dalsze przekazywanie) w odniesieniu do danych osobowych pochodzących z ogólnodostępnych źródeł (chyba że podmiot przekazujący dane z UE wskaże, że informacje te podlegają ograniczeniom wiążącym się z koniecznością zastosowania tych zasad) lub danych osobowych pochodzących z ogólnodostępnych rejestrów (o ile nie są one połączone z informacjami z rejestrów niepublicznych i pod warunkiem przestrzegania wszelkich warunków uzyskania dostępu do takich informacji). Podobnie zasada uzupełniająca 14 (załącznik I sekcja III pkt 14 lit. f)) przewiduje wyjątek od zasady *wyboru* (jak również zasad *powiadomienia* i *odpowiedzialności za dalsze przekazywanie*)w odniesieniu do przetwarzania danych osobowych przez przedsiębiorstwo zajmujące się wytwarzaniem produktów farmaceutycznych i wyrobów medycznych przy podejmowaniu działań dotyczących monitorowania bezpieczeństwa stosowania i skuteczności produktów, w zakresie, w jakim zapewnienie zgodności z tymi zasadami uniemożliwia spełnienie wymogów regulacyjnych.

([29]) Ma to zastosowanie do każdorazowego przekazywania danych zgodnie z DPF UE–USA, w tym jeżeli dotyczy to danych zgromadzonych w kontekście stosunku pracy. Chociaż amerykański podmiot certyfikowany może zatem co do zasady wykorzystywać dane o zasobach ludzkich do różnych, niezwiązanych z zatrudnieniem celów (np. niektórych materiałów marketingowych), musi on przestrzegać zakazu przetwarzania danych w sposób niezgodny z zasadami, a ponadto może to czynić wyłącznie zgodnie z zasadami *powiadomienia* i *wyboru*. W wyjątkowych przypadkach podmiot może wykorzystywać dane osobowe do dodatkowego, zgodnego celu nie stosując zasad *powiadomienia* i *wyboru*, ale wyłącznie w okresie i w stopniu, w którym będzie to niezbędne do uniknięcia negatywnego wpływu na zdolność podmiotu do dokonywania awansów, powoływania na stanowiska lub do podejmowania podobnych decyzji dotyczących zatrudnienia (zob. załącznik I sekcja III pkt 9 lit. b) ppkt (iv)). Dzięki zakazowi podejmowania przez amerykański podmiot jakichkolwiek działań odwetowych wobec pracownika, który skorzystał z takiego wyboru, w tym nakładania jakichkolwiek ograniczeń w zakresie możliwości zatrudnienia, pracownik – mimo stosunku podporządkowania i nieodłącznie z nim związanej zależności – będzie wolny od presji, a zatem będzie mógł dokonać naprawdę wolnego wyboru. Zob. załącznik I sekcja III pkt 9 lit. b) ppkt (i).

2.2.2. ***Przetwarzanie szczególnych kategorii danych osobowych***

(16) Jeżeli przetwarzane są „szczególne kategorie danych osobowych", powinny istnieć szczególne zabezpieczenia.

(17) Zgodnie z *zasadą wyboru* szczególne zabezpieczenia mają zastosowanie do przetwarzania „informacji szczególnie chronionych", tj. danych osobowych dotyczących informacji medycznych lub stanu zdrowia, pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych, członkostwa w związkach zawodowych, danych związanych z życiem seksualnym danej osoby lub wszelkich innych informacji przekazanych przez stronę trzecią, które ta strona określa i traktuje jako szczególnie chronione ([30]). Oznacza to, że wszelkie dane uważane za wrażliwe na mocy unijnego prawa o ochronie danych (w tym dane dotyczące orientacji seksualnej, dane genetyczne i dane biometryczne) będą traktowane przez podmioty certyfikowane jako szczególnie chronione zgodnie z DPF UE–USA.

(18) Co do zasady podmioty muszą uzyskać wyraźną zgodę (tj. zezwolenie) osób fizycznych na wykorzystywanie informacji szczególnie chronionych w celach innych niż cele, dla których były pierwotnie gromadzone lub na które osoba fizyczna wyraziła później zgodę (poprzez udzielenie zezwolenia), lub na ujawnienie ich stronom trzecim ([31]).

(19) Nie wymaga się uzyskania takiej zgody w ściśle określonych okolicznościach podobnych do porównywalnych wyjątków przewidzianych w unijnym prawie o ochronie danych, np. gdy przetwarzanie danych wrażliwych leży w żywotnym interesie osoby, jest konieczne do ustalenia roszczeń prawnych, lub jest wymagane do udzielenia opieki medycznej lub postawienia diagnozy ([32]);

2.2.3. ***Prawidłowość, minimalizacja i bezpieczeństwo danych***

(20) Dane powinny być prawidłowe i w stosownych przypadkach uaktualniane. Powinny być również adekwatne, stosowne oraz ograniczone do celów, w których są przetwarzane, a także co do zasady przechowywane przez okres nie dłuższy niż jest to niezbędne do celów, w których przetwarza się dane osobowe.

(21) Zgodnie z *zasadą integralności danych i ograniczenia celu* ([33]) dane osobowe muszą być ograniczone do tego, co jest istotne dla celu przetwarzania. Podmioty muszą ponadto – w zakresie niezbędnym do osiągnięcia celów przetwarzania – podjąć zasadne działania w celu zapewnienia, aby dane osobowe były zgodne ze swoim przeznaczeniem, prawidłowe, kompletne i aktualne.

(22) Dane osobowe można ponadto przechowywać w postaci identyfikującej osobę fizyczną lub umożliwiającej jej zidentyfikowanie (a zatem w postaci danych osobowych) ([34]) wyłącznie dopóty, dopóki służy to celowi lub celom, dla których dane te pierwotnie zgromadzono lub na które osoba fizyczna wyraziła później zgodę zgodnie z *zasadą wyboru*. Obowiązek ten nie uniemożliwia podmiotom dalszego przetwarzania danych osobowych przez dłuższy okres, ale tylko przez taki czas i w takim zakresie, który jest z rozsądnego punktu widzenia potrzebny do osiągnięcia jednego z następujących celów szczegółowych podobnych do porównywalnych wyjątków przewidzianych w unijnym prawie o ochronie danych: archiwizacji w interesie publicznym, badań na potrzeby dziennikarstwa, literatury i sztuki, nauki i historii oraz analizy statystycznej ([35]). Jeśli dane osobowe są przechowywane do jednego z tych celów, ich przetwarzanie podlega gwarancjom zapewnianym przez zasady ([36]).

(23) Dane osobowe powinny być także przetwarzane w sposób zapewniający im bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. W tym celu administratorzy i podmioty przetwarzające powinni wdrożyć odpowiednie środki techniczne lub organizacyjne, aby chronić dane osobowe przed ewentualnymi zagrożeniami. Środki te należy ocenić, biorąc pod uwagę stan wiedzy technicznej, koszty ich wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania, a także zagrożenia dla praw osób fizycznych.

([30]) Załącznik I sekcja II pkt 2 lit. c).
([31]) Załącznik I sekcja II pkt 2 lit. c).
([32]) Załącznik I sekcja III pkt 1.
([33]) Załącznik I sekcja II pkt 5.
([34]) Zob. załącznik I przypis 7, w którym wyjaśniono, że osobę fizyczną uznaje się za „możliwą do zidentyfikowania", o ile podmiot lub strona trzecia może racjonalnie zidentyfikować tę osobę, biorąc pod uwagę środki, jakimi można się racjonalnie posłużyć w celu identyfikacji (uwzględniając między innymi koszt i czas potrzebny do zidentyfikowania danej osoby oraz technologię dostępną w momencie przetwarzania danych).
([35]) Załącznik I sekcja II pkt 5 lit. b).
([36]) *Ibid.*

(24) W DPF UE–USA zapewnia to *zasada bezpieczeństwa*, która wymaga, podobnie jak art. 32 rozporządzenia (UE) 2016/679, stosowania zasadnych i odpowiednich środków bezpieczeństwa, biorąc pod uwagę zagrożenia związane z przetwarzaniem i charakterem danych ([37]).

2.2.4. ***Przejrzystość***

(25) Osoby, których dane dotyczą, powinny być informowane o głównych cechach przetwarzania ich danych osobowych.

(26) Zapewnia to *zasada powiadomienia* ([38]), zgodnie z którą – podobnie jak w przypadku wymogów w zakresie przejrzystości określonych w rozporządzeniu (UE) 2016/679 – podmioty są zobowiązane do przekazania osobom, których dane dotyczą, informacji na temat, między innymi: (i) uczestnictwa podmiotu w DPF, (ii) rodzaju gromadzonych danych, (iii) celu przetwarzania, (iv) rodzaju lub tożsamości stron trzecich, którym dane osobowe mogą zostać ujawnione, oraz celów takiego ujawnienia, (v) ich praw indywidualnych, (vi) sposobu kontaktowania się z podmiotem oraz (vii) dostępnych środków dochodzenia roszczeń.

(27) Powiadomienie to musi być sformułowane jasno i jednoznacznie z chwilą, gdy osoby fizyczne zostały po raz pierwszy poproszone o przekazanie danych osobowych, lub w najbliższym możliwym terminie po zwróceniu się do tych osób o dane osobowe po raz pierwszy, ale w każdym przypadku przed użyciem takich danych w celu znacząco różnym, ale nadal zgodnym, z tym, w którym były one gromadzone, lub przed ujawnieniem ich stronie trzeciej ([39]).

(28) Podmioty muszą ponadto upublicznić swoje strategie polityczne w obszarze ochrony prywatności odzwierciedlające zasady (lub – w przypadku danych dotyczących zasobów ludzkich – udostępnić je osobom, których to dotyczy) oraz zamieścić linki do strony internetowej DoC (wraz z dalszymi szczegółowymi informacjami na temat certyfikacji, praw osób, których dane dotyczą, oraz dostępnych mechanizmów ochrony prawnej), wykaz podmiotów objętych ramami ochrony danych (wykaz DPF) oraz stronę internetową odpowiedniego podmiotu świadczącego usługi w zakresie pozasądowego rozstrzygania sporów ([40]).

2.2.5. ***Prawa indywidualne***

(29) Osobom, których dane dotyczą, powinny przysługiwać określone prawa, które można egzekwować wobec administratora lub podmiotu przetwarzającego, w szczególności prawo dostępu do zebranych danych, prawo do sprzeciwu wobec przetwarzania oraz prawo do sprostowania i usunięcia danych.

(30) Zgodnie z określoną w DPF UE–USA *zasadą dostępu* ([41]) osobom fizycznym przysługują takie prawa. W szczególności osoby, których dane dotyczą, mają prawo, bez konieczności uzasadnienia, uzyskać od podmiotu potwierdzenie, że przetwarza on ich dane osobowe, uzyskać te dane oraz uzyskać informacje o celu przetwarzania, kategoriach przetwarzanych danych osobowych oraz (kategoriach) odbiorców, którym dane są ujawniane ([42]). Podmioty są zobowiązane do udzielania odpowiedzi na wnioski o udostępnienie danych w rozsądnym terminie ([43]). Podmiot może wyznaczyć rozsądne ograniczenia co do liczby wniosków o udostępnienie danych składanych przez daną osobę

([37]) Załącznik I sekcja II pkt 4 lit. a). W odniesieniu do danych o zasobach ludzkich zgodnie z DPF UE–USA wymaga się ponadto od pracodawców uwzględnienia preferencji pracowników w obszarze ochrony prywatności poprzez ograniczanie dostępu do danych osobowych, anonimizację pewnych danych lub przypisywanie kodów lub pseudonimów (załącznik I sekcja III pkt 9 lit. b) ppkt (iii)).

([38]) Załącznik I sekcja II pkt 1.

([39]) Załącznik I sekcja II pkt 1 lit. b). W zasadzie uzupełniającej 14 (załącznik I sekcja III pkt 14 lit. b) i c)) określono przepisy szczególne dotyczące przetwarzania danych osobowych w kontekście badań w dziedzinie zdrowia i badań klinicznych. W szczególności zasada ta umożliwia podmiotom przetwarzanie danych z badań klinicznych nawet po wycofaniu się danej osoby z badania, o ile osoba ta została w jednoznaczny sposób poinformowana o tym fakcie w powiadomieniu przekazanym jej w chwili, gdy wyraziła zgodę na udział w badaniu. Podobnie gdy podmiot objęty DPF UE–USA otrzymuje dane osobowe do celów badań w dziedzinie zdrowia, może je wykorzystywać do nowej działalności badawczej wyłącznie zgodnie z zasadami *powiadomienia* i *wyboru*. W takim przypadku w powiadomieniu przekazanym osobie fizycznej należy zasadniczo zawrzeć informacje o wszelkich przyszłych sposobach korzystania z danych (np. o zamiarze wykorzystania ich do celów związanych prowadzeniem powiązanych badań). W przypadku gdy od samego początku nie jest możliwe uwzględnienie wszystkich przyszłych zastosowań określonych danych (ponieważ decyzja o wykorzystaniu danych do celów związanych z nowymi badaniami może zostać podjęta w rezultacie wyciągnięcia nowych wniosków bądź rozwoju medycyny lub badań), należy zawrzeć wyjaśnienie, że dane osobowe mogą być wykorzystywane do celów związanych z przyszłymi badaniami medycznymi i farmaceutycznymi, których charakteru nie można obecnie przewidzieć. Jeżeli takie dalsze wykorzystanie nie jest spójne z ogólnymi celami badawczymi, dla których zebrano dane (tj. jeżeli nowe cele są zasadniczo różne, ale nadal zgodne z pierwotnym celem, zob. motywy 14–15), należy uzyskać nową zgodę (tj. *opt-in*). Zob. ponadto szczegółowe ograniczenia/wyjątki od zasady *powiadomienia* opisane w przypisie 28.

([40]) Załącznik I sekcja III pkt 6 lit. d).

([41]) Zob. również zasada uzupełniająca dotycząca „dostępu" (załącznik I sekcja III pkt 8).

([42]) Załącznik I sekcja III pkt 8 lit. a) ppkt (i)–(ii).

([43]) Załącznik I sekcja III pkt 8 lit. i).

fizyczną, które zostaną rozpatrzone w określonym okresie, oraz jest uprawniony do pobierania opłaty z tego tytułu, o ile nie będzie ona nadmiernie wysoka, na przykład w przypadku, gdy wnioski o udostępnienie danych są ewidentnie nadużywane, w szczególności ze względu na ich powtarzalność ([44]).

(31) Prawo dostępu może zostać ograniczone wyłącznie w wyjątkowych okolicznościach, podobnych do tych przewidzianych w unijnym prawie o ochronie danych, w szczególności jeżeli istnieje ryzyko naruszenia uzasadnionych praw innych osób; jeżeli obciążenia związane z udzieleniem dostępu lub koszty udzielenia dostępu byłyby nieproporcjonalne w stosunku do zagrożeń dla prywatności osoby fizycznej, biorąc pod uwagę okoliczności danej sprawy (chociaż koszty i obciążenia nie mają decydującego znaczenia przy ustalaniu, czy udzielenie dostępu jest w danym przypadku zasadne); jeżeli ich ujawnienie mogłoby utrudnić zapewnienie ochrony istotnego nadrzędnego interesu publicznego, takiego jak bezpieczeństwo narodowe, bezpieczeństwo publiczne lub obronność; dane zawierają poufne informacje handlowe; lub dane przetwarza się wyłącznie w celach naukowych lub statystycznych ([45]). Każda odmowa lub każde ograniczenie prawa muszą być koniecznie i należycie uzasadnione, przy czym to na podmiocie spoczywa obowiązek wykazania spełnienia wspomnianych wymogów ([46]). Dokonując tej oceny, podmiot musi w szczególności wziąć pod uwagę interesy danej osoby ([47]). Jeśli możliwe jest odseparowanie informacji od innych danych, których dotyczy ograniczenie, podmiot musi utajnić informacje chronione oraz ujawnić pozostałe informacje ([48]).

(32) Osoby, których dane dotyczą, mają ponadto prawo do uzyskania sprostowania lub zmiany nieprawidłowych danych oraz usunięcia danych, które zostały przetworzone z naruszeniem zasad ([49]). Ponadto, jak wyjaśniono w motywie 15, osoby fizyczne mają prawo sprzeciwu wobec przetwarzania ich danych lub prawo do wycofania zgody na przetwarzanie ich danych w celach zasadniczo różnych niż te, w których dane zgromadzono (ale zgodnych z tymi celami), oraz wobec ujawnienia ich danych stronom trzecim. Gdy dane osobowe są wykorzystywane w celach związanych z marketingiem bezpośrednim, osoby fizyczne mają ogólne prawo do wycofania zgody na przetwarzanie w dowolnym momencie ([50]).

(33) Zasady nie odnoszą się konkretnie do kwestii decyzji wpływających na osobę, której dane dotyczą, opierających się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych. Jeżeli jednak chodzi o dane osobowe zebrane w Unii, wszelkie decyzje opierające się na zautomatyzowanym przetwarzaniu podejmowane są zazwyczaj przez administratora w Unii (który ma bezpośrednie powiązanie z zainteresowaną osobą, której dane dotyczą) i bezpośrednio podlegają tym samym przepisom rozporządzenia (UE) 2016/679 ([51]). Obejmuje to scenariusze przekazywania, w których za przetwarzanie odpowiada zagraniczny (np. amerykański) podmiot gospodarczy działający w charakterze przedstawiciela (podmiotu przetwarzającego) w imieniu administratora w Unii (lub działający w charakterze podwykonawcy przetwarzania w imieniu unijnego podmiotu przetwarzającego po otrzymaniu danych od unijnego administratora, który je zebrał), który na tej podstawie podejmuje następnie decyzję.

(34) Zostało to potwierdzone w badaniu zleconym przez Komisję w 2018 r. w kontekście drugiego corocznego przeglądu funkcjonowania Tarczy Prywatności ([52]), w którym stwierdzono, że w tamtym czasie nie było dowodów sugerujących, że podmioty uczestniczące w programie Tarczy Prywatności zwykle podejmowały zautomatyzowane decyzje na podstawie danych osobowych przekazywanych zgodnie z Tarczą Prywatności.

([44]) Załącznik I sekcja III pkt 8 lit. f) ppkt (i)–(ii) oraz lit. g).
([45]) Załącznik I sekcja III pkt 4; pkt 8 lit. b), c), e); pkt 14 lit. e), f) oraz pkt 15 lit. d).
([46]) Załącznik I sekcja III pkt 8 lit. e) ppkt (ii). Podmiot musi poinformować osobę fizyczną o powodach odmowy lub ograniczenia i wskazać punkt kontaktowy, do którego należy kierować ewentualne dalsze pytania, sekcja III pkt 8 lit. a) ppkt (iii).
([47]) Załącznik I sekcja III pkt 8 lit. a) ppkt (ii)–(iii).
([48]) Załącznik I sekcja III pkt 8 lit. a) ppkt (i).
([49]) Załącznik I sekcja II pkt 6 oraz sekcja III pkt 8 lit. a) ppkt (i).
([50]) Załącznik I sekcja III pkt 8 ppkt 12.
([51]) Natomiast w wyjątkowych przypadkach, w których amerykański podmiot ma bezpośrednie powiązanie z osobą z Unii, której dane dotyczą, wynika to zazwyczaj z faktu, że podmiot ten oferuje towary i usługi danej osobie z Unii lub że monitoruje on jej zachowanie. W tym scenariuszu sam amerykański podmiot objęty jest zakresem stosowania rozporządzenia (UE) 2016/679 (art. 3 ust. 2) i ma tym samym obowiązek bezpośrednio przestrzegać unijnych przepisów o ochronie danych.
([52]) SWD(2018) 497 final, pkt 4.1.5. Badanie koncentrowało się na (i) zakresie, w jakim podmioty uczestniczące w programie Tarczy Prywatności w USA podejmują decyzje dotyczące osób fizycznych, opierając się na zautomatyzowanym przetwarzaniu danych osobowych przekazywanych z przedsiębiorstw w UE w ramach Tarczy Prywatności, oraz (ii) gwarancjach dla osób fizycznych, które amerykańskie prawo federalne przewiduje w tego rodzaju sytuacjach, i warunkach stosowania tych gwarancji.

(35) W każdym przypadku w obszarach, w których najbardziej prawdopodobne jest, że przedsiębiorstwa stosują zautomatyzowane przetwarzanie danych osobowych, podejmując decyzje mające wpływ na osoby fizyczne (np. udzielanie kredytów, oferty kredytów, zatrudnienie, mieszkalnictwo i ubezpieczenia), w prawie amerykańskim zagwarantowano szczególne środki ochrony przed niekorzystnymi decyzjami ([53]). Wspomniane akty prawne zazwyczaj zapewniają osobom fizycznym prawo do poznania szczegółowych powodów będących podstawą decyzji (np. odrzucenia wniosku o kredyt), prawo do zakwestionowania niekompletnych lub nieprawidłowych informacji (i podważenia faktu powołania się na czynniki niezgodne z prawem) oraz prawo do ochrony prawnej. W obszarze kredytów konsumenckich ustawa o rzetelnej sprawozdawczości kredytowej i ustawa o równych możliwościach kredytowych zawierają gwarancje, które zapewniają konsumentom pewną formę prawa do zażądania wyjaśnień i prawa do zakwestionowania decyzji. Ustawy te dotyczą szerokiego zakresu dziedzin, między innymi kredytów, zatrudnienia, mieszkalnictwa i ubezpieczeń. Niektóre przepisy antydyskryminacyjne, takie jak tytuł VII ustawy o prawach obywatelskich i ustawa o uczciwych praktykach w mieszkalnictwie, zapewniają ponadto osobom fizycznym ochronę w odniesieniu do modeli wykorzystywanych w zautomatyzowanym podejmowaniu decyzji, które mogą prowadzić do dyskryminacji ze względu na określone cechy, oraz przyznają osobom fizycznym prawa do kwestionowania takich decyzji, w tym decyzji zautomatyzowanych. W odniesieniu do informacji dotyczących zdrowia zasada dotycząca prywatności określona w ustawie o możliwości przenoszenia ubezpieczenia zdrowotnego i odpowiedzialności w zakresie ubezpieczenia zdrowotnego zapewnia określone prawa, które są podobne do tych przewidzianych w rozporządzeniu (UE) 2016/679 odnoszących się do dostępu do osobistych informacji dotyczących zdrowia. W wytycznych amerykańskich organów istnieje ponadto wymóg, by dostawcy usług medycznych otrzymywali informacje, które umożliwią im informowanie osób fizycznych o zautomatyzowanych systemach podejmowania decyzji stosowanych w sektorze medycznym ([54]).

(36) W związku z tym przepisy te zapewniają środki ochrony podobne do środków ochrony przewidzianych w unijnych przepisach o ochronie danych w mało prawdopodobnej sytuacji, w której sam podmiot objęty DPF UE–USA podjąłby zautomatyzowane decyzje.

2.2.6. ***Ograniczenia dotyczące dalszego przekazywania***

(37) Stopień ochrony zapewnianej danym osobowym przekazywanym z Unii podmiotom w Stanach Zjednoczonych nie może zostać obniżony wskutek dalszego przekazywania takich danych odbiorcy ze Stanów Zjednoczonych lub innego państwa trzeciego.

(38) Zgodnie z *zasadą odpowiedzialności za dalsze przekazywanie* ([55]) zasady szczególne mają zastosowanie do tzw. „dalszego przekazywania", tj. przekazywania danych osobowych przez podmiot objęty DPF UE–USA administratorowi lub podmiotowi przetwarzającemu będącymi stroną trzecią, bez względu na to, czy ten administrator lub podmiot przetwarzający ma siedzibę w USA lub w państwie trzecim poza Stanami Zjednoczonymi (i Unią). Wszelkie dalsze przekazywanie może mieć miejsce wyłącznie (i) w ograniczonym i określonym celu, (ii) na podstawie umowy między podmiotem objętym DPF UE–USA a stroną trzecią ([56]) (lub porównywalnego uzgodnienia w ramach grupy przedsiębiorstw ([57])) i (iii) tylko wtedy, gdy umowa ta zobowiązuje stronę trzecią do zapewnienia takiego samego stopnia ochrony jak ten gwarantowany przez zasady.

(39) Ten obowiązek zapewnienia takiego samego stopnia ochrony jak stopień zagwarantowany w zasadach, w związku z *zasadą integralności danych i ograniczenia celu*, oznacza w szczególności, że strona trzecia może tylko przetwarzać przekazane jej dane osobowe do celów zgodnych z celami, dla których je pierwotnie zgromadzono lub dla których osoba fizyczna je następnie zatwierdziła (zgodnie z *zasadą wyboru*).

([53]) Zob. np. ustawa o równych możliwościach kredytowych (tytuł 15 § 1691 i nast. U.S.C.), ustawa o rzetelnej sprawozdawczości kredytowej (tytuł 15 § 1681 i nast. U.S.C.) lub ustawa o uczciwych praktykach w mieszkalnictwie (tytuł 42 § 3601 i nast. U.S.C.). Stany Zjednoczone przyjęły ponadto zasady Organizacji Współpracy Gospodarczej i Rozwoju dotyczące sztucznej inteligencji, które obejmują między innymi zasady dotyczące przejrzystości, zdolności wyjaśniania, bezpieczeństwa i rozliczalności.

([54]) Zob. np. wytyczne dostępne na stronie:2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov.

([55]) Zob. załącznik I sekcja II pkt 3 oraz zasada uzupełniająca „Obowiązkowe umowy dotyczące dalszego przekazywania" (załącznik I sekcja III pkt 10).

([56]) W drodze wyjątku od tej ogólnej zasady dopuszcza się możliwość dalszego przekazywania danych osobowych niewielkiej liczby pracowników przez podmiot bez konieczności zawarcia umowy z odbiorcą w przypadku wystąpienia sporadycznych, związanych z zatrudnieniem potrzeb operacyjnych, np. rezerwacji biletu lotniczego, pokoju hotelowego lub wykupienia polisy ubezpieczeniowej. Również w tym przypadku podmiot nadal musi jednak przestrzegać zasad *powiadomienia* i *wyboru* (zob. załącznik I sekcja III pkt 9 lit. e)).

([57]) Zob. zasada uzupełniająca „Obowiązkowe umowy dotyczące dalszego przekazywania" (załącznik I sekcja III pkt 10 lit. b)). Chociaż zasada ta umożliwia przekazywanie danych w oparciu również o instrumenty pozaumowne (np. wewnątrzgrupowe programy zgodności i kontroli), w tekście wyraźnie zaznaczono, że instrumenty te muszą zawsze „zapewniać ciągłość ochrony danych osobowych zgodnie z zasadami". Co więcej, przyjmując że amerykański podmiot certyfikowany pozostanie odpowiedzialny za zgodność z zasadami, będzie on miał silną motywację do stosowania instrumentów, które istotnie są skuteczne w praktyce.

(40) *Zasadę odpowiedzialności za dalsze przekazywanie* należy interpretować również w związku z *zasadą powiadomienia*, a w przypadku dalszego przekazywania administratorowi danych będącemu stroną trzecią ([58]) – *zasadą wyboru*; zgodnie z tymi zasadami osoby, których dane dotyczą, muszą być (między innymi) informowane o rodzaju/tożsamości jakiegokolwiek odbiorcy będącego stroną trzecią do celu dalszego przekazywania oraz o oferowanym im wyborze, a także mogą sprzeciwić się (wycofać zgodę) lub w przypadku danych wrażliwych udzielić „wyraźnej zgody" na dalsze przekazywanie.

(41) Obowiązek zapewnienia takiego samego stopnia ochrony jak stopień wymagany w zasadach ma zastosowanie do wszystkich stron trzecich zaangażowanych w przetwarzanie danych przekazywanych w taki sposób bez względu na ich położenie (w USA lub w innym państwie trzecim) oraz w przypadku gdy pierwotny odbiorca będący stroną trzecią sam przekazuje te dane innemu odbiorcy będącemu stroną trzecią przykładowo do celów dalszego przetwarzania.

(42) We wszystkich przypadkach w umowie z odbiorcą będącym stroną trzecią należy przewidzieć, aby ten odbiorca powiadomił podmiot objęty DPF UE–USA, jeżeli ustali, że nie jest w stanie dłużej spełniać swojego obowiązku. W przypadku dokonania takiego ustalenia przetwarzanie przez stronę trzecią musi ustać lub konieczne będzie zastosowanie innych zasadnych i właściwych środków, aby znaleźć rozwiązanie zaistniałej sytuacji ([59]).

(43) Dodatkowe środki ochrony mają zastosowanie w przypadku dalszego przekazywania danych przedstawicielowi będącemu stroną trzecią (tj. podmiotowi przetwarzającemu). W takim przypadku amerykański podmiot musi zapewnić, aby przedstawiciel działał wyłącznie zgodnie z jego instrukcjami, i zastosować zasadne i właściwe środki: (i) w celu zapewnienia skutecznego przetwarzania przez przedstawiciela danych osobowych przekazanych w sposób zgodny z obowiązkami tego podmiotu na mocy zasad oraz (ii) w celu zaprzestania nieuprawnionego przetwarzania i naprawienia zaistniałej sytuacji, po otrzymaniu stosownego wniosku ([60]). Podmiot może zostać zobowiązany przez DoC do przedstawienia streszczenia lub poświadczonej kopii postanowień dotyczących prywatności zawartych w umowie ([61]). W przypadku problemów związanych ze zgodnością w łańcuchu (dalszego) przetwarzania podmiot działający jako administrator danych osobowych będzie co do zasady ponosił odpowiedzialność, jak określono w *zasadzie dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności*, chyba że udowodni, że nie jest odpowiedzialny za zdarzenie powodujące szkodę ([62]).

2.2.7. ***Rozliczalność***

(44) Zgodnie z zasadą rozliczalności podmioty przetwarzające dane są zobowiązane do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby skutecznie przestrzegać swoich obowiązków w zakresie ochrony danych oraz być w stanie wykazać taką zgodność, zwłaszcza wobec właściwego organu nadzorczego.

(45) Jeżeli podmiot dobrowolnie zdecyduje się na certyfikację ([63]) zgodnie z DPF UE–USA, ma obowiązek skutecznie przestrzegać zasad, co musi być możliwe do wyegzekwowania. Zgodnie z *zasadą dotyczącą ochrony prawnej, egzekwowania prawa oraz odpowiedzialności* ([64]) podmioty objęte DPF UE–USA muszą przedstawić skuteczne mechanizmy służące zapewnieniu zgodności z zasadami. Podmioty muszą również zastosować środki w celu sprawdzenia ([65]), czy ich polityka ochrony prywatności odpowiada zasadom i czy jest w istocie przestrzegana. Można tego dokonać za pośrednictwem systemu samooceny, który musi obejmować wewnętrzne procedury zapewniające przeszkolenie pracowników w zakresie wdrażania polityki ochrony prywatności danego podmiotu oraz przeprowadzanie okresowego, obiektywnego przeglądu zgodności lub zewnętrznych przeglądów zgodności, które mogą odbywać się w formie audytów lub kontroli wyrywkowych albo poprzez wykorzystanie narzędzi technologicznych.

([58]) Osoby fizyczne nie będą miały prawa do wycofania zgody, jeżeli dane osobowe przekazuje się stronie trzeciej, która działa jako przedstawiciel upoważniony do wykonania czynności w imieniu i zgodnie z instrukcjami amerykańskiego podmiotu. Wymaga to jednak zawarcia umowy z przedstawicielem, a amerykański podmiot będzie odpowiedzialny za zagwarantowanie środków ochrony przewidzianych w zasadach poprzez wykonywanie swoich uprawnień do wydawania instrukcji.

([59]) Sytuacja przedstawia się różnie w zależności od tego, czy strona trzecia jest administratorem, czy też podmiotem przetwarzającym (przedstawicielem). W pierwszym scenariuszu w umowie ze stroną trzecią należy przewidzieć, że podmiot przetwarzający zaprzestanie przetwarzania lub zastosuje inne zasadne i właściwe środki, aby znaleźć rozwiązanie zaistniałej sytuacji. W drugim scenariuszu to podmiot objęty DPF UE–USA – jako podmiot kontrolujący przetwarzanie, którego instrukcje wiążą przedstawiciela w jego działaniach – ma zastosować te środki. Zob. załącznik I sekcja II pkt 3.

([60]) Załącznik I sekcja II pkt 3 lit. b).

([61]) *Ibid.*

([62]) Załącznik I sekcja II pkt 7 lit. d).

([63]) Zob. również zasada uzupełniająca „Samocertyfikacja" (załącznik I sekcja III pkt 6).

([64]) Zob. również zasada uzupełniająca „Rozstrzyganie sporów i egzekwowanie prawa" (załącznik I sekcja III pkt 11).

([65]) Zob. również zasada uzupełniająca „Kontrola" (załącznik I sekcja III pkt 7).

(46) Podmioty muszą ponadto zachowywać dokumenty dotyczące wdrażania praktyk zgodnie z DPF UE–USA oraz udostępniać je na żądanie, w toku dochodzenia bądź badania skargi dotyczącej nieprzestrzegania zasad, niezależnemu organowi ds. rozstrzygania sporów bądź właściwemu organowi egzekwowania prawa ([66]).

2.3. **Zarządzanie, nadzór i egzekwowanie**

(47) Programem DPF UE–USA będzie zarządzał i będzie go monitorował DoC. Ramy te przewidują mechanizmy nadzoru i egzekwowania w celu kontroli i zapewnienia przestrzegania zasad przez podmioty objęte DPF UE–USA oraz usunięcie każdego przypadku nieprzestrzegania zasad. Wspomniane mechanizmy opisano w zasadach (załącznik I) i zobowiązaniach podjętych przez DoC (załącznik III), FTC (załącznik IV) i DoT (załącznik V).

2.3.1. ***(Ponowna) certyfikacja***

(48) Aby dokonać certyfikacji zgodnie z DPF UE–USA (lub corocznej ponownej certyfikacji), podmioty mają obowiązek publicznie zadeklarować swoje zobowiązanie do przestrzegania zasad, udostępnić swoją politykę ochrony prywatności oraz w pełni ją wdrożyć ([67]). W ramach wniosku o (ponowną) certyfikację podmioty muszą przedłożyć DoC informacje dotyczące, między innymi, nazwy odpowiedniego podmiotu, opisu celów, w których podmiot będzie przetwarzał dane osobowe, danych osobowych, które będą objęte certyfikacją, a także wybranej metody kontroli, odpowiedniego niezależnego mechanizmu ochrony prawnej i organu ustawowego właściwego do egzekwowania przestrzegania zasad ([68]).

(49) Podmioty mogą otrzymywać dane osobowe na podstawie DPF UE–USA od dnia umieszczenia ich w wykazie DPF przez DoC. Aby zagwarantować pewność prawa i uniknąć „fałszywych oświadczeń", podmioty dokonujące po raz pierwszy certyfikacji nie mogą publicznie informować o przestrzeganiu przez siebie zasad, zanim DoC nie stwierdzi, że zgłoszenie certyfikacji podmiotu jest kompletne, i nie doda podmiotu do wykazu DPF ([69]). Aby móc nadal korzystać z DPF UE–USA w celu otrzymywania danych osobowych z Unii, podmioty takie muszą co roku ponownie dokonywać certyfikacji swojego uczestnictwa w przedmiotowych ramach. Podmiot, który z jakiegokolwiek powodu wycofuje się z DPF UE–USA, musi usunąć wszelkie oświadczenia, które sugerują, że wciąż aktywnie uczestniczy w ramach ([70]).

(50) Jak wynika z zobowiązań określonych w załączniku III, DoC zweryfikuje, czy podmioty spełniają wszystkie wymogi certyfikacyjne i czy wprowadziły (publiczną) politykę prywatności zawierającą informacje wymagane zgodnie z *zasadą powiadomienia* ([71]). Opierając się na doświadczeniach z procesem (ponownej) certyfikacji w ramach Tarczy Prywatności, DoC przeprowadzi szereg kontroli, między innymi w celu sprawdzenia, czy polityka ochrony prywatności podmiotów zawiera hiperłącze do właściwego formularza skargi na stronie internetowej odpowiedniego mechanizmu rozstrzygania sporów oraz – w przypadku gdy zgłoszenie certyfikacji obejmuje kilka podmiotów i spółek zależnych jednego podmiotu – czy polityka prywatności każdego z tych podmiotów spełnia wymogi certyfikacyjne i jest łatwo dostępna dla osób, których dane dotyczą ([72]). W razie potrzeby DoC przeprowadzi ponadto kontrole krzyżowe z FTC i DoT w celu sprawdzenia, czy podmioty podlegają organowi nadzoru wskazanemu w ich zgłoszeniach (ponownej) certyfikacji, oraz będzie współpracować z organami ds. rozstrzygania sporów stosującymi alternatywne metody rozwiązywania sporów w celu sprawdzenia, czy podmioty są zarejestrowane w niezależnym mechanizmie ochrony prawnej wskazanym w ich zgłoszeniu (ponownej) certyfikacji ([73]).

([66]) Załącznik I sekcja III pkt 7.
([67]) Załącznik I sekcja I pkt 2.
([68]) Załącznik I sekcja III pkt 6 lit. b) oraz załącznik III, zob. „Weryfikacja wymogów samocertyfikacji".
([69]) Załącznik I przypis 12.
([70]) Załącznik I sekcja III pkt 6 lit. h).
([71]) Załącznik I sekcja III pkt 6 lit. a) i przypis 12 oraz załącznik III, zob. sekcja „Weryfikacja wymogów samocertyfikacji".
([72]) Załącznik III sekcja „Weryfikacja wymogów samocertyfikacji".
([73]) Podobnie DoC będzie współpracować ze stroną trzecią, która będzie depozytariuszem środków zebranych w ramach opłaty na rzecz panelu organu ochrony danych (zob. motyw 73) w celu sprawdzenia, czy podmioty wybierające organy ochrony danych jako niezależne mechanizmy ochrony prawnej uiściły opłatę za dany rok. Zob. załącznik III sekcja „Weryfikacja wymogów samocertyfikacji".

(51) DoC poinformuje podmioty, że w celu zakończenia (ponownej) certyfikacji muszą one zaradzić wszystkim problemom zidentyfikowanym podczas przeprowadzonego przez DoC przeglądu. W przypadku gdy podmiot nie odpowie w terminie określonym przez DoC (przy ponownej certyfikacji oczekuje się na przykład, że proces zostanie zakończony w terminie 45 dni) ([74]) lub w inny sposób nie zakończy certyfikacji, zgłoszenie zostanie uznane za wycofane. W takim przypadku każde podanie fałszywych informacji dotyczących uczestnictwa lub zgodności z DPF UE–USA może skutkować podjęciem czynności egzekucyjnych ze strony FTC lub DoT ([75]).

(52) W celu zagwarantowania prawidłowego stosowania DPF UE-USA zainteresowane strony, takie jak osoby, których dane dotyczą, podmioty przekazujące dane i krajowe organy ochrony danych muszą być w stanie identyfikować te podmioty, które przestrzegają zasad. W celu zapewnienia takiej przejrzystości w „punkcie wejścia" DoC zobowiązał się prowadzić i publicznie udostępniać wykaz podmiotów, które przyjęły zasady w drodze certyfikacji oraz podlegają właściwości co najmniej jednego organu egzekwowania prawa wymienionego w załącznikach IV i V do niniejszej decyzji ([76]). DoC będzie aktualizował wykaz na podstawie dokonywanych przez podmioty corocznych zgłoszeń dotyczących ponownej certyfikacji oraz gdy dany podmiot wycofa się lub zostanie usunięty z DPF UE–USA. Ponadto, w celu zapewnienia przejrzystości także w „punkcie wyjścia", DoC będzie prowadził i publicznie udostępniał oficjalny rejestr podmiotów, które usunięto z wykazu, za każdym razem przedstawiając powód takiego usunięcia ([77]). DoC dostarczy ponadto link do strony internetowej FTC dotyczącej DPF UE–USA, zawierającej wykaz czynności egzekucyjnych FTC zgodnie z przedmiotowymi ramami ([78]).

2.3.2. ***Monitorowanie zgodności***

(53) DoC będzie na bieżąco monitorować skuteczne przestrzeganie zasad przez podmioty objęte DPF UE–USA za pomocą różnego rodzaju mechanizmów ([79]). W szczególności DoC będzie przeprowadzać „kontrole wyrywkowe" losowo wybranych podmiotów, a także kontrole wyrywkowe *ad hoc* określonych podmiotów, w przypadku gdy wykryte zostaną potencjalne problemy dotyczące zgodności (np. zgłoszone DoC przez strony trzecie) w celu sprawdzenia, czy (i) osoba lub osoby odpowiedzialne za kontakty zajmujące się rozpatrywaniem skarg i wniosków osób, których dane dotyczą, są dostępne i odpowiednio reagują; (ii) polityka prywatności podmiotu jest łatwo dostępna, zarówno na jego stronie internetowej, jak i za pośrednictwem linku na stronie internetowej DoC; (iii) polityka prywatności podmiotu jest niezmiennie zgodna z wymogami certyfikacyjnymi oraz (iv) wybrany przez podmiot niezależny mechanizm rozstrzygania sporów jest dostępny do rozpatrywania skarg ([80]).

(54) Jeśli istnieją wiarygodne dowody na to, że podmiot nie spełnia swoich zobowiązań wynikających z DPF UE–USA (włącznie z sytuacją, gdy DoC otrzyma skargi lub podmiot nie odpowie na zapytania DoC w zadowalający sposób), DoC zażąda od podmiotu wypełnienia i przedłożenia szczegółowego kwestionariusza ([81]). Podmiot, który nie przedłoży terminowo uzupełnionego w sposób zadowalający kwestionariusza, zostanie skierowany do odpowiedniego organu (FTC lub DoT) w celu podjęcia ewentualnych czynności egzekucyjnych ([82]). Jako element działań w zakresie monitorowania zgodności w ramach Tarczy Prywatności DoC regularnie przeprowadzał wyrywkowe kontrole, o których mowa w motywie 53, i stale monitorował publiczne sprawozdania, co pozwoliło na zidentyfikowanie

([74]) Załącznik III przypis 2.
([75]) Zob. załącznik III sekcja „Weryfikacja wymogów samocertyfikacji".
([76]) Informacje na temat zarządzania wykazem podmiotów objętych DPF można znaleźć w załączniku III (zob. wprowadzenie w części „Zarządzanie i nadzór nad programem ram ochrony danych przez Departament Handlu") oraz w załączniku I (sekcja I pkt 3, sekcja I pkt 4, sekcja III pkt 6 lit. d) i sekcja III pkt 11 lit. g)).
([77]) Załącznik III, zob. wprowadzenie w części „Zarządzanie i nadzór nad programem ram ochrony danych przez Departament Handlu".
([78]) Zob. załącznik III sekcja „Dostosowanie strony internetowej ram ochrony danych do indywidualnych potrzeb docelowych odbiorców".
([79]) Zob. załącznik III sekcja „Dokonywanie z urzędu przeglądów i oceny przestrzegania zasad programu ram ochrony danych".
([80]) W ramach swoich działań monitorujących DoC może korzystać z różnego rodzaju narzędzi, takich jak kontrole niedziałających linków przekierowujących do polityk prywatności lub aktywne monitorowanie wiadomości w poszukiwaniu doniesień dostarczających wiarygodnych dowodów niezgodności.
([81]) Zob. załącznik III sekcja „Dokonywanie z urzędu przeglądów i oceny przestrzegania zasad programu ram ochrony danych".
([82]) Zob. załącznik III sekcja „Dokonywanie z urzędu przeglądów i oceny przestrzegania zasad programu ram ochrony danych".

problemów dotyczących przestrzegania zasad, podjęcie działań zaradczych i rozwiązanie tych problemów ([83]). Podmioty, które uporczywie nie przestrzegają zasad, zostaną usunięte z wykazu podmiotów objętych DPF i będą zobowiązane do zwrócenia lub usunięcia danych osobowych, które otrzymały zgodnie z przedmiotowymi ramami ochrony danych ([84]).

(55) W innych przypadkach usunięcia, np. w przypadku dobrowolnego wycofania się z udziału w programie lub niedopełnienia obowiązku odnowienia certyfikacji, podmiot musi usunąć albo zwrócić takie dane, albo może je zatrzymać, jeżeli co roku przedstawi DoC swoje zobowiązanie do stosowania zasad lub zapewniania odpowiedniej ochrony danych osobowych za pomocą innych zatwierdzonych środków (na przykład stosując umowę w pełni odzwierciedlającą wymogi odpowiednich standardowych klauzul umownych zatwierdzonych przez Komisję) ([85]). W takim przypadku podmiot musi również wskazać osobę odpowiedzialną za kontakty w obrębie podmiotu, która odpowie na wszystkie zapytania związane z DPF UE–USA.

2.3.3. *Identyfikacja fałszywych oświadczeń o uczestnictwie i przeciwdziałanie im*

(56) DoC będzie monitorować wszelkie fałszywe oświadczenia o uczestnictwie w DPF UE–USA lub niewłaściwym użyciu znaku certyfikującego DPF UE–USA, zarówno z urzędu, jak i na podstawie skarg (np. otrzymanych od organów ochrony danych) ([86]). W szczególności DoC będzie na bieżąco sprawdzać, czy podmioty, które (i) wycofały się z udziału w programie DPF UE–USA, (ii) nie dokonały corocznej ponownej certyfikacji (tj. albo rozpoczęły coroczny proces ponownej certyfikacji, ale nie ukończyły go w odpowiednim czasie, albo nawet nie rozpoczęły tego procesu), (iii) zostały usunięte z wykazu uczestników, w szczególności z powodu „uporczywego nieprzestrzegania zasad", lub (iv) nie ukończyły wstępnej certyfikacji (tj. rozpoczęły proces wstępnej certyfikacji, ale nie ukończyły go w odpowiednim czasie), usunęły z wszelkich odpowiednich opublikowanych polityk prywatności odniesienia do DPF UE–USA sugerujące, że podmiot aktywnie uczestniczy w DPF ([87]). DoC przeprowadzi również wyszukiwanie w internecie w celu zidentyfikowania odniesień do DPF UE–USA w politykach prywatności podmiotów, w tym w celu zidentyfikowania fałszywych oświadczeń podmiotów, które nigdy nie były objęte DPF UE–USA ([88]).

(57) W przypadku, gdy DoC stwierdzi, że odniesienia do DPF UE–USA nie zostały usunięte lub są niewłaściwie wykorzystywane, poinformuje podmiot o możliwym zgłoszeniu sprawy do FTC/DoT ([89]). Jeśli podmiot nie odpowie w sposób zadowalający, DoC przekaże sprawę odpowiedniej agencji w celu podjęcia ewentualnych czynności egzekucyjnych ([90]). Każde podanie do publicznej wiadomości fałszywej informacji dotyczącej przestrzegania przez podmiot zasad w postaci wprowadzających w błąd oświadczeń lub praktyk stanowi podstawę wszczęcia postępowania przez FTC, DoT lub inny odpowiedni organ egzekwowania prawa Stanów Zjednoczonych. Podanie DoC fałszywych informacji stanowi podstawę wszczęcia postępowania na podstawie ustawy o fałszywych oświadczeniach (tytuł 18 § 1001 U.S.C.).

([83]) Podczas drugiego rocznego przeglądu Tarczy Prywatności DoC poinformował, że przeprowadził kontrole wyrywkowe 100 podmiotów i w 21 przypadkach przesłał kwestionariusze dotyczące zgodności (po czym wykryte problemy zostały usunięte), zob. SWD(2018) 497 final, s. 9. Podobnie podczas trzeciego rocznego przeglądu Tarczy Prywatności DoC poinformował, że dzięki monitorowaniu publicznych sprawozdań wykrył trzy przypadki naruszeń i rozpoczął działania polegające na przeprowadzaniu kontroli wyrywkowych w 30 przedsiębiorstwach każdego miesiąca, co doprowadziło do działań następczych w postaci kwestionariuszy dotyczących zgodności przesłanych w 28 % przypadków (po czym wykryte problemy zostały natychmiast usunięte lub, w trzech przypadkach, rozwiązane po wystosowaniu pisma zawierającego ostrzeżenia), zob. SWD(2019) 495 final, s. 8.

([84]) Załącznik I sekcja III pkt 11 lit. g). Do uporczywego nieprzestrzegania zasad dochodzi w szczególności, gdy podmiot odmawia zastosowania się do ostatecznego ustalenia dowolnej instytucji samoregulującej ochronę prywatności, niezależnego organu rozstrzygania sporów lub organu egzekwowania prawa.

([85]) Załącznik I sekcja III pkt 6 lit. f).

([86]) Załącznik III sekcja „Wyszukiwanie fałszywych oświadczeń dotyczących uczestnictwa w programie i przeciwdziałanie im".

([87]) *Ibid.*

([88]) *Ibid.*

([89]) *Ibid.*

([90]) W ramach Tarczy Prywatności podczas trzeciego rocznego przeglądu programu DoC poinformował, że zidentyfikował 669 przypadków fałszywych oświadczeń o uczestnictwie (w okresie między październikiem 2018 r. a październikiem 2019 r.), z czego większość spraw została rozwiązana po wystosowaniu przez DoC pisma zawierającego ostrzeżenia, a 143 sprawy zostały skierowane do FTC (zob. motyw 62 poniżej). Zob. SWD(2019) 495 final, s. 10.

2.3.4. ***Egzekwowanie prawa***

(58) W celu zapewnienia odpowiedniego stopnia ochrony danych w praktyce, należy ustanowić niezależny organ nadzorczy, któremu powierzone zostaną uprawnienia do monitorowania i egzekwowania zgodności z przepisami o ochronie danych.

(59) Podmioty objęte DPF UE–USA muszą podlegać jurysdykcji właściwych organów amerykańskich – FTC i DoT – które mają niezbędne uprawnienia do prowadzenia dochodzeń i egzekwowania przepisów prawa w celu skutecznego zapewnienia przestrzegania zasad przez te podmioty ([91]).

(60) FTC jest niezależnym organem składającym się z pięciu komisarzy, którzy są mianowani przez Prezydenta za radą i zgodą Senatu ([92]). Komisarze powoływani są na siedmioletnią kadencję i mogą zostać odwołani przez Prezydenta wyłącznie z powodu braku efektywności, zaniedbania obowiązków lub niewłaściwego sprawowania urzędu. W skład FTC nie może wchodzić więcej niż trzech komisarzy wywodzących się z tej samej partii politycznej, a w okresie swojej kadencji komisarze nie mogą angażować się w żadną inną działalność ani podejmować żadnej innej pracy.

(61) FTC może badać zgodność z zasadami, a także fałszywe oświadczenia o przestrzeganiu zasad lub o udziale w DPF UE–USA składane przez podmioty, które nie figurują już w wykazie DPF albo które nigdy nie dokonały certyfikacji ([93]). FTC może wyegzekwować przestrzeganie zasad za pomocą decyzji administracyjnych lub orzeczeń sądu federalnego (w tym „ugód" uzyskanych w drodze porozumienia) ([94]) o nałożeniu wstępnych lub stałych nakazów lub zakazów sądowych lub innych środków ochrony prawnej i systematycznie będzie monitorować stosowanie się do takich decyzji lub orzeczeń ([95]). Jeżeli podmioty nie przestrzegają takich decyzji lub orzeczeń, FTC może dochodzić sankcji cywilnych i innych środków ochrony prawnej, w tym za wszelkie szkody spowodowane niezgodnym z prawem postępowaniem. Każda ugoda wystawiona na rzecz podmiotu objętego DPF UE–USA będzie zawierała postanowienia dotyczące samozgłaszania ([96]), a podmioty będą zobowiązane do podawania do wiadomości publicznej wszelkich istotnych i związanych z DPF UE–USA sekcji wszelkich przedłożonych FTC sprawozdań dotyczących przestrzegania zasad lub sprawozdań z oceny. Ponadto FTC będzie prowadziło internetowy wykaz podmiotów podlegających decyzjom FTC lub orzeczeniom sądu w sprawach dotyczących DPF UE–USA ([97]).

(62) W odniesieniu do Tarczy Prywatności FTC podjęła czynności egzekucyjne w około 22 sprawach, zarówno w odniesieniu do naruszeń określonych wymogów przedmiotowego programu (np. brak potwierdzenia wobec DoC, że podmiot nieprzerwanie stosował środki ochrony w ramach Tarczy Prywatności po opuszczeniu programu, brak weryfikacji w drodze samooceny albo zewnętrznych przeglądów zgodności z wymogami, że podmiot przestrzegał zasad programu) ([98]), jak i fałszywych oświadczeń o uczestnictwie w programie (np. ze strony podmiotów, które nie wykonały niezbędnych kroków w celu uzyskania certyfikacji lub pozwoliły na jej wygaśnięcie, ale fałszywie twierdziły, że nadal ją posiadają) ([99]). Takie czynności egzekucyjne wynikały między innymi z aktywnego wykorzystania wezwań administracyjnych do uzyskania materiałów od niektórych uczestników programu Tarczy Prywatności w celu sprawdzenia, czy nie doszło do istotnych naruszeń zobowiązań wynikających z Tarczy Prywatności ([100]).

([91]) Podmiot objęty DPF UE–USA musi publicznie zobowiązać się do przestrzegania zasad, podać do wiadomości publicznej stosowaną przez siebie politykę ochrony prywatności opracowaną zgodnie z tymi zasadami i w pełni wdrożyć te zasady. W razie nieprzestrzegania zasad przez podmiot można dochodzić wykonania tego obowiązku na podstawie sekcji 5 ustawy o FTC, w której ustanowiono zakaz podejmowania nieuczciwych i wprowadzających w błąd działań w ramach wymiany handlowej lub mających wpływ na wymianę handlową (tytuł 15 § 45 U.S.C.) oraz na podstawie tytułu 49 § 41712 U.S.C., w którym zakazuje się przewoźnikowi lub pośrednikowi sprzedaży biletów stosowania nieuczciwych lub wprowadzających w błąd praktyk w sprzedaży usług transportu lotniczego lub sprzedaży transportu lotniczego.

([92]) Tytuł 15 § 41 U.S.C.

([93]) ZAŁĄCZNIK IV

([94]) Z informacji przekazanych przez FTC wynika, że FTC nie jest uprawnione do przeprowadzania kontroli na miejscu przy podejmowaniu działań w obszarze ochrony prywatności. FTC może jednak zażądać od podmiotu przedstawienia dokumentów i oświadczeń świadków (zob. sekcja 20 ustawy o FTC) i w przypadku nieprzestrzegania zasad może egzekwować nakazy przedstawienia dokumentów i oświadczeń świadków na drodze sądowej.

([95]) Zob. załącznik IV sekcja „Ubieganie się o wydanie decyzji i zarządzeń i monitorowanie ich przestrzegania".

([96]) Na mocy decyzji FTC lub orzeczeń sądu przedsiębiorstwa są zobowiązane do wdrożenia programów ochrony prywatności i regularnego udostępniania FTC sprawozdań dotyczących przestrzegania zasad lub ocen tych programów przeprowadzonych przez niezależne strony trzecie.

([97]) Załącznik IV sekcja „Ubieganie się o wydanie decyzji i zarządzeń i monitorowanie ich przestrzegania".

([98]) Zob. SWD(2019) 495 final, s. 11.

([99]) Zob. sprawy wymienione na stronie internetowej FTC, dostępnej pod adresem https://www.ftc.gov/business-guidance/privacy-security/privacy-shield Zob. także SWD(2017) 344 final, s. 17; SWD(2018) 497 final, s. 12 oraz SWD(2019) 495 final, s. 11.

([100]) Zob. np. Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review [Uwagi przygotowane przez przewodniczącego Josepha Simonsa na drugim dorocznym przeglądzie Tarczy Prywatności] (ftc.gov).

(63) Ogólniej rzecz biorąc, w ostatnich latach FTC podjęła działania egzekucyjne w szeregu spraw dotyczących zgodności ze szczegółowymi wymogami w zakresie ochrony danych, które są również przewidziane w DPF UE-USA, np. w odniesieniu do zasad ograniczenia celu i przechowywania danych ([101]), minimalizacji danych ([102]), bezpieczeństwa danych ([103]) i dokładności danych ([104]).

(64) Na mocy prawa federalnego DoT dysponuje wyłącznym uprawnieniem do regulowania praktyk ochrony prywatności przewoźników lotniczych i uprawnieniem dzielonym z FTC w odniesieniu do praktyk ochrony prywatności stosowanych przez pośredników sprzedaży biletów w sprzedaży usług transportu lotniczego. Urzędnicy DoT w pierwszej kolejności dążą do osiągnięcia ugody, a jeśli nie jest to możliwe, mogą wszcząć postępowanie egzekucyjne obejmujące postępowanie dowodowe przed sędzią administracyjnym w DoT, uprawnionym do wydawania nakazów zaprzestania stosowania zaskarżonych praktyk i nakładania kar cywilnych ([105]). Sędziowie administracyjni korzystają z szeregu środków ochrony na mocy ustawy o postępowaniu administracyjnym w celu zapewnienia ich niezawisłości i bezstronności. Mogą oni na przykład zostać odwołani z urzędu wyłącznie z ważnego powodu; są przydzielani do spraw rotacyjnie; nie mogą wykonywać działań zawodowych niezgodnych z zakresem ich obowiązków jako sędziów administracyjnych; nie podlegają nadzorowi zespołu dochodzeniowego organu, przez który są zatrudnieni (w tym przypadku DoT); oraz muszą wykonywać swoją funkcję sądowniczą/wykonawczą w sposób bezstronny ([106]). DoT zobowiązany jest monitorować decyzje służące egzekwowaniu przepisów i zapewnić, aby decyzje wydane w sprawach dotyczących DPF UE–USA były dostępne na jego stronie internetowej ([107]).

2.4. **Dochodzenie roszczeń**

(65) W celu zapewnienia odpowiedniej ochrony, a w szczególności egzekwowania praw indywidualnych, osoba, której dane dotyczą, powinna mieć możliwość dochodzenia roszczeń na drodze administracyjnej i sądowej.

(66) DPF UE–USA, za pośrednictwem *zasady dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności*, nakłada na podmioty obowiązek zapewnienia osobom fizycznym, na które fakt nieprzestrzegania zasad wywarł wpływ, możliwości skorzystania z mechanizmu ochrony prawnej, tj. możliwości złożenia przez osoby z Unii, których dane dotyczą, skarg na nieprzestrzeganie zasad przez podmioty objęte DPF UE–USA, a także możliwości rozpatrzenia tych skarg, w razie potrzeby w drodze decyzji zapewniającej skuteczny środek ochrony prawnej ([108]). W ramach podejmowanych działań w obszarze certyfikacji podmioty muszą spełnić wymogi przewidziane w tej zasadzie, zapewniając możliwość skorzystania ze skutecznych i łatwo dostępnych niezależnych mechanizmów ochrony prawnej umożliwiających badanie i szybkie rozstrzyganie skarg oraz sporów poszczególnych osób fizycznych bez konieczności ponoszenia przez nie jakichkolwiek kosztów ([109]).

([101]) Zob. np. postanowienie FTC w sprawie Drizly, LLC, m.in. zobowiązujące przedsiębiorstwo (1) do zniszczenia wszelkich zgromadzonych przez nie danych osobowych, które nie są niezbędne do dostarczania produktów lub świadczenia usług konsumentom, 2) powstrzymania się od gromadzenia lub przechowywania danych osobowych, chyba że jest to konieczne do konkretnych celów określonych w harmonogramie zatrzymywania.

([102]) Zob. np. postanowienie FTC w sprawie CafePress (24 marca 2022 r.), w którym zawarto między innymi wymóg zminimalizowania ilości gromadzonych danych.

([103]) Zob. np. działania egzekucyjne FTC w sprawach Drizzly, LLC i CafePress, w których wymagała ona od odpowiednich przedsiębiorstw wprowadzenia specjalnego programu bezpieczeństwa lub szczególnych środków bezpieczeństwa. Ponadto w odniesieniu do naruszeń ochrony danych zob. również postanowienie FTC z dnia 27 stycznia 2023 r. w sprawie Chegg, ugoda zawarta z Equifax w 2019 r. (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Zob. np. sprawa RealPage, Inc (16 października 2018 r.), w której FTC podjęła działania egzekucyjne na podstawie FCRA przeciwko przedsiębiorstwu zajmującemu się monitorowaniem najemców, które przekazało właścicielom nieruchomości i przedsiębiorstwom zarządzającym nieruchomościami podstawowe sprawozdania na temat osób fizycznych na podstawie informacji z historii najmu, informacji z rejestrów publicznych (w tym historii przestępstw i eksmisji) oraz informacji kredytowych, które wykorzystano jako czynnik decydujący o kwalifikowalności do dostępu do mieszkań. FTC stwierdziła, że przedsiębiorstwo nie wprowadziło racjonalnych środków w celu zapewnienia dokładności informacji, które dostarczyło w oparciu o narzędzie samodecyzyjne.

([105]) Zob. załącznik V sekcja „Praktyki w zakresie egzekwowania prawa".

([106]) Zob. tytuł 5 § 3105, § 7521 lit. a), § 554 lit. d) oraz § 556 lit. b) pkt 3 U.S.C.

([107]) Załącznik V, zob. sekcja „Monitorowanie i publikowanie decyzji służących egzekwowaniu przepisów w sprawach naruszeń DPF UE–USA".

([108]) Załącznik I sekcja II pkt 7.

([109]) Załącznik I sekcja III pkt 11.

(67) Podmioty mogą wybrać niezależne mechanizmy ochrony prawnej w Unii albo w Stanach Zjednoczonych. Jak szczegółowo wyjaśniono w motywie 73, obejmuje to możliwość podjęcia dobrowolnego zobowiązania do współpracy z unijnymi organami ochrony danych. W przypadkach, w których podmioty przetwarzają dane o zasobach ludzkich, takie zobowiązanie do współpracy z unijnymi organami ochrony danych jest obowiązkowe. Wśród innych rozwiązań alternatywnych należy wymienić niezależne pozasądowe rozstrzyganie sporów lub programy prywatności opracowane przez podmioty sektora prywatnego, w które wbudowano przedmiotowe zasady. Wspomniane programy muszą obejmować skuteczne mechanizmy egzekwowania prawa zgodne z wymogami *zasady dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności*.

(68) Tym samym DPF UE–USA zapewnia osobom, których dane dotyczą, szereg środków służących egzekwowaniu przysługujących im praw, składaniu skarg na nieprzestrzeganie zasad przez podmioty prowadzące działania zarówno na rynku unijnym, jak i amerykańskim, a także uzyskanie rozstrzygnięcia takich skarg, w razie potrzeby w drodze decyzji zapewniającej skuteczny środek ochrony prawnej. Osoby fizyczne mogą wnieść skargę bezpośrednio do podmiotu, niezależnego organu ds. rozstrzygania sporów wyznaczonego przez podmiot, krajowych organów ochrony danych, DoC lub FTC. Jeżeli skargi wniesione przez osoby fizyczne nie zostaną rozstrzygnięte w ramach żadnego z wymienionych mechanizmów ochrony prawnej lub egzekwowania prawa, osoby fizyczne mają również prawo poddać sprawę pod arbitraż (załącznik I do załącznika I do niniejszej decyzji). Poza panelem arbitrażowym, do którego można wnieść dany spór wyłącznie po wyczerpaniu określonych środków ochrony prawnej, osoby fizyczne mogą podjąć decyzję o zastosowaniu dowolnego mechanizmu dochodzenia roszczeń lub wszystkich tych mechanizmów jednocześnie i nie są zobowiązane do ograniczenia się wyłącznie do jednego mechanizmu ani do korzystania z nich w określonym porządku.

(69) Po pierwsze, osoby z Unii, których dane dotyczą, mogą zgłaszać roszczenia dotyczące nieprzestrzegania zasad za pośrednictwem osób odpowiedzialnych za bezpośrednie kontakty w podmiotach objętych DPF UE–USA ([110]). Aby ułatwić rozstrzygnięcie sporu, podmiot musi wdrożyć skuteczny mechanizm dochodzenia roszczeń w celu rozpatrywania takich skarg. Dlatego też prowadzona przez dany podmiot polityka ochrony prywatności musi zapewniać osobom fizycznym wyraźne informacje na temat osoby odpowiedzialnej za kontakty wewnątrz podmiotu albo poza podmiotem, która będzie rozpatrywać skargi (w tym wszelkie istotne organy w Unii, które mogą odpowiadać na zapytania lub skargi), oraz na temat wyznaczonego niezależnego organu ds. rozstrzygania sporów (zob. motyw 70). Po otrzymaniu skargi złożonej przez osobę fizyczną bezpośrednio lub za pośrednictwem DoC w następstwie zgłoszenia przez organ ochrony danych podmiot musi, w terminie 45 dni, udzielić odpowiedzi osobie z Unii, której dane dotyczą ([111]). Podobnie podmioty są zobowiązane do bezzwłocznego reagowania na zapytania i inne wnioski o udzielenie informacji złożone przez DoC lub organ ochrony danych ([112]) (jeżeli podmiot zobowiązał się do współpracy z organem ochrony danych) dotyczące przestrzegania przez nie zasad.

(70) Po drugie, osoby fizyczne mogą również wnieść skargę bezpośrednio do niezależnego organu ds. rozstrzygania sporów (w Stanach Zjednoczonych albo Unii) wyznaczonego przez podmiot w celu badania i rozstrzygania skarg osób fizycznych (chyba że są w oczywisty sposób bezpodstawne lub niepoważne) oraz zapewnienia właściwej nieodpłatnej ochrony prawnej osobie fizycznej ([113]). Sankcje i środki ochrony prawnej nałożone przez taki organ muszą być wystarczająco rygorystyczne, aby zapewnić przestrzeganie zasad przez podmioty, oraz powinny przewidywać usunięcie lub skorygowanie przez podmiot skutków nieprzestrzegania zasad oraz, w zależności od okoliczności, zakończenie dalszego przetwarzania danych osobowych lub ich usunięcie, a także podanie do publicznej wiadomości stwierdzonych przypadków nieprzestrzegania zasad ([114]). Wyznaczone przez podmiot niezależne organy ds. rozstrzygania sporów będą zobowiązane do umieszczania na swoich ogólnodostępnych stronach internetowych stosownych informacji na temat DPF UE–USA i usług, jakie świadczą w ramach tego programu ([115]). Co roku muszą publikować sprawozdanie roczne zawierające zagregowane dane statystyczne dotyczące takich usług ([116]).

([110]) Załącznik I sekcja III pkt 11 lit. d) ppkt (i).
([111]) Załącznik I sekcja III pkt 11 lit. d) ppkt (i).
([112]) Tj. organ zajmujący się zapytaniami wyznaczony przez grupę organów ochrony danych przewidzianą w ramach zasady uzupełniającej dotyczącej „Roli organów ochrony danych" (załącznik I sekcja III pkt 5).
([113]) Załącznik I sekcja III pkt 11 lit. d).
([114]) Załącznik I sekcja II pkt 7 oraz sekcja III pkt 11 lit. e).
([115]) Załącznik I sekcja III pkt 11 lit. d) ppkt (ii).
([116]) Sprawozdanie roczne musi zawierać następujące informacje: 1) łączną liczbę skarg związanych z DPF UE–USA otrzymanych w roku sprawozdawczym; 2) rodzaje otrzymanych skarg; 3) wskaźniki pomiaru jakości rozstrzygania sporów, np. czas niezbędny do rozpatrzenia skarg; oraz 4) wyniki rozpatrywania otrzymanych skarg, w szczególności liczbę i rodzaj zastosowanych środków ochrony prawnej lub nałożonych sankcji.

(71) W ramach swoich procedur kontroli zgodności DoC może sprawdzić, czy podmioty objęte DPF UE–USA faktycznie zarejestrowały się, jak twierdzą, w niezależnych mechanizmach ochrony prawnej ([117]). Zarówno podmioty, jak i odpowiedzialne niezależne mechanizmy ochrony prawnej są zobowiązane do bezzwłocznego reagowania na złożone przez DoC zapytania i wnioski o informacje dotyczące DPF UE–USA. DoC będzie współpracować z niezależnymi mechanizmami ochrony prawnej w celu zweryfikowania, czy na swoich stronach internetowych podmioty te podają informacje dotyczące zasad i usług, które świadczą zgodnie z DPF UE–USA oraz czy publikują sprawozdania roczne ([118]).

(72) W przypadkach, w których podmiot nie zastosuje się do orzeczenia organu ds. rozstrzygania sporów lub organu samoregulacyjnego, ten ostatni musi zgłosić taki przypadek DoC i FTC (lub innemu amerykańskiemu organowi właściwemu do badania przypadków nieprzestrzegania zasad przez podmioty) lub właściwemu sądowi ([119]). Jeżeli podmiot odmówi zastosowania się do ostatecznego ustalenia dowolnego organu samoregulacyjnego ds. ochrony prywatności, niezależnego organu ds. rozwiązywania sporów lub organu rządowego lub gdy organ taki uzna, że podmiot często nie przestrzega zasad, sytuacja taka może zostać uznana za uporczywe nieprzestrzeganie zasad, w rezultacie czego DoC – po przekazaniu podmiotowi nieprzestrzegającemu zasad stosownego powiadomienia z trzydziestodniowym wyprzedzeniem, aby zapewnić mu możliwość ustosunkowania się do zarzutów – skreśli ten podmiot z wykazu podmiotów objętych DPF ([120]). Jeżeli po usunięciu podmiotu z wykazu w dalszym ciągu będzie on deklarował zgodność z zasadami DPF UE–USA, DoC przekaże sprawę do rozpoznania FTC lub innemu organowi egzekwowania prawa ([121]).

(73) Po trzecie, osoby fizyczne mogą również wnosić skargi do krajowego organu ochrony danych w Unii, który może skorzystać ze swoich uprawnień dochodzeniowych i naprawczych na mocy rozporządzenia (UE) 2016/679. Podmioty są zobowiązane do współpracy przy badaniu i rozstrzyganiu skarg przez organ ochrony danych, jeżeli dotyczą one przetwarzania danych o zasobach ludzkich gromadzonych w kontekście stosunku pracy albo jeżeli dany podmiot dobrowolnie poddał się nadzorowi organów ochrony danych ([122]). W szczególności podmioty muszą odpowiadać na zapytania, postępować zgodnie z zaleceniami organów ochrony danych, w tym środkami ochrony prawnej lub środkami odszkodowawczymi, oraz przekazywać organowi ochrony danych pisemne potwierdzenie o podjęciu takich działań ([123]). W przypadku niezastosowania się do porady udzielonej przez organ ochrony danych organ ten przekazuje takie sprawy do DoC (który może usunąć podmioty z wykazu DPF UE-USA) lub, w przypadku ewentualnych działań egzekucyjnych, do FTC lub DoT (z powodu braku współpracy z organami ochrony danych lub nieprzestrzegania zasad na mocy prawa amerykańskiego można podjąć działania) ([124]).

(74) W celu ułatwienia współpracy w zakresie skutecznego rozpatrywania skarg zarówno DoC, jak i FTC ustanowiły specjalne stanowisko osoby odpowiedzialnej za kontakty, odpowiadającej za bezpośrednie kontakty z organami ochrony danych ([125]). Takie osoby odpowiedzialne za kontakty pomagają w przypadku zapytań organu ochrony danych dotyczących zgodności podmiotu z zasadami.

(75) Porady organów ochrony danych ([126]) są udzielane dopiero wówczas, gdy obie strony sporu miały należytą możliwość wypowiedzenia się i przedstawienia wszystkich dowodów zgodnie z własnym uznaniem. Panel może przekazać porady tak szybko, jak stanowi wymóg należytej procedury, i co do zasady w ciągu 60 dni po otrzymaniu skargi ([127]). Jeżeli podmiot nie zastosuje się do porad w ciągu 25 dni od ich otrzymania i nie poda zadowalającego usprawiedliwienia takiego opóźnienia, panel może zawiadomić go o swoim zamiarze przekazania sprawy FTC (lub innemu właściwemu amerykańskiemu organowi egzekwowania prawa) albo o zamiarze stwierdzenia poważnego naruszenia zobowiązania do współpracy. W pierwszym przypadku może to prowadzić do podjęcia czynności egze-

([117]) Załącznik I sekcja „Weryfikacja wymogów samocertyfikacji".
([118]) Zob. załącznik III sekcja „Ułatwianie współpracy z organami pozasądowego rozstrzygania sporów świadczącymi usługi związane z zasadami". Zob. także załącznik I sekcja III pkt 11 lit. d) ppkt (ii)–(iii).
([119]) Zob. załącznik I sekcja III pkt 11 lit. e).
([120]) Zob. załącznik I sekcja III pkt 11 lit. g), w szczególności ppkt (ii) i (iii).
([121]) Zob. załącznik III sekcja „Wyszukiwanie fałszywych oświadczeń dotyczących uczestnictwa w programie i podejmowanie działań zaradczych".
([122]) Załącznik I sekcja II pkt 7 lit. b).
([123]) Załącznik I sekcja III pkt 5.
([124]) Załącznik I sekcja III pkt 5 lit c) ppkt (ii).
([125]) Załącznik III (zob. sekcja „Ułatwianie współpracy z organami ochrony danych") i załącznik IV (zob. sekcje „Określanie pierwszeństwa zgłoszeń i ich badanie" oraz „Współpraca w zakresie egzekwowania prawa z unijnymi organami ochrony danych").
([126]) Organy ochrony danych powinny przyjąć regulamin nieformalnego panelu organów ochrony danych w oparciu o ich zdolność do organizacji pracy i wzajemnej współpracy.
([127]) Załącznik I sekcja III pkt 5 lit c) ppkt (i).

kucyjnych na podstawie sekcji 5 ustawy o FTC (lub podobnej ustawy) ([128]). W drugim przypadku panel poinformuje DoC, który uzna fakt niezastosowania się przez podmiot do wydanych przez panel organów ochrony danych zaleceń za uporczywe nieprzestrzeganie zasad, co doprowadzi do usunięcia podmiotu z wykazu podmiotów objętych DPF.

(76) Jeżeli organ ochrony danych, do którego skierowano skargę, nie podejmie żadnego działania w celu rozstrzygnięcia skargi lub podjęte przez niego działanie okaże się niewystarczające, skarżący będący osobą fizyczną może zaskarżyć takie działanie (zaniechanie) do sądów krajowych danego państwa członkowskiego UE.

(77) Osoby fizyczne mogą również wnieść skargi do organów ochrony danych nawet w przypadku, gdy panel organów ochrony danych nie został wyznaczony jako organ ds. rozstrzygania sporów danego podmiotu. W takich przypadkach organ ochrony danych może przekazać otrzymane skargi do rozpoznania przez DoC albo FTC. Aby ułatwić i pogłębić współpracę w kwestiach dotyczących skarg wnoszonych przez osoby fizyczne i nieprzestrzegania zasad przez podmioty objęte DPF UE–USA, DoC powoła specjalną osobę odpowiedzialną za kontakty, która będzie działała jako łącznik oraz będzie pomagać organowi ochrony danych w udzielaniu odpowiedzi na zapytania dotyczące przestrzegania zasad przez dany podmiot ([129]). Podobnie FTC zobowiązało się do ustanowienia specjalnej osoby odpowiedzialnej za kontakty ([130]).

(78) Po czwarte, DoC zobowiązał się do przyjmowania i rozpatrywania skarg oraz dokładania wszelkich starań w celu rozstrzygnięcia skarg dotyczących nieprzestrzegania zasad przez podmioty ([131]). W tym celu DoC zapewnia organom ochrony danych szczegółowe procedury przekazywania skarg osobie wyznaczonej do kontaktów, śledzenia ich oraz kontaktowania się z podmiotami w celu ułatwienia procesu rozstrzygania skarg ([132]). Aby przyspieszyć proces rozpatrywania skarg osób fizycznych, osoba wyznaczona do kontaktów współpracuje bezpośrednio z odpowiednim organem ochrony danych w kwestiach przestrzegania zasad, a w szczególności przekazuje mu aktualne informacje na temat statusu skarg w okresie nie dłuższym niż 90 dni od daty zgłoszenia ([133]). Dzięki temu osoby, których dane dotyczą, będą mogły składać skargi dotyczące nieprzestrzegania zasad przez podmioty objęte DPF UE–USA bezpośrednio ich krajowemu organowi ochrony danych, który następnie przekaże je DoC jako amerykańskiemu organowi zarządzającemu DPF UE–USA.

(79) Jeżeli, na podstawie kontroli przeprowadzonej z urzędu, skarg lub innych informacji, DoC stwierdzi, że podmiot uporczywie nie przestrzega zasad ochrony prywatności, wówczas może usunąć taki podmiot z wykazu podmiotów objętych DPF ([134]). Odmowa zastosowania się do ostatecznego ustalenia dowolnej instytucji samoregulującej ochronę prywatności, niezależnego organu rozstrzygania sporów lub organu rządowego, w tym organu ochrony danych, zostanie uznana za uporczywe nieprzestrzeganie zasad ([135]).

(80) Po piąte, podmiot objęty DPF UE–USA musi podlegać jurysdykcji organów amerykańskich, w szczególności FTC ([136]), które mają niezbędne uprawnienia w zakresie prowadzenia dochodzeń i egzekwowania prawa, aby skutecznie zapewnić przestrzeganie zasad przez ten podmiot. FTC priorytetowo traktuje zgłoszenia dotyczące nieprzestrzegania zasad otrzymane od niezależnego organu ds. rozstrzygania sporów lub organu samoregulacyjnego, DoC i organów ochrony danych (działających z własnej inicjatywy lub na podstawie skarg), aby ustalić, czy doszło do naruszenia przepisów sekcji 5 ustawy o FTC ([137]). FTC zobowiązało się do ustanowienia standardowego procesu zgłaszania, wyznaczenia osoby odpowiedzialnej za kontakty w agencji, która będzie zajmowała się zgłoszeniami organów ochrony danych, oraz do wymiany informacji na temat zgłoszeń. Ponadto FTC może przyjmować skargi bezpośrednio od osób fizycznych i z urzędu przeprowadzać dochodzenia dotyczące DPF UE–USA, w szczególności w ramach szerzej zakrojonych dochodzeń dotyczących kwestii prywatności.

([128]) Załącznik I sekcja III pkt 5 lit c) ppkt (ii).
([129]) Zob. załącznik III sekcja „Ułatwianie współpracy z organami ochrony danych".
([130]) Zob. załącznik IV sekcje „Określanie pierwszeństwa zgłoszeń i ich badanie" oraz „Współpraca w zakresie egzekwowania prawa z unijnymi organami ochrony danych".
([131]) Załącznik III, zob. np. sekcja „Ułatwianie współpracy z organami ochrony danych".
([132]) Załącznik I sekcja II pkt 7 lit. e) oraz załącznik III sekcja „Ułatwianie współpracy z organami ochrony danych".
([133]) *Ibid.*
([134]) Załącznik I sekcja III pkt 11 lit. g).
([135]) Załącznik I sekcja III pkt 11 lit. g).
([136]) Podmiot objęty DPF UE–USA musi publicznie zobowiązać się do przestrzegania zasad, podać do wiadomości publicznej stosowaną przez siebie politykę ochrony prywatności opracowaną zgodnie z tymi zasadami i w pełni wdrożyć te zasady. W razie nieprzestrzegania zasad przez podmiot można dochodzić wykonania tego obowiązku na podstawie sekcji 5 ustawy o FTC, w której ustanowiono zakaz podejmowania nieuczciwych i wprowadzających w błąd działań w ramach wymiany handlowej lub mających wpływ na wymianę handlową.
([137]) Zob. także podobne zobowiązania podjęte przez DoT, załącznik V.

(81) Po szóste, w ramach mechanizmu ochrony prawnej „ostatniej szansy", w przypadku gdy żadne z pozostałych dostępnych środków odwoławczych nie przyniosły zadowalającego rozstrzygnięcia skargi osoby fizycznej, osoba z Unii, której dane dotyczą, może poddać sprawę pod arbitraż panelu ds. ram ochrony danych UE–USA (panel DPF UE–USA) ([138]). Podmioty muszą poinformować osoby fizyczne o możliwości wystąpienia o arbitraż i są zobowiązane do udzielenia odpowiedzi, w przypadku gdy dana osoba fizyczna zdecyduje się skorzystać z tej możliwości, przekazując powiadomienie stosownemu podmiotowi ([139]).

(82) Panel DPF UE–USA składa się z co najmniej dziesięciu arbitrów, którzy zostaną wyznaczeni przez DoC i Komisję w oparciu o ich niezależność, prawość oraz doświadczenie w zakresie amerykańskich przepisów dotyczących ochrony prywatności i unijnego prawa o ochronie danych. W odniesieniu do każdego sporu dotyczącego osoby fizycznej strony wybierają z tej grupy panel złożony z jednego arbitra lub trzech ([140]) arbitrów.

(83) Międzynarodowe Centrum Rozstrzygania Sporów (ICDR), międzynarodowy oddział Amerykańskiego Stowarzyszenia Arbitrażowego (AAA), zostało wybrane przez DoC do zarządzania postępowaniami arbitrażowymi. Postępowania przed panelem DPF UE–USA będą regulowane uzgodnionym regulaminem arbitrażowym oraz kodeksem postępowania obowiązującym wyznaczonych arbitrów. Strona internetowa ICDR-AAA zawiera jasne i zwięzłe informacje dla osób fizycznych na temat mechanizmu arbitrażowego i procedury występowania o arbitraż.

(84) Regulamin arbitrażowy uzgodniony między DoC i Komisją uzupełnia DPF UE–USA, w którym przewidziano szereg elementów przyczyniających się do zwiększenia dostępności tego mechanizmu dla osób z Unii, których dane dotyczą: (i) przygotowując skargę do rozpoznania przez panel, osoba, której dane dotyczą, może korzystać ze wsparcia swojego krajowego organu ochrony danych; (ii) chociaż miejscem prowadzenia postępowania arbitrażowego będą Stany Zjednoczone, osoba z Unii, której dane dotyczą, może zdecydować się na udział w nim za pośrednictwem wideokonferencji lub konferencji telefonicznej, która zostanie zorganizowana nieodpłatnie; (iii) choć zasadniczo postępowanie arbitrażowe będzie prowadzone w języku angielskim, po otrzymaniu uzasadnionego wniosku tłumaczenie ustne podczas postępowania arbitrażowego oraz tłumaczenie pisemne zostanie co do zasady zapewnione nieodpłatnie; (iv) chociaż każda ze stron musi ponieść własne koszty zastępstwa procesowego, jeżeli jest reprezentowana przed panelem przez pełnomocnika, DoC będzie prowadzić fundusz zasilany rocznymi składkami wpłacanymi przez podmioty objęte DPF UE–USA, które mają pokryć koszty procedury arbitrażowej, do kwot maksymalnych, które zostaną ustalone przez organy amerykańskie w porozumieniu z Komisją ([141]).

(85) Panel ds. DPF UE–USA jest uprawniony do przyznania niepieniężnego godziwego zadośćuczynienia danej osobie fizycznej ([142]), które jest niezbędne do usunięcia niezgodności z zasadami. Chociaż panel, podejmując decyzję, uwzględnia inne środki ochrony prawnej uzyskane już w ramach innych mechanizmów DPF UE–USA, osoby fizyczne mogą nadal wnieść o arbitraż, jeżeli uznają te inne środki ochrony prawnej za niewystarczające. Pozwala to osobom z Unii, których dane dotyczą, wszczęcie arbitrażu we wszystkich przypadkach, gdy działanie lub bezczynność właściwych podmiotów objętych DPF UE–USA, niezależnych mechanizmów ochrony prawnej lub właściwych organów amerykańskich (np. FTC) nie doprowadziły do zadowalającego rozstrzygnięcia ich skarg. Z arbitrażu nie można skorzystać w przypadku, gdy organ ochrony danych jest uprawniony z mocy prawa do rozstrzygnięcia konkretnego roszczenia dotyczącego podmiotu objętego DPF UE–USA, tj. w tych przypadkach, w których podmiot albo jest zobowiązany do współpracy i zastosowania się do porad organów ochrony danych dotyczących przetwarzania danych o zasobach ludzkich zgromadzonych w ramach stosunku pracy, albo dobrowolnie się do tego zobowiązał. Osoby fizyczne mogą dochodzić wykonania orzeczenia arbitrażowego przed sądami amerykańskimi zgodnie z federalną ustawą o arbitrażu, co zapewnia środek ochrony prawnej w sytuacji, gdy podmiot nie wywiąże się ze spoczywających na nim zobowiązań.

([138]) Zob. załącznik I do załącznika I „Model arbitrażowy".
([139]) Zob. załącznik I sekcja II pkt 1 lit. a) ppkt (xi) oraz sekcja II pkt 7 lit. c).
([140]) Liczba arbitrów w danym panelu zostanie uzgodniona między stronami.
([141]) Załącznik I do załącznika I, sekcja G pkt 6.
([142]) Osoby fizyczne nie mogą dochodzić odszkodowania w postępowaniu arbitrażowym, ale wszczęcie postępowania arbitrażowego nie uniemożliwia dochodzenia odszkodowania przed amerykańskimi sądami powszechnymi.

(86) Po siódme, jeżeli podmiot nie wywiąże się ze swojego zobowiązania do przestrzegania zasad i opublikowanej polityki ochrony prywatności, wówczas mogą być dostępne inne sądowe środki odwoławcze na mocy prawa amerykańskiego, takie jak możliwość uzyskania odszkodowania. Osoby fizyczne mogą na przykład pod pewnymi warunkami skorzystać z sądowych środków odwoławczych (takich jak odszkodowanie) na mocy stanowego prawa ochrony konsumentów w przypadkach podania fałszywych informacji w celu wprowadzenia w błąd, podejmowania nieuczciwych lub oszukańczych działań lub stosowania nieuczciwych lub oszukańczych praktyk ([143]) oraz na mocy prawa deliktów (w szczególności w przypadku czynów niedozwolonych polegających na naruszeniu miru domowego ([144]), przywłaszczeniu nazwiska lub wizerunku ([145]) oraz publicznym ujawnieniu informacji o charakterze prywatnym ([146])).

(87) Wszystkie opisane powyżej sposoby dochodzenia roszczeń gwarantują, że każda skarga dotycząca niezgodności z DPF UE-USA przez certyfikowane podmioty zostanie skutecznie rozstrzygnięta i naprawiona.

3. DOSTĘP ORGANÓW PUBLICZNYCH W STANACH ZJEDNOCZONYCH DO DANYCH OSOBOWYCH PRZEKAZYWANYCH Z UNII EUROPEJSKIEJ I KORZYSTANIE Z TYCH DANYCH PRZEZ TE ORGANY

(88) Komisja oceniła również ograniczenia i zabezpieczenia, w tym mechanizmy nadzoru i indywidualne mechanizmy dochodzenia roszczeń dostępnych w prawie Stanów Zjednoczonych, jeśli chodzi o zbieranie i późniejsze wykorzystanie przez amerykańskie organy publiczne danych osobowych przekazywanych w interesie publicznym administratorom i podmiotom przetwarzającym w Stanach Zjednoczonych, szczególnie do celów ścigania przestępstw i bezpieczeństwa narodowego (dostęp rządowy) ([147]). Oceniając, czy warunki dostępu rządu do danych przekazywanych do Stanów Zjednoczonych na podstawie niniejszej decyzji spełniają kryterium „zasadniczej równoważności" przewidziane w art. 45 ust. 1 rozporządzenia (UE) 2016/679, zgodnie z wykładnią Trybunału Sprawiedliwości w świetle Karty praw podstawowych, Komisja uwzględniła szereg kryteriów.

(89) W szczególności wszelkie ograniczenia prawa do ochrony danych osobowych muszą być przewidziane przepisami prawa, a podstawa prawna, która pozwala na ingerencję w takie prawo, musi sama określać zakres ograniczenia w wykonywaniu danego prawa ([148]). Ponadto, aby spełnić wymóg proporcjonalności, zgodnie z którym odstępstwa od ochrony danych osobowych i ograniczenia tej ochrony powinny mieć zastosowanie tylko w takim zakresie, w jakim jest to absolutnie niezbędne w społeczeństwie demokratycznym do osiągnięcia szczególnych celów interesu ogólnego, równoważnych z celami uznanymi przez Unię, taka podstawa prawna musi określać jasne i precyzyjne zasady regulujące zakres i stosowanie środków oraz przewidywać wymagane zabezpieczenia, aby osoby, których dane zostały przekazane, miały wystarczające gwarancje skutecznej ochrony swoich danych osobowych przed ryzykiem nadużyć ([149]). Ponadto takie zasady i zabezpieczenia muszą mieć charakter prawnie wiążący i być możliwe do

([143]) Zob. np. stanowe przepisy dotyczące ochrony konsumentów w Kalifornii (kodeks cywilny Kalifornii, §§ 1750–1785 (Zachód) – ustawa o środkach ochrony prawnej konsumentów); dystrykt Kolumbii (kodeks dystryktu Kolumbii, §§ 28–3901); Floryda (statuty Florydy, §§ 501.201–501.213 – ustawa o wprowadzających w błąd i nieuczciwych praktykach handlowych); Illinois (statut stanu Illinois nr 815, §§ 505/1–505/12 – ustawa o oszustwach konsumenckich i wprowadzających w błąd praktykach biznesowych); Pensylwania (statut Pensylwanii nr 73, §§ 201-1–201-9.3 (Zachód) – ustawa o nieuczciwych praktykach handlowych i ochronie konsumentów).

([144]) Tj. w przypadku celowej ingerencji w prywatne sprawy osoby fizycznej lub dotyczące jej kwestie w sposób, który byłby wysoce obraźliwy dla racjonalnej osoby ((drugi) zbiór prawa, czyny niedozwolone, § 652 lit. b)).

([145]) Ten czyn niedozwolony ma zwykle zastosowanie w przypadku przywłaszczenia i wykorzystania nazwiska lub wizerunku osoby fizycznej w celu reklamowania przedsiębiorstwa lub produktu lub w podobnym celu komercyjnym (zob. (drugi) zbiór prawa, czyny niedozwolone, § 652 pkt C).

([146]) Tj. w przypadku, gdy upubliczniane są informacje dotyczące życia prywatnego danej osoby będące informacjami wysoce obraźliwymi dla racjonalnej osoby, przy czym informacje te nie są przedmiotem uzasadnionego zainteresowania ogółu ((drugi) zbiór prawa, czyny niedozwolone, § 652 pkt D).

([147]) Jest to również istotne w świetle sekcji I pkt 5 załącznika I. Zgodnie z tą sekcją i podobnie jak w przypadku RODO zgodność z wymogami i prawami w zakresie ochrony danych, które stanowią część zasad ochrony prywatności, może podlegać ograniczeniom. Ograniczenia takie nie mają jednak charakteru bezwzględnego, ale można się na nie powoływać jedynie pod kilkoma warunkami, na przykład w zakresie niezbędnym do wykonania nakazu sądowego lub spełnienia wymogów interesu publicznego, egzekwowania prawa lub bezpieczeństwa narodowego. W tym kontekście i w celu zapewnienia jasności sekcja odnosi się również do warunków określonych w rozporządzeniu wykonawczym 14086, które oceniono m.in. w motywach 127–141.

([148]) Zob. Schrems II, pkt 174–175 oraz przytaczane orzecznictwo. W odniesieniu do dostępu organów publicznych państw członkowskich zob. również sprawa C-623/17 Privacy International, ECLI:EU:C:2020:790, pkt 65 oraz sprawy połączone C-511/18, C-512/18 i C-520/18 La Quadrature du Net i in., ECLI:EU:C:2020:791, pkt 175.

([149]) Zob. Schrems II, pkt 176 i 181, jak również przytaczane orzecznictwo. W odniesieniu do dostępu organów publicznych państw członkowskich zob. również Privacy International, pkt 68; oraz La Quadrature du Net i in., pkt 132.

wyegzekwowania przez osoby fizyczne ([150]). W szczególności osoby, których dane dotyczą, muszą mieć możliwość wytoczenia powództwa przed niezależnym i bezstronnym sądem, aby uzyskać dostęp do swoich danych osobowych lub uzyskać sprostowanie lub usunięcie takich danych ([151]).

3.1. **Dostęp amerykańskich organów publicznych do danych na potrzeby ścigania przestępstw i wykorzystanie tych danych przez te organy w tym samym celu**

(90) W odniesieniu do ingerencji w dane osobowe przekazywane na podstawie DPF UE–USA do celów ścigania przestępstw w prawie Stanów Zjednoczonych nakłada się szereg ograniczeń w zakresie dostępu do danych osobowych i ich wykorzystywania, a także zapewnia się mechanizmy nadzoru i dochodzenia roszczeń zgodne z wymogami, o których mowa w motywie 89 niniejszej decyzji. Warunki uzyskania takiego dostępu oraz zabezpieczenia mające zastosowanie do wykonywania tych uprawnień poddano szczegółowej ocenie w kolejnych sekcjach. W tym względzie rząd USA (za pośrednictwem Departamentu Sprawiedliwości – DoJ) również złożył zapewnienia dotyczące obowiązujących ograniczeń i zabezpieczeń (załącznik VI do niniejszej decyzji).

3.1.1. ***Podstawy prawne, ograniczenia i zabezpieczenia***

3.1.1.1. *Ograniczenia i zabezpieczenia odnoszące się do gromadzenia danych osobowych do celów związanych ze ściganiem przestępstw*

(91) Dane osobowe przetwarzane przez certyfikowane podmioty amerykańskie, które byłyby przekazywane z Unii na podstawie DPF UE–USA, mogą być wykorzystywane do celów ścigania przestępstw przez amerykańskich prokuratorów federalnych i federalnych agentów śledczych w ramach różnych procedur, jak wyjaśniono bardziej szczegółowo w motywach 92–99. Procedury te mają zastosowanie w ten sam sposób, gdy informacje uzyskiwane są od dowolnego podmiotu amerykańskiego, niezależnie od narodowości lub miejsca zamieszkania osoby, której dane dotyczą ([152]).

(92) Po pierwsze, na wniosek federalnego funkcjonariusza organów ścigania lub pełnomocnika rządu, sędzia może wydać nakaz przeszukania lub zajęcia (w tym informacji przechowywanych w formie elektronicznej) ([153]). Nakaz taki może zostać wydany tylko wtedy, gdy istnieje „uzasadnione podejrzenie" ([154]), że „przedmioty podlegające zajęciu" (dowody przestępstwa, nielegalnie posiadane przedmioty lub składniki majątku zaprojektowane lub przeznaczone do wykorzystania lub wykorzystane do popełnienia przestępstwa) prawdopodobnie znajdują się w miejscu wskazanym w nakazie. W nakazie należy określić składnik majątku lub przedmiot, który ma zostać zajęty, oraz wskazać sędziego, któremu nakaz musi zostać przekazany. Osoba, której dotyczy przeszukanie lub której składnik majątku jest przedmiotem przeszukania, może wystąpić o wyłączenie z postępowania dowodów uzyskanych

([150]) Zob. Schrems II, pkt 181–182.

([151]) Zob. Schrems I, pkt 95 oraz Schrems II, pkt 194. W tym zakresie Trybunał Sprawiedliwości Unii Europejskiej podkreślił w szczególności, że zgodność z art. 47 Karty praw podstawowych, gwarantującej prawo do skutecznego środka odwoławczego przed niezależnym i bezstronnym sądem, „przyczynia się do wypracowania wymaganego w Unii stopnia ochrony, [a jego] poszanowanie Komisja musi stwierdzić, zanim wyda na podstawie art. 45 ust. 1 [rozporządzenia (UE) 2016/679] decyzję stwierdzającą odpowiedni stopień ochrony" (Schrems II, pkt 186).

([152]) Zob. załącznik VI. Zob. na przykład, w odniesieniu do ustawy o podsłuchach, ustawy o przechowywanych danych przekazywanych za pomocą łączności elektronicznej i ustawy o urządzeniach rejestrujących wybierane numery (wspomnianych bardziej szczegółowo w motywach 95–98), Suzlon Energy Ltd/Microsoft Corp., 671 F.3d 726, 729 (9th Cir. 2011).

([153]) Federalny kodeks postępowania karnego, zasada 41. W wyroku z 2018 r. Sąd Najwyższy USA potwierdził, że nakaz przeszukania lub wyjątek od nakazu są również wymagane, w przypadku gdy organy egzekwowania prawa chcą uzyskać dostęp do historycznych rejestrów danych dotyczących lokalizacji telefonów komórkowych, które zapewniają kompleksowy przegląd informacji o przemieszczaniu się użytkownika, a także że użytkownik może mieć uzasadnione oczekiwania co do ochrony prywatności w odniesieniu do takich informacji (Timothy Ivory Carpenter/Stany Zjednoczone Ameryki, sprawa nr 16–402, 585 U.S. (2018)). W rezultacie takie dane co do zasady nie mogą być pozyskiwane od operatora komórkowego na podstawie nakazu sądowego wydanego w oparciu o uzasadnione przesłanki pozwalające sądzić, że informacje są istotne i znaczące dla toczącego się dochodzenia, ale w przypadku skorzystania z nakazu wymagane jest wykazanie istnienia uzasadnionego podejrzenia.

([154]) Według Sądu Najwyższego „uzasadnione podejrzenie" jest „praktycznym, nietechnicznym" standardem odwołującym się do „faktycznych i praktycznych względów życia codziennego, na których opierają się rozsądni i rozważni ludzie [...]" (Illinois/Gates, 462 U.S. 213, 232 (1983)). W odniesieniu do nakazów przeszukania uzasadnione podejrzenie istnieje, gdy pojawia się znaczne prawdopodobieństwo, że przeszukanie doprowadzi do wykrycia dowodów przestępstwa (id).

w wyniku bezprawnego przeszukania lub pochodzących z takiego przeszukania, jeżeli dowody te zostały przedstawione przeciwko tej osobie w postępowaniu karnym ([155]). W przypadku gdy posiadacz danych (np. przedsiębiorstwo) jest zobowiązany do ujawnienia danych na mocy nakazu, może w szczególności zakwestionować wymóg ujawnienia jako nadmiernie obciążający ([156]).

(93) Po drugie, wezwanie może zostać wydane przez wielką ławę przysięgłych (sądowe ciało dochodzeniowe wyznaczone przez sędziego) w kontekście dochodzeń w sprawie niektórych poważnych przestępstw ([157]), co do zasady na wniosek prokuratora federalnego, w celu zażądania od danej osoby przedstawienia lub udostępnienia rejestrów związanych z prowadzoną działalnością, informacji przechowywanych w formie elektronicznej lub dostarczenia innych przedmiotów materialnych. Ponadto różnego rodzaju ustawy dopuszczają możliwość stosowania wezwań administracyjnych w celu pozyskania rejestrów dotyczących prowadzonej działalności, informacji przechowywanych w formie elektronicznej lub innych przedmiotów materialnych lub uzyskania dostępu do takich rejestrów, informacji lub przedmiotów w ramach postępowań w przedmiocie nadużyć w obszarze opieki zdrowotnej, znęcania się nad dziećmi, ochrony tajnych służb, spraw dotyczących substancji kontrolowanych i prowadzonych przez Inspektora Generalnego dochodzeń ([158]). W obu przypadkach informacje muszą mieć istotne znaczenie dla prowadzonego dochodzenia, a wezwanie nie może być nieuzasadnione, tj. jego zakres nie może być zbyt szeroki ani nie może mieć zbyt uciążliwego lub obciążającego charakteru (i wezwanie takie może zostać zakwestionowane przez odbiorcę z tych powodów) ([159]).

(94) Bardzo podobne warunki mają zastosowanie do wezwań administracyjnych wydanych w celu uzyskania dostępu do danych będących w posiadaniu przedsiębiorstw w Stanach Zjednoczonych w sprawach cywilnych lub regulacyjnych („interes publiczny"). Uprawnienia agencji o kompetencjach cywilnych i regulacyjnych do wydawania takich wezwań administracyjnych muszą zostać ustanowione w statucie. Zastosowanie wezwania administracyjnego podlega „testowi zasadności", który wymaga, aby dochodzenie było prowadzone w uzasadnionym celu, informacje, o które wystąpiono na podstawie wezwania, były istotne dla tego celu, agencja nie posiadała już informacji, których żąda za pomocą wezwania, i dopełniono niezbędnych kroków administracyjnych w celu wydania wezwania ([160]). W orzecznictwie Sądu Najwyższego wyjaśniono również potrzebę wyważenia znaczenia żądanych informacji dla interesu publicznego oraz znaczenia osobistej i organizacyjnej ochrony prywatności ([161]). Chociaż zastosowanie wezwania administracyjnego nie podlega uprzedniej zgodzie organu sądowego, podlega ono kontroli sądowej w przypadku zakwestionowania przez podmiot z wyżej wymienionych powodów lub w przypadku, gdy agencja wydająca nakaz dąży do wystąpienia do sądu o zobowiązanie danego podmiotu do zastosowania się do treści wezwania administracyjnego ([162]). Oprócz tych ogólnych nadrzędnych ograniczeń, z poszczególnych ustaw mogą wynikać szczególne (surowsze) wymogi ([163]).

([155]) Mapp/Ohio, 367 U.S. 643 (1961).

([156]) Zob. In re Application of United States, 610 F.2d 1148, 1157 (3d Cir. 1979) (w sprawie tej sąd orzekł, że „aby zapewnić rzetelność procesu, należy przeprowadzić przesłuchanie w kwestii uciążliwości przed zobowiązaniem przedsiębiorstwa telekomunikacyjnego do udzielenia" pomocy w odniesieniu do nakazu przeszukania) oraz In re Application of United States, 616 F.2d 1122 (9th Cir. 1980).

([157]) W piątej poprawce do Konstytucji Stanów Zjednoczonych wymaga się od wielkiej ławy przysięgłych przyjęcia aktu oskarżenia za wszelką „zbrodnię główną lub inne hańbiące przestępstwo". Ława przysięgłych składa się z 16 do 23 członków i ustala, czy istnieje uzasadnione podejrzenie, że popełniono przestępstwo. Aby to ustalić, wielkim ławom przysięgłych przyznano uprawnienia śledcze, w ramach których mogą wydawać wezwania sądowe.

([158]) Zob. załącznik VI.

([159]) Federalny kodeks postępowania karnego, zasada 17.

([160]) United States/Powell, 379 U.S. 48 (1964).

([161]) Oklahoma Press Publishing Co./Walling, 327 U.S. 186 (1946).

([162]) Sąd Najwyższy wyjaśnił, że w przypadku zakwestionowania wezwania administracyjnego sąd musi rozważyć, czy 1) dochodzenie ma należycie uzasadniony cel, 2) w zakresie uprawnień Kongresu jest kierowanie organem wystawiającym wezwanie i czy 3) „żądane dokumenty mają znaczenie dla dochodzenia". Sąd zauważył również, że wniosek o wezwanie administracyjne musi być „rozsądny", tj. wymagający „adekwatnej lecz nie nadmiernej specyfikacji dokumentów, które należy przedstawić, do celów odpowiedniego dochodzenia", w tym „szczegółowości w « opisywaniu miejsca, które ma zostać przeszukane i osób lub przedmiotów, które mają zostać zatrzymane lub zajęte »".

([163]) Na przykład ustawa o prawie do prywatności w kwestiach finansowych przyznaje organowi rządowemu uprawnienia do uzyskiwania dokumentacji finansowej prowadzonej przez instytucję finansową na podstawie wezwania administracyjnego tylko wtedy, gdy 1) istnieją powody, by sądzić, że poszukiwana dokumentacja ma znaczenie dla zgodnego z prawem dochodzenia prowadzonego przez organy ścigania oraz 2) kopia wezwania lub wezwania do stawienia się przed sądem została dostarczona klientowi wraz z zawiadomieniem określającym w rozsądny sposób charakter dochodzenia (tytuł 12 § 3405 U.S.C.). Innym przykładem jest ustawa o rzetelnej sprawozdawczości kredytowej, która zakazuje agencjom zgłaszającym konsumentów ujawniania sprawozdań konsumentów w odpowiedzi na wezwania administracyjne (i zezwala im jedynie na udzielanie odpowiedzi na wnioski wielkiej ławy przysięgłych lub nakazy sądowe, tytuł 15 §1681 i nast. U.S.C.). Jeżeli chodzi o dostęp do informacji komunikacyjnych, zastosowanie mają szczególne wymogi ustawy o przechowywanych danych przekazywanych za pomocą łączności elektronicznej, w tym w odniesieniu do możliwości stosowania wezwań administracyjnych (szczegółowy przegląd znajduje się w motywach 96–97).

(95) Po trzecie, niektóre podstawy prawne umożliwiają organom egzekwowania prawa w sprawach karnych uzyskanie dostępu do danych komunikacyjnych. Sąd może wydać nakaz sądowy upoważniający do gromadzenia zarejestrowanych w czasie rzeczywistym informacji billingowych, informacji o trasowaniu, informacji adresowych i informacji przekazywanych w ramach sygnalizacji telekomunikacyjnej dotyczących danego numeru telefonu lub adresu e-mail (za pomocą urządzenia rejestrującego wybierane numery lub urządzenia śledzącego), jeśli stwierdzi, że organ poświadczył, że informacje, które mogą zostać pozyskane, mają istotne znaczenie dla toczącego się dochodzenia ([164]). Nakaz musi zawierać, między innymi, określenie tożsamości podejrzanego, jeśli jest znana, cechy komunikacji, której nakaz dotyczy, oraz oświadczenie dotyczące przestępstwa, do którego odnoszą się gromadzone informacje. Korzystanie z urządzenia rejestrującego wybierane numery lub urządzenia śledzącego może być dozwolone na maksymalny okres sześćdziesięciu dni, który to okres może zostać przedłużony wyłącznie na podstawie nowego nakazu sądowego.

(96) Ponadto uzyskanie dostępu do informacji na temat abonentów, danych o ruchu oraz treści komunikatów przechowywanych przez dostawców usług internetowych, przedsiębiorstwa telekomunikacyjne oraz innych dostawców usług internetowych będących stronami trzecimi do celów związanych ze ściganiem przestępstw możliwe jest na podstawie ustawy o przechowywanych danych przekazywanych za pomocą łączności elektronicznej ([165]). Aby uzyskać dostęp do treści komunikatów przekazywanych za pomocą łączności elektronicznej, organy egzekwowania prawa w sprawach karnych muszą co do zasady uzyskać nakaz wydany przez sędziego na podstawie uzasadnionego podejrzenia, że dane konto użytkownika zawiera dowody popełnienia przestępstwa ([166]). Aby uzyskać dostęp do danych zgromadzonych przy rejestracji abonentów, ich adresów IP, powiązanych z tymi adresami znaczników czasu oraz informacji billingowych, organy egzekwowania prawa w sprawach karnych mogą skorzystać z nakazu. Aby uzyskać dostęp do większości innych przechowywanych informacji niedotyczących treści, takich jak nagłówki wiadomości e-mail bez tematu, organ egzekwowania prawa w sprawach karnych musi uzyskać nakaz sądowy, który zostanie wydany, jeśli sędzia uzna, że istnieją konkretne uzasadnione przesłanki świadczące o tym, że żądane informacje mają istotne i zasadnicze znaczenie dla toczącego się dochodzenia.

(97) Dostawcy, którzy otrzymują wnioski na podstawie ustawy o przechowywanych danych przekazywanych za pomocą łączności elektronicznej, mogą według własnego uznania powiadomić klienta lub abonenta, których dane mają zostać pozyskane, z wyjątkiem sytuacji, gdy odpowiedni organ egzekwowania prawa w sprawach karnych uzyska nakaz ochronny zakazujący dokonania takiego powiadomienia ([167]). Taki nakaz ochronny jest nakazem sądowym, na mocy którego od dostawcy usług łączności elektronicznej lub dostawcy zdalnych usług komputerowych, do którego skierowane są nakaz, wezwanie sądowe lub nakaz sądowy, wymaga się, aby nie powiadamiał żadnej innej osoby o istnieniu nakazu, wezwania sądowego lub nakazu sądowego tak długo, jak sąd uzna za stosowne. Nakazy ochronne wydaje się wówczas, gdy sąd uzna, że istnieją powody, by przypuszczać, że powiadomienie poważnie zagroziłoby dochodzeniu lub nadmiernie opóźniłoby proces, np. ze względu na spowodowanie zagrożenia życia lub bezpieczeństwa fizycznego osoby, ucieczkę przed oskarżeniem, zastraszenie potencjalnych świadków itp. Na mocy memorandum zastępcy prokuratora generalnego (które ma charakter wiążący dla wszystkich prawników i przedstawicieli DoJ) wymagane jest, aby prokuratorzy dokonali szczegółowej oceny potrzeby wydania nakazu ochronnego i uzasadnili sądowi, w jaki sposób w danej sprawie spełnione zostały ustawowe kryteria uzyskania nakazu ochronnego ([168]). Na mocy memorandum wymaga się również, aby wnioski o wydanie nakazów ochronnych zasadniczo nie miały na celu opóźnienia powiadomienia o więcej niż jeden rok. W przypadkach gdy w wyjątkowych okolicznościach konieczne mogą być nakazy o dłuższym okresie obowiązywania, o takie nakazy można ubiegać się wyłącznie za pisemną zgodą przełożonego wyznaczonego przez prokuratora Stanów Zjednoczonych lub odpowiedniego asystenta prokuratora generalnego. Ponadto zamykając dochodzenie, prokurator musi niezwłocznie ocenić, czy istnieją podstawy do utrzymania w mocy wszelkich niewykonanych nakazów ochronnych, a jeśli tak nie jest, zobowiązany jest uchylić nakaz ochronny i upewnić się, że dostawca usług został o tym fakcie powiadomiony ([169]).

([164]) Tytuł 18 § 3123 U.S.C.

([165]) Tytuł 18 §§ 2701–2713 U.S.C.

([166]) Tytuł 18 §§ 2701 lit. a) i b) pkt 1 ppkt A U.S.C. Jeśli odnośny abonent lub klient zostanie powiadomiony (z wyprzedzeniem albo, w pewnych okolicznościach, w drodze opóźnionego powiadomienia), informacje dotyczące treści przechowywane dłużej niż 180 dni można również uzyskać na podstawie wezwania administracyjnego lub wezwania wydanego przez wielką ławę przysięgłych (tytuł 18 § 2701 lit. b) pkt 1 ppkt B U.S.C.) lub nakazu sądowego (jeśli istnieją uzasadnione przesłanki, by przypuszczać, że informacje te mają istotne i zasadnicze znaczenie dla toczącego się dochodzenia (tytuł 18 §§ 2701 lit. d) U.S.C.). Zgodnie z orzeczeniem federalnego sądu apelacyjnego śledczy rządowi zazwyczaj uzyskują jednak nakazy przeszukania od sędziów w celu zgromadzenia treści prywatnej komunikacji lub przechowywanych danych od komercyjnego dostawcy usług komunikacyjnych. Stany Zjednoczone/Warshak, 631 F.3d 266 (6th Cir. 2010).

([167]) Tytuł 18 § 2705 lit. b) U.S.C.

([168]) Zob. memorandum zastępcy prokuratora generalnego Roda Rosensteina z dnia 19 października 2017 r. w sprawie bardziej restrykcyjnej polityki dotyczącej wniosków o wydanie nakazu ochronnego (lub nakazu nieujawniania), dostępne pod adresem: https://www.justice.gov/criminal-ccips/page/file/1005791/download

([169]) Memorandum zastępcy prokuratora generalnego Lisy Moncao z dnia 27 maja 2022 r. w sprawie dodatkowej polityki dotyczącej wniosków o wydanie nakazów ochronnych zgodnie z tytułem 18 § 2705 lit. b) U.S.C.

(98) Organy egzekwowania prawa w sprawach karnych mogą również przechwytywać w czasie rzeczywistym komunikaty przekazywane za pomocą łączności kablowej, ustnie lub za pomocą łączności elektronicznej na podstawie nakazu sądowego, w którym sędzia stwierdzi m.in., że istnieje uzasadnione podejrzenie, iż informacje uzyskane dzięki zainstalowaniu podsłuchu lub zastosowaniu środków przechwytywania komunikatów przekazywanych drogą elektroniczną pozwolą uzyskać dowody popełnienia przestępstwa federalnego lub ustalić miejsce pobytu osoby ukrywającej się przed wymiarem sprawiedliwości ([170]).

(99) Dalszą ochronę gwarantują różnego rodzaju polityki i wytyczne Departamentu Sprawiedliwości, takie jak wytyczne prokuratora generalnego w sprawie krajowych operacji Federalnego Biura Śledczego (FBI) (AGG-DOM), na mocy których, między innymi, wymagane jest, aby FBI stosowało jak najmniej inwazyjne metody dochodzeniowe, biorąc pod uwagę ich wpływ na prywatność i wolności obywatelskie ([171]).

(100) Zgodnie z oświadczeniami przedstawionymi przez rząd USA te same lub większe zabezpieczenia opisane powyżej mają zastosowanie do dochodzeń w sprawach egzekwowania prawa na szczeblu stanowym (w odniesieniu do dochodzeń prowadzonych na podstawie przepisów prawa stanowego) ([172]). W szczególności przepisy konstytucyjne, a także ustawy i orzecznictwo na szczeblu państwowym potwierdzają wspomniane powyżej środki ochrony przed nieuzasadnionymi przeszukaniami i zajęciami, wymagając wydania nakazu przeszukania ([173]). Podobnie jak w przypadku ochrony przyznanej na szczeblu federalnym, nakazy przeszukania mogą być wydawane wyłącznie po wykazaniu prawdopodobnej przyczyny i muszą określać miejsce, które ma zostać przeszukane, oraz osobę lub przedmiot, które mają zostać zatrzymane lub zajęte ([174]).

([170]) Tytuł 18 §§ 2510–2522 U.S.C.

([171]) Wytyczne prokuratora generalnego w sprawie krajowych operacji Federalnego Biura Śledczego (FBI) (wrzesień 2008) dostępne pod adresem http://www.justice.gov/archive/opa/docs/guidelines.pdf Dodatkowe zasady i strategie ograniczające działalność śledczą prokuratorów federalnych zostały ustanowione w podręczniku dla prokuratorów Stanów Zjednoczonych, który jest również dostępny pod adresem http://www.justice.gov/usam/united-states-attorneys-manual W celu odstąpienia od przestrzegania tych wytycznych, należy uzyskać uprzednią zgodę dyrektora FBI, zastępcy dyrektora FBI lub zastępcy dyrektora wykonawczego wyznaczonego przez dyrektora FBI, chyba że nie ma możliwości uzyskania takiej zgody ze względu na bezpośredniość lub powagę zagrożenia dla bezpieczeństwa osób lub składników majątku lub bezpieczeństwa narodowego (w takim przypadku należy powiadomić dyrektora FBI lub inną osobę upoważnioną do wydania takiej zgody tak szybko, jak to możliwe). W przypadku nieprzestrzegania wytycznych FBI zobowiązane jest powiadomić o tym fakcie DoJ, który z kolei informuje prokuratora generalnego i zastępcę prokuratora generalnego.

([172]) Załącznik VI przypis 2. Zob. również np. Arnold/City of Cleveland, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) („W dziedzinie praw indywidualnych i wolności obywatelskich konstytucja Stanów Zjednoczonych, tam gdzie ma ona zastosowanie do stanów, zapewnia dolny pułap, poniżej którego orzeczenia sądów stanowych nie mogą zapadać"); Cooper/California, 386 U.S. 58, 62, 87 S. Ct. 788, 17 L.Ed.2d 730 (1967 r.) („Nasz holding oczywiście nie wpływa na uprawnienie stanu do narzucania wyższych standardów przeszukiwań i konfiskat, niż wymaga tego konstytucja federalna, jeżeli państwo się na to zdecyduje."); Petersen/City of Mesa, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) („Mimo iż konstytucja Arizony może nakładać surowsze standardy przeszukiwań i konfiskat, niż wymaga tego konstytucja federalna, sądy Arizony nie mogą zapewnić niższej ochrony, niż gwarantuje czwarta poprawka.").

([173]) Większość stanów powieliła w swoich konstytucjach środki ochrony przewidziane w czwartej poprawce. Zob. konstytucja Alabamy art. I, § 5); konstytucja Alaski art. I, § 14; 1; konstytucja Arkansas art. II, § 15; konstytucja Kalifornii art. I, § 13; konstytucja Kolorado art. II, § 7; konstytucja Connecticut art. I, § 7; konstytucja Delaware art. I, § 6; konstytucja Florydy art. I, § 12; konstytucja Georgii art. I, § I ust. XIII; konstytucja Hawai art. I, § 7; konstytucja Idaho art. I, § 17; konstytucja Illinois art. I, § 6; konstytucja Indiany art. I, § 11; konstytucja Iowy art. I, § 8; konstytucja Kansas karta praw, § 15; konstytucja Kentucky § 10; konstytucja Luizjany art. I, § 5; konstytucja Maine art. I, § 5; konstytucja Massachusets deklaracja praw, art. 14; konstytucja Michigan art. I, § 11; konstytucja Minnesoty art. I, § 10; konstytucja Mississippi art. III, § 23; konstytucja Missouri art. I, § 15; konstytucja Montany art. II, § 11; konstytucja Nebraski art. I, § 7; konstytucja Nevady art. I, § 18; konstytucja New Hampshire pkt 1 art.. 19; konstytucja N.J. art. II, § 7; konstytucja Nowego Meksyku art. II, § 10; konstytucja Nowego Jorku art. I, § 12; konstytucja Północnej Dakoty art. I, § 8; konstytucja Ohio art. I, § 14; konstytucja Oklahomy art. II, § 30; konstytucja Oregonu art. I, § 9; konstytucja Pennsylvanii art. I, § 8; konstytucja Rhode Island art. I, § 6; konstytucja Południowej Karoliny art. I, § 10; konstytucja Południowej Dakoty art. VI, § 11; konstytucja Tennessee art. I, § 7; konstytucja Teksasu art. I, § 9; konstytucja Utah art. I, § 14; konstytucja Vermont rozdz. I, art. 11; konstytucja Zachodniej Virginii art. III, § 6; konstytucja Wisconsin art. I, § 11; konstytucja Wyoming art. I, § 4. Inne (np. Maryland, Karolina Północna i Wirginia) zapisały w swoich konstytucjach konkretny język dotyczący nakazów, który został zinterpretowany sądowo w celu zapewnienia podobnej lub wyższej ochrony co czwarta poprawka (zob. Maryland. deklaracja praw, art. 26; konstytucja Południowej Karoliny art. I, § 20; konstytucja Wirginii art. I, § 10, i odpowiednie orzecznictwo, np. Hamel/State, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; State/Johnson, 861 S.E.2d 474, 483 (N.C. 2021) i Lowe/Commonwealth, 337 S.E.2d 273, 274 (Va. 1985)). Ponadto Arizona i Waszyngton posiadają przepisy konstytucyjne, które ogólniej chronią prywatność (konstytucja Arizony. art. 2 § 8; konstytucja Waszyngtonu art. I, § 7, która została zinterpretowana przez sądy jako gwarantująca wyższą ochronę niż czwarta poprawka (zob. np. State/Bolt, 689 P.2d 519, 523 (Ariz. 1984), State/Ault, 759 P.2d 1320, 1324 (Ariz. 1988), State/Myrick, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984), State/Young, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

([174]) Zob. np. kalifornijski kodeks karny, § 1524,3 lit. b); zasada 3.6–3.13 Regulaminu postępowania karnego Alabamy; rozdział 10.79.035; zmieniony kodeks Waszyngtonu; rozdział 5 sekcja 19.2–59, tytuł 19.2 Postępowanie karne, kodeks Wirginii.

3.1.1.2. *Dalsze wykorzystywanie zebranych informacji*

(101) W odniesieniu do dalszego wykorzystywania danych zebranych przez federalne organy egzekwowania prawa w sprawach karnych, różnego rodzaju ustawy, wytyczne i normy przewidują określone zabezpieczenia. Z wyjątkiem konkretnych instrumentów mających zastosowanie do działalności FBI (AGG-DOM i poradnika FBI dotyczącego prowadzenia dochodzeń i operacji na szczeblu krajowym), wymogi opisane w niniejszej sekcji mają zasadniczo zastosowanie do dalszego wykorzystywania danych przez dowolny organ federalny, w tym do danych, do których uzyskano dostęp do celów cywilnych lub regulacyjnych. Obejmuje to wymogi wynikające z not/rozporządzeń Urzędu ds. Administracji i Budżetu, ustawy federalnej o modernizacji bezpieczeństwa informacji, ustawy o administracji elektronicznej oraz ustawy o rejestrach federalnych.

(102) Zgodnie z uprawnieniami nadanymi na mocy ustawy Clinger-Cohen (P.L. 104–106, dział E) i ustawy o bezpieczeństwie komputerowym z 1987 r. (P.L. 100–235) Urząd ds. Administracji i Budżetu (OMB) wydał okólnik nr A–130 w celu ustanowienia ogólnych wiążących wytycznych mających zastosowanie do wszystkich agencji federalnych (w tym do organów egzekwowania prawa), w przypadku gdy przetwarzają one dane identyfikujące osobę ([175]). Zgodnie z treścią tego okólnika wymagane jest w szczególności, aby wszystkie agencje federalne „ograniczyły tworzenie, gromadzenie, wykorzystywanie, przetwarzanie, przechowywanie, utrzymywanie, rozpowszechnianie i ujawnianie danych identyfikujących osobę do tych, które są prawnie dozwolone, istotne i z rozsądnego punktu widzenia uznane za niezbędne do prawidłowego wykonywania funkcji upoważnionej agencji" ([176]). Ponadto w zakresie, w jakim jest to wykonalne, agencje federalne muszą zapewnić, by dane identyfikujące osobę były prawidłowe, istotne, aktualne i kompletne oraz ograniczone do minimum niezbędnego do prawidłowego wykonywania funkcji agencji. Ogólniej rzecz ujmując, agencje federalne muszą ustanowić kompleksowy program ochrony prywatności w celu zapewnienia zgodności z obowiązującymi wymogami dotyczącymi ochrony prywatności, opracować i oceniać polityki prywatności oraz zarządzać ryzykiem związanym z ochroną prywatności, stosować procedury wykrywania, dokumentowania i zgłaszania incydentów związanych z przestrzeganiem zasad ochrony prywatności, opracowywać szkolenia i programy mające na celu zwiększenie świadomości na temat ochrony prywatności dla pracowników i wykonawców, oraz wdrożyć zasady i procedury na rzecz zapewnienia, by personel ponosił odpowiedzialność za przestrzeganie wymogów i zasad dotyczących ochrony prywatności ([177]).

(103) Ponadto zgodnie z ustawą o administracji elektronicznej ([178]) wszystkie agencje federalne (w tym organy egzekwowania prawa w sprawach karnych) są zobowiązane do wprowadzenia zabezpieczeń zapewniających bezpieczeństwo informacji, współmiernych do ryzyka i wielkości szkody, która wynikałaby z nieuprawnionego dostępu, wykorzystywania, ujawniania, zakłócenia, zmodyfikowania lub zniszczenia, oraz do wyznaczenia głównego urzędnika ds. informacji w celu zapewnienia spełnienia wymogów w zakresie bezpieczeństwa informacji oraz przeprowadzenia corocznej niezależnej oceny (np. przez Inspektora Generalnego, zob. motyw 109) ich programu i praktyk na rzecz bezpieczeństwa informacji ([179]). Podobnie zgodnie z ustawą o rejestrach federalnych (FRA) ([180]) i dodatkowymi regulacjami ([181]) informacje przechowywane przez agencje federalne muszą podlegać zabezpieczeniom zapewniającym fizyczną integralność danych oraz chroniącym dane przed nieuprawnionym dostępem.

(104) Zgodnie z ustawowym upoważnieniem federalnym, w tym z ustawą federalną o modernizacji bezpieczeństwa informacji z 2014 r., OMB oraz Narodowy Instytut Standaryzacji i Technologii (NIST) opracowały normy wiążące dla agencji federalnych (w tym dla organów egzekwowania prawa w sprawach karnych), w których szczegółowo określono minimalne wymogi w zakresie bezpieczeństwa informacji, które należy wdrożyć i które obejmują kontrole dostępu, zapewnienie podnoszenia świadomości i szkoleń, planowanie ewentualnościowe, reagowanie na incydenty, narzędzia w zakresie audytów i rozliczalności, zapewnienie integralności systemu i danych, przeprowadzanie ocen ryzyka związanego z prywatnością i bezpieczeństwem itp. ([182]) Ponadto zgodnie z wytycznymi OMB wszystkie

([175]) Tj. „informacje, które można wykorzystać do rozróżnienia lub wyśledzenia tożsamości osoby fizycznej, zarówno indywidualnie, jak i w połączeniu z innymi informacjami, które są powiązane lub możliwe do powiązania z konkretną osobą fizyczną", zob. okólnik OMB nr A-130, s. 33 (definicja „danych identyfikujących osobę").

([176]) Okólnik OMB nr A-130, „Managing Information as a Strategic Resource" („Zarządzanie informacjami jako zasobami strategicznymi", dodatek II, „Responsibilities for Managing Personally Identifiable Information" („Obowiązki w zakresie zarządzania danymi identyfikującymi osobę"), Rejestr Federalny (t. 81, s. 49689, 28 lipca 2016 r.), s. 17.

([177]) Dodatek II, § 5 lit. a)–h).

([178]) Tytuł 44 rozdział 36 U.S.C.

([179]) Tytuł 44 §§ 3544–3545 U.S.C.

([180]) FAC, tytuł 44 § 3105 U.S.C.

([181]) Tytuł 36 §§ 1228,150 i nast. oraz 1228,228 C.F.R. oraz dodatek A do C.F.R.

([182]) Zob. na przykład okólnik OMB nr A-130; NIST SP 800-53, Rev. 5, „Security and Privacy Controls for Information Systems and Organizations" („Kontrole bezpieczeństwa i prywatności w odniesieniu do systemów informacyjnych i organizacji" (10 grudnia 2020 r.), oraz opracowane przez NIST normy FIPS (federalne normy przetwarzania danych) 200: Minimum Security Requirements for Federal Information and Information Systems (minimalne wymagania bezpieczeństwa federalnych danych i systemów informacyjnych).

agencje federalne (w tym organy egzekwowania prawa w sprawach karnych) muszą utrzymywać i wdrożyć plan postępowania w razie naruszenia ochrony danych, w tym reagowania na takie naruszenia oraz oceny ryzyka wystąpienia szkód ([183]).

(105) Jeśli chodzi o przechowywanie danych, zgodnie z ustawą o rejestrach federalnych (FRA) ([184]) agencje federalne Stanów Zjednoczonych (w tym organy egzekwowania prawa w sprawach karnych) są zobowiązane do określenia okresów przechowywania swojej dokumentacji (po których upływie dokumentacja ta musi zostać usunięta), które to okresy muszą zostać zatwierdzone przez Krajową Administrację Archiwów i Rejestrów ([185]). Długość tych okresów przechowywania jest uzależniona od różnych czynników, takich jak rodzaj dochodzenia, to, czy dowody są nadal istotne dla danego dochodzenia, itp. Jeśli chodzi o FBI, zgodnie z AGG-DOM FBI musi mieć taki plan przechowywania dokumentacji oraz prowadzić system, za którego pomocą można szybko sprawdzić status i podstawę dochodzeń.

(106) Okólnik OMB nr A-130 również zawiera określone wymogi dotyczące rozpowszechniania danych identyfikujących osobę. Co do zasady rozpowszechnianie i ujawnianie danych identyfikujących osobę musi ograniczać się do tego, co jest prawnie dozwolone, istotne i racjonalnie uznane za niezbędne do właściwego wykonywania funkcji agencji ([186]). Podczas udostępniania danych identyfikujących osobę innym podmiotom rządowym amerykańskie agencje federalne muszą, w stosownych przypadkach, narzucić warunki (w tym warunek wdrożenia konkretnych kontroli bezpieczeństwa i prywatności) regulujące przetwarzanie takich danych na podstawie umów pisemnych (w tym kontraktów, umów w sprawie wykorzystywania danych, umów w sprawie wymiany danych i protokołów ustaleń) ([187]). Jeżeli chodzi o powody, dla których informacje mogą być rozpowszechniane, w wytycznych AGG-DOM i w poradniku FBI dotyczącym prowadzenia dochodzeń i operacji na szczeblu krajowym ([188]) przewidziano, że FBI może podlegać wymogowi prawnemu (np. na mocy umowy międzynarodowej) rozpowszechniania danych lub może udostępniać informacje w określonych okolicznościach, np. innym agencjom amerykańskim, jeżeli ujawnienie jest zgodne z celem, dla którego zebrano informacje, i są związane z obowiązkami tych agencji; komisjom kongresowym; agencjom zagranicznym, jeżeli dane są związane z ich obowiązkami, a ich rozpowszechnianie jest zgodne z interesami Stanów Zjednoczonych; ich rozpowszechnianie jest szczególnie niezbędne do zapewnienia bezpieczeństwa lub ochrony osób lub mienia lub do ochrony przed przestępstwem lub zagrożeniem bezpieczeństwa narodowego lub do zapobieżenia przestępstwu lub zagrożeniu bezpieczeństwa narodowego, a ujawnienie jest zgodne z celem, dla którego zebrano dane ([189]).

3.1.2. ***Nadzór***

(107) Działalność federalnych organów ścigania podlega nadzorowi ze strony różnych podmiotów ([190]). Jak wyjaśniono w motywach 92–99, w większości przypadków obejmuje to uprzedni nadzór ze strony wymiaru sprawiedliwości, który musi zezwolić na indywidualne środki zbierania danych przed ich zastosowaniem. Ponadto inne organy nadzorują różne etapy działalności organów egzekwowania prawa w sprawach karnych, w tym gromadzenie i przetwarzanie danych osobowych. Te organy sądowe i pozasądowe wspólnie zapewniają, aby organy egzekwowania prawa podlegały niezależnemu nadzorowi.

([183]) Memorandum 17–12, „Preparing for and Responding to a Breach of Personally Identifiable Information" („Przygotowanie na naruszenie ochrony danych identyfikujących osobę oraz reagowanie na takie naruszenie") dostępne pod adresem https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf i okólnik OMB nr A-130. Na przykład procedury Departamentu Sprawiedliwości w zakresie reagowania na naruszenia danych, *zob*. https://www.justice.gov/file/4336/download

([184]) FRA, tytuł 44 §§ 3101 i nast. U.S.C.

([185]) Krajowa Administracja Archiwów i Rejestrów (National Archives and Record Administration) jest uprawniona do oceny praktyk w zakresie zarządzania dokumentacją agencji i może określić, czy dalsze przechowywanie określonej dokumentacji jest uzasadnione (tytuł 44 § 2904 lit. c) i § 2906 U.S.C.).

([186]) Zob. okólnik OMB nr A-130, sekcja 5 lit. f) ust. 1 lit. d).

([187]) Zob. okólnik OMB nr A-130, dodatek I § 3 lit. d).

([188]) Zob. również poradnik FBI dotyczący prowadzenia dochodzeń i operacji na szczeblu krajowym (DIOG), sekcja 14.

([189]) AGG-DOM, sekcja VI, B i C; poradnik FBI dotyczący prowadzenia dochodzeń i operacji na szczeblu krajowym (DIOG), sekcja 14.

([190]) Mechanizmy, o których mowa w niniejszej sekcji, mają również zastosowanie do gromadzenia i wykorzystywania danych przez organy federalne do celów cywilnych i regulacyjnych. Federalne agencje cywilne i regulacyjne podlegają kontroli ze strony swoich odpowiednich Inspektorów Generalnych oraz nadzorowi ze strony Kongresu, w tym Rządowego Biura Odpowiedzialności, agencji audytu i agencji śledczej Kongresu. Obowiązki te spoczywają na urzędniku wyższego szczebla Agencji ds. Prywatności (SAOP), chyba że agencja wyznaczyła urzędnika ds. prywatności i wolności obywatelskich – stanowisko to zazwyczaj znajduje się w takich agencjach jak Departament Sprawiedliwości i Departament Bezpieczeństwa Wewnętrznego (DHS) ze względu na ich obowiązki w zakresie egzekwowania prawa i bezpieczeństwa narodowego. Wszystkie agencje federalne są prawnie zobowiązane do wyznaczenia SAOP, który ponosi odpowiedzialność za zapewnienie przestrzegania przez agencję przepisów o ochronie prywatności i nadzór nad powiązanymi kwestiami. Zob. np. OMB M-16-24, Role i wyznaczenie urzędników wyższego szczebla Agencji ds. Prywatności (2016).

(108) Po pierwsze, urzędnicy ds. prywatności i wolności obywatelskich pełnią obowiązki w różnych departamentach, którym powierzono obowiązki w zakresie ścigania przestępstw ([191]). Chociaż konkretne uprawnienia tych urzędników mogą się nieco różnić w zależności od ustawy stanowiącej podstawę prawną, zazwyczaj obejmują nadzór nad procedurami w celu zapewnienia, aby dany departament lub dana agencja odpowiednio uwzględniały kwestie dotyczące prywatności i wolności obywatelskich oraz aby wdrażały odpowiednie procedury rozpatrywania skarg złożonych przez osoby fizyczne, które uważają, że ich prywatność lub wolności obywatelskie zostały naruszone. Szefowie poszczególnych departamentów lub agencji muszą dopilnować, aby urzędnicy ds. prywatności i wolności obywatelskich dysponowali materiałami i zasobami niezbędnymi do wykonywania swoich uprawnień, mieli dostęp do wszelkich materiałów i zasobów osobowych niezbędnych do wypełniania swoich funkcji oraz byli informowani o proponowanych zmianach polityki, a także aby konsultowano się z nimi w sprawie odnośnych zmian ([192]). Urzędnicy ds. prywatności i wolności obywatelskich składają Kongresowi okresowe sprawozdania dotyczące m.in. liczby i rodzaju skarg otrzymanych przez departament/agencję oraz podsumowanie sposobu rozpatrzenia takich skarg, prowadzonych przeglądów i postępowań oraz wpływu działań przeprowadzonych przez urzędnika ([193]).

(109) Po drugie, niezależny Inspektor Generalny nadzoruje działalność Departamentu Sprawiedliwości, w tym FBI ([194]). Inspektorzy Generalni są niezależni ustawowo ([195]) i odpowiadają za przeprowadzanie niezależnych dochodzeń, audytów oraz kontroli programów i operacji departamentu. Mają wgląd we wszystkie rejestry, sprawozdania, audyty, przeglądy, dokumenty, opracowania, zalecenia lub inne istotne materiały, w razie potrzeby na mocy wezwania, oraz mogą odbierać zeznania ([196]). Chociaż Inspektorzy Generalni wydają niewiążące zalecenia dotyczące działań naprawczych, ich sprawozdania, m.in. na temat działań następczych (lub braku takich działań) ([197]), co do zasady są podawane do publicznej wiadomości i wysyłane do Kongresu, który na ich podstawie może wykonywać swoją funkcję nadzorczą (zob. motyw 111) ([198]).

([191]) Zob. tytuł 42 § 2000ee-1 U.S.C. Obejmuje to np. Departament Sprawiedliwości, Departament Bezpieczeństwa Wewnętrznego i FBI. Dodatkowo w przypadku Departamentu Bezpieczeństwa Krajowego główny urzędnik ds. prywatności odpowiada za zachowanie i wzmocnienie zabezpieczeń prywatności oraz za propagowanie przejrzystości w ramach departamentu (tytuł 6 rozdział 142 sekcja 222 U.S.C.). Wszystkie stosowane przez Departament Bezpieczeństwa Krajowego systemy, technologie, formularze i programy, które służą do gromadzenia danych osobowych lub mają wpływ na prywatność, podlegają nadzorowi ze strony głównego urzędnika ds. prywatności, który ma wgląd we wszystkie rejestry, sprawozdania, audyty, przeglądy, dokumenty, opracowania, zalecenia i inne materiały, do których departament ten ma dostęp, w razie potrzeby na mocy wezwania. Urzędnik ds. prywatności musi składać Kongresowi coroczne sprawozdanie z działań Departamentu Bezpieczeństwa Krajowego, które wpływają na prywatność, w tym skarg dotyczących naruszenia prywatności.

([192]) Tytuł 42 § 2000ee-1 lit. d) U.S.C.

([193]) Zob. tytuł 42 §§ 2000ee-1 lit. f) pkt 1–2 U.S.C. Na przykład ze sprawozdania głównego urzędnika ds. prywatności i wolności obywatelskich z ramienia DoJ oraz Biura Ochrony Prywatności i Wolności Obywatelskich, obejmującego okres od października 2020 r. do marca 2021 r., wynika, że przeprowadzono 389 przeglądów dotyczących prywatności, w tym systemów informacyjnych i innych programów (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

([194]) Podobnie w ustawie o bezpieczeństwie krajowym z 2002 r. ustanowiono Biuro Inspektora Generalnego w Departamencie Bezpieczeństwa Wewnętrznego.

([195]) Inspektorzy Generalni są powoływani na określoną kadencję i mogą zostać odwołani wyłącznie przez Prezydenta, który musi przedstawić Kongresowi pisemne uzasadnienie decyzji o ich odwołaniu.

([196]) Zob. § 6 ustawy o Inspektorze Generalnym z 1978 r.

([197]) Zob. w tym kontekście np. przygotowany przez Biuro Inspektora Generalnego w DoJ przegląd wydanych zaleceń oraz zakresu ich wdrożenia za pośrednictwem działań następczych departamentu i agencji, https://oig.justice.gov/sites/default/files/reports/22-043.pdf

([198]) Zob. § 4 ust. 5 i § 5 ustawy o Inspektorze Generalnym z 1978 r. Na przykład Biuro Inspektora Generalnego w DoJ opublikowało niedawno swoje sprawozdanie półroczne (za okres od 1 października 2021 r. do 31 marca 2022 r., https://oig.justice.gov/node/23596), które zostało przedłożone Kongresowi i które zawiera przegląd jego audytów, ocen, inspekcji, przeglądów specjalnych oraz dochodzeń w sprawie programów i operacji Departamentu Sprawiedliwości. Działania te obejmowały dochodzenie wszczęte wobec byłego wykonawcy w sprawie nielegalnego ujawnienia nadzoru elektronicznego (podsłuchu osoby fizycznej) w ramach prowadzonego dochodzenia, które doprowadziło do skazania wykonawcy. Biuro Inspektora Generalnego przeprowadziło również dochodzenie w sprawie programów i praktyk w zakresie bezpieczeństwa informacji stosowanych przez agencje DoJ, które obejmowało sprawdzenie skuteczności polityk, procedur i praktyk w zakresie bezpieczeństwa informacji wykorzystywanych przez reprezentatywny podzbiór systemów agencji.

(110) Po trzecie, w zakresie, w jakim prowadzą one działania antyterrorystyczne, departamenty odpowiedzialne za egzekwowanie prawa w sprawach karnych podlegają nadzorowi Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi (PCLOB), niezależnej agencji w ramach władzy wykonawczej złożonej z dwupartyjnego, pięcioosobowego zarządu powoływanego przez Prezydenta na sześcioletnią kadencję za zgodą Senatu ([199]). Zgodnie ze statutem założycielskim PCLOB powierzono obowiązki w obszarze kształtowania i wdrażania polityki walki z terroryzmem, aby zapewnić ochronę prywatności i wolności obywatelskich. W swoim przeglądzie Rada ma dostęp do wszystkich stosownych rejestrów, sprawozdań, audytów, przeglądów, dokumentów, opracowań i zaleceń agencji, z uwzględnieniem informacji niejawnych, oraz może przeprowadzać przesłuchania i odbierać zeznania ([200]). Rada otrzymuje sprawozdania od urzędników ds. wolności obywatelskich i prywatności z szeregu departamentów/agencji federalnych ([201]), może wydawać zalecenia skierowane do rządu i organów egzekwowania prawa i regularnie sporządza sprawozdania dla komisji Kongresu i dla Prezydenta ([202]). Sprawozdania Rady, w tym te przedkładane Kongresowi, muszą być w możliwie największym stopniu dostępne publicznie ([203]).

(111) Ponadto działania w zakresie ścigania przestępstw podlegają nadzorowi ze strony konkretnych komisji działających w Kongresie Stanów Zjednoczonych (Komisje ds. Sprawiedliwości w Izbie Reprezentantów i w Senacie). Komisje ds. Sprawiedliwości przeprowadzają regularny nadzór w różnych formach, w szczególności w formie przesłuchań, dochodzeń, przeglądów i sprawozdań ([204]).

3.1.3. *Dochodzenie roszczeń*

(112) Jak już wskazano, w większości przypadków organy egzekwowania prawa w sprawach karnych muszą uzyskać wcześniej zgodę organu sądowego na gromadzenie danych osobowych. Chociaż wcześniejsza zgoda organu sądowego nie jest wymagana w odniesieniu do wezwań administracyjnych, wezwania te ograniczają się do określonych sytuacji i będą podlegać niezależnej kontroli sądowej przynajmniej wtedy, gdy rząd dochodzi egzekwowania prawa w sądzie. W szczególności adresaci wezwań administracyjnych mogą podważyć je w sądzie na tej podstawie, że są one niezasadne, tj. przesadzone, opresyjne lub uciążliwe ([205]).

(113) Osoby fizyczne mogą najpierw składać wnioski lub skargi do organów egzekwowania prawa w sprawach karnych dotyczące przetwarzania ich danych osobowych. Obejmuje to możliwość wnioskowania o dostęp do danych osobowych i ich korektę ([206]). Jeżeli chodzi o działania związane ze zwalczaniem terroryzmu, osoby fizyczne mogą również złożyć skargę do urzędników ds. prywatności i wolności obywatelskich (lub innych urzędników ds. ochrony prywatności) w organach egzekwowania prawa ([207]).

(114) Ponadto w prawie amerykańskim osobom fizycznym zapewniono szereg sądowych środków odwoławczych wobec organu publicznego lub jednego z urzędników takiego organu, w przypadku gdy te organy przetwarzają dane osobowe ([208]). Ze wspomnianych środków przewidzianych w szczególności w ustawie o postępowaniu administracyjnym, ustawie o dostępie do informacji publicznej i ustawie o ochronie danych w łączności elektronicznej mogą skorzystać wszystkie osoby fizyczne, niezależnie od ich obywatelstwa, o ile spełnią odpowiednie warunki.

([199]) Członkowie Rady muszą być wybierani wyłącznie na podstawie kwalifikacji zawodowych, osiągnięć, pozycji społecznej, wiedzy fachowej w dziedzinie wolności obywatelskich i prywatności oraz odpowiedniego doświadczenia, bez względu na przynależność polityczną. W skład Rady w żadnym wypadku nie może wchodzić więcej niż trzech członków tej samej partii politycznej. Podczas pełnienia funkcji w Radzie osoba powołana do Rady nie może być urzędnikiem wybieranym, urzędnikiem ani pracownikiem rządu federalnego, innym niż pełniącym funkcję członka Rady. Zob. tytuł 42 § 2000ee lit. h) U.S.C.

([200]) Tytuł 42 § 2000ee lit. g) U.S.C.

([201]) Zob. tytuł 42 § 2000ee-1 lit. f) pkt 1 ppkt A pppkt (iii) U.S.C. Należy wśród nich wymienić przynajmniej Departament Sprawiedliwości, Departament Obrony, Departament Bezpieczeństwa Wewnętrznego, a także wszelkie inne departamenty, agencje lub jednostki struktury władzy wykonawczej wskazane jako właściwe przez PCLOB.

([202]) Tytuł 42 § 2000ee lit. e) U.S.C.

([203]) Tytuł 42 § 2000ee lit. f) U.S.C.

([204]) Na przykład komisje organizują przesłuchania tematyczne (zob. na przykład ostatnie przesłuchanie Komisji ds. Sprawiedliwości w Izbie Reprezentantów w sprawie „cyfrowych obław",https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), jak również regularne przesłuchania nadzorcze, np. FBI i DoJ, zob. https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 i https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899

([205]) Zob. załącznik VI.

([206]) Okólnik OMB nr A-130, dodatek II, sekcja 3 lit. a) i f), który zobowiązuje agencje federalne do zapewnienia odpowiedniego dostępu i korekty na wniosek osób fizycznych oraz do ustanowienia procedur przyjmowania i rozpatrywania skarg i wniosków dotyczących prywatności.

([207]) Zob. tytuł 42 § 2000ee-1 U.S.C. w odniesieniu do np. Departamentu Sprawiedliwości USA i Departamentu Bezpieczeństwa Wewnętrznego. Zob. również Memorandum OMB M-16-24, Role i wyznaczenie urzędników wyższego szczebla Agencji ds. Prywatności.

([208]) Mechanizmy odwoławcze, o których mowa w niniejszej sekcji, mają również zastosowanie do gromadzenia i wykorzystywania danych przez organy federalne do celów cywilnych i regulacyjnych.

(115) Co do zasady, zgodnie z przepisami dotyczącymi kontroli sądowej ustanowionymi w ustawie o postępowaniu administracyjnym ([209]) „każda osoba doznająca krzywdy w świetle prawa w wyniku działania agencji lub dotknięta negatywnymi skutkami takiego działania lub poszkodowana w wyniku działań prowadzonych przez agencję" może wystąpić o kontrolę sądową ([210]). Obejmuje to możliwość wystąpienia do sądu o „uznanie za bezprawne i uchylenie działań, ustaleń i wniosków agencji, w przypadku których okazało się, że są […] arbitralne, nieprzemyślane, stanowią nadużycie uprawnień lub w inny sposób są niezgodne z prawem" ([211]).

(116) Ściślej rzecz ujmując, w tytule II ustawy o ochronie danych w łączności elektronicznej ([212]) ustanowiono system ustawowych praw w obszarze prywatności, który reguluje kwestie związane z dostępem organów egzekwowania prawa do treści komunikatów przekazywanych za pomocą łączności przewodowej, ustnie lub za pomocą łączności elektronicznej przechowywanych przez dostawców usług będących stronami trzecimi ([213]). W świetle przepisów ustawy bezprawny (tj. w braku stosownego upoważnienia wydanego przez sąd lub innego zezwolenia) dostęp do takich komunikatów jest uznawany za przestępstwo i daje pokrzywdzonej osobie prawo wytoczenia powództwa cywilnego przed amerykański sąd federalny o odszkodowanie za faktycznie poniesione szkody lub o odszkodowanie karne, a także o zasądzenie godziwego zadośćuczynienia od Stanów Zjednoczonych lub od urzędnika rządowego, który umyślnie dopuścił się tego rodzaju czynów zabronionych, lub wystąpienia z wnioskiem o wydanie deklaratywnego orzeczenia ustalającego wobec takiego urzędnika lub wobec Stanów Zjednoczonych.

(117) Ponadto w kilku innych ustawach przyznaje się osobom fizycznym prawo do wytoczenia powództwa przeciwko organowi publicznemu lub urzędnikowi Stanów Zjednoczonych w związku z przetwarzaniem ich danych osobowych, takich jak ustawa o podsłuchach ([214]), ustawa o oszustwach i nadużyciach komputerowych ([215]), ustawa federalna o roszczeniach z tytułu czynu niedozwolonego ([216]), ustawa o prawie do prywatności w kwestiach finansowych ([217]) oraz ustawa o rzetelnej sprawozdawczości kredytowej ([218]).

([209]) Tytuł 5 § 702 U.S.C.

([210]) Zasadniczo przedmiotem kontroli sądowej może być wyłącznie „końcowe" działanie agencji, a nie jej „wstępne, procesowe lub pośrednie" działanie. Zob. tytuł 5 § 704 U.S.C.

([211]) Tytuł 5 § 706 ust. 2 pkt A U.S.C.

([212]) Tytuł 18 §§ 2701–2712 U.S.C.

([213]) Przepisy ustawy o ochronie danych w łączności elektronicznej chronią komunikaty przechowywane przez podmioty należące do dwóch określonych kategorii dostawców usług sieciowych, mianowicie: (i) dostawców usług łączności elektronicznej, na przykład usług telefonicznych lub usług poczty elektronicznej; (ii) dostawców zdalnych usług komputerowych, takich jak komputerowe usługi przechowywania lub przetwarzania danych.

([214]) Tytuł 18 §§ 2510 i nast. U.S.C. Na mocy ustawy o podsłuchach (tytuł 18 § 2520 U.S.C.) osoba, której łączność przewodowa, komunikacja ustna lub elektroniczna jest przechwytywana, ujawniana lub celowo wykorzystywana, może wytoczyć powództwo cywilne o naruszenie ustawy o podsłuchach, w tym, w pewnych okolicznościach, wobec określonego urzędnika rządowego lub Stanów Zjednoczonych. Aby uzyskać więcej informacji na temat gromadzenia informacji niedotyczących treści (np. adresu IP, przychodzący/wychodzący adres e-mail), zob. także rozdział w tytule 18 dotyczący urządzeń rejestrujących wybierane numery oraz urządzeń śledzących (tytuł 18 §§ 3121–3127 U.S.C., a w przypadku powództwa cywilnego – § 2707).

([215]) Tytuł 18 § 1030 U.S.C. Na mocy ustawy o oszustwach i nadużyciach komputerowych osoba może wnieść powództwo przeciwko dowolnej osobie w związku z umyślnym uzyskiwaniem nieuprawnionego dostępu (lub przekraczaniem granic uprawnionego dostępu) w celu pozyskania informacji z instytucji finansowej, systemu komputerowego rządu Stanów Zjednoczonych lub innego określonego komputera, w tym, w pewnych okolicznościach, przeciwko określonemu urzędnikowi rządowemu.

([216]) Tytuł 28 §§ 2671 i nast. U.S.C. Na mocy ustawy federalnej o roszczeniach z tytułu czynu niedozwolonego dana osoba może wytoczyć powództwo, w pewnych okolicznościach, przeciwko Stanom Zjednoczonym w związku z „zaniedbaniem lub niewłaściwym działaniem lub zaniechaniem ze strony dowolnego pracownika rządu podczas prowadzenia działań wchodzących w zakres jego urzędu lub stanowiska".

([217]) Tytuł 12 §§ 3401 i nast. U.S.C. Na mocy ustawy o prawie do prywatności w kwestiach finansowych dana osoba może wytoczyć powództwo, w pewnych okolicznościach, przeciwko Stanom Zjednoczonym w związku z uzyskaniem lub ujawnieniem chronionych dokumentów finansowych z naruszeniem ustawy. Rząd co do zasady nie ma dostępu do chronionych dokumentów finansowych, chyba że złoży wniosek, z zastrzeżeniem zgodnego z prawem wezwania lub nakazu przeszukania, lub – z zastrzeżeniem ograniczeń – formalny wniosek pisemny, a osoba fizyczna, na temat której chce uzyskać informacje, zostanie powiadomiona o takim wniosku.

([218]) Tytuł 15 §§ 1681–1681x U.S.C. Na mocy ustawy o rzetelnej sprawozdawczości kredytowej dana osoba może wnieść powództwo przeciwko dowolnej osobie, która nie przestrzega wymogów (w szczególności wymogu uzyskania prawnego upoważnienia) dotyczących gromadzenia, upowszechniania i wykorzystywania informacji dotyczących kredytów konsumentów, lub, w pewnych okolicznościach, przeciwko agencji rządowej.

(118) Ponadto zgodnie z Ustawą o dostępie do informacji publicznej ([219]) (tytuł 5 § 552 U.S.C.) każdy ma prawo do wglądu w rejestr prowadzony przez agencję federalną, w tym w przypadku, gdy zawiera on dane osobowe tej osoby. Po wyczerpaniu administracyjnych środków ochrony prawnej – do egzekwowania tego prawa przed sądem, o ile wspomniane rejestry nie są objęte ochroną przed publicznym ujawnieniem na mocy wyjątku lub przepisów szczególnych wyłączających ich jawność ze względów związanych z egzekwowaniem prawa ([220]). W takim przypadku sąd oceni, czy zastosowanie ma jakikolwiek wyjątek lub czy został on zgodnie z prawem przywołany przez właściwy organ publiczny.

3.2. **Dostęp amerykańskich organów publicznych do danych w celach związanych z bezpieczeństwem narodowym i korzystanie przez amerykańskie organy publiczne z tych danych w celach związanych z bezpieczeństwem narodowym**

(119) W prawie Stanów Zjednoczonych ustanowiono różne ograniczenia i zabezpieczenia w zakresie dostępu do danych osobowych i korzystania z nich do celów bezpieczeństwa narodowego, a także mechanizmy nadzoru i dochodzenia roszczeń, które są zgodne z wymogami określonymi w motywie 89 niniejszej decyzji. Warunki uzyskania takiego dostępu oraz zabezpieczenia mające zastosowanie do wykonywania tych uprawnień poddano szczegółowej ocenie w kolejnych sekcjach.

3.2.1. ***Podstawy prawne, ograniczenia i zabezpieczenia***

3.2.1.1. *Obowiązujące ramy prawne*

(120) Organy amerykańskie mogą gromadzić dane osobowe przekazywane z Unii do podmiotów objętych DPF UE–USA do celów bezpieczeństwa narodowego na podstawie różnych instrumentów prawnych, z zastrzeżeniem szczególnych warunków i zabezpieczeń.

(121) Po otrzymaniu danych osobowych przez podmioty mające siedzibę w Stanach Zjednoczonych, amerykańskie agencje wywiadowcze mogą ubiegać się o dostęp do tych danych jedynie do celów związanych z bezpieczeństwem narodowym wyłącznie zgodnie z ustawą stanowiącą podstawę prawną, w szczególności zgodnie z ustawą o kontroli wywiadu lub przepisami prawa stanowionego zezwalających na dostęp z wykorzystaniem wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego ([221]). W ustawie o kontroli wywiadu przewidziano szereg podstaw prawnych, na których można się oprzeć przy gromadzeniu (i późniejszym przetwarzaniu) danych osobowych osób z Unii, których dane dotyczą, przekazywanych zgodnie z DPF UE–USA (sekcja 105 ustawy o kontroli wywiadu ([222]), sekcja 302 ustawy o kontroli wywiadu ([223]), sekcja 402 ustawy o kontroli wywiadu ([224]), sekcja 501 ustawy o kontroli wywiadu ([225]) i sekcja 702 ustawy o kontroli wywiadu ([226])), co opisano bardziej szczegółowo w motywach 142–152.

([219]) Tytuł 5 § 552 U.S.C.

([220]) Wspomniane wyłączenia są jednak objęte ramami. Np. zgodnie z tytułem 5 § 552 lit. b) pkt 7 U.S.C. niemożliwe jest egzekwowanie praw wynikających z Ustawy o dostępie do informacji publicznej w odniesieniu do „rejestrów lub informacji zebranych do celów egzekwowania prawa, ale tylko w zakresie, w jakim sporządzanie takich rejestrów lub informacji przez organy egzekwowania prawa (A) może w sposób uzasadniony zakłócić postępowanie egzekucyjne, (B) może pozbawić daną osobę prawa do rzetelnego procesu sądowego lub bezstronnego wyroku, (C) może w sposób uzasadniony stanowić nieuzasadnione naruszenie prywatności danej osoby, (D) może doprowadzić do ujawnienia tożsamości poufnego źródła, w tym państwa, lokalnej lub zagranicznej agencji lub organu lub dowolnej prywatnej instytucji, która przekazała informacje o charakterze poufnym, a także w przypadku rejestrów lub informacji zebranych przez organ egzekwowania prawa w sprawach karnych w toku dochodzenia lub przez agencję prowadzącą zgodne z prawem krajowe dochodzenie do celów bezpieczeństwa narodowego, informacji przekazanych przez poufne źródło, (E) może doprowadzić do ujawnienia technik i procedur prowadzenia dochodzeń i spraw sądowych dotyczących egzekwowania prawa, jeżeli takie ujawnienie mogłoby w uzasadniony sposób zagrozić obejściem prawa, lub (F) może w sposób uzasadniony zagrozić życiu lub bezpieczeństwu fizycznemu dowolnej osoby fizycznej". Ponadto „ilekroć zostanie złożony wniosek dotyczący dostępu do rejestrów [których przedstawienie może w sposób uzasadniony zakłócić postępowanie egzekucyjne] oraz – ilekroć (A) dochodzenie lub postępowanie dotyczy możliwego naruszenia prawa karnego; (B) jeżeli istnieje powód, aby sądzić, że (i) osoba objęta dochodzeniem lub postępowaniem nie zdaje sobie sprawy z trwania takiego dochodzenia lub postępowania oraz (ii) ujawnienie istnienia rejestrów może w sposób uzasadniony zakłócić postępowanie egzekucyjne, agencja może, tylko w takich okolicznościach, uznać, że wymogi określone w tej sekcji nie mają zastosowania do rejestrów" (tytuł 5 § 552 lit. c) pkt 1 U.S.C.).

([221]) Tytuł 12 § 3414 U.S.C.; tytuł 15 §§ 1681u–1681v U.S.C. oraz tytuł 18 § 2709 U.S.C. Zob. motyw 153.

([222]) Tytuł 50 § 1804 U.S.C., który dotyczy tradycyjnego zindywidualizowanego dozoru elektronicznego.

([223]) Tytuł 50 § 1822 U.S.C., który dotyczy przeszukań fizycznych do celów wywiadu zagranicznego.

([224]) Tytuł 50 § 1842 i § 1841 ust. 2 i tytuł 18 sekcja 3127 U.S.C., które dotyczą instalacji urządzeń rejestrujących wybierane numery lub urządzeń śledzących.

([225]) Tytuł 50 § 1861 U.S.C., który zezwala FBI na złożenie „wniosku o wydanie nakazu upoważniającego przewoźnika, publiczny obiekt noclegowy, punkt fizycznego składowania lub wypożyczalnię pojazdów do udostępnienia danych znajdujących się w ich posiadaniu na potrzeby dochodzenia mającego na celu pozyskanie danych wywiadowczych lub dochodzenia dotyczącego międzynarodowego terroryzmu".

([226]) Tytuł 50 § 1881 lit. a) U.S.C., który umożliwia amerykańskiej Wspólnocie Wywiadowczej staranie się o uzyskanie dostępu do informacji, w tym treści komunikatów internetowych, od przedsiębiorstw amerykańskich, ukierunkowując działania na określone osoby niebędące obywatelami ani rezydentami USA przebywające poza Stanami Zjednoczonymi, z prawnie wymaganą pomocą dostawców usług łączności elektronicznej.

(122) Amerykańskie agencje wywiadowcze mają również możliwość gromadzenia danych osobowych poza Stanami Zjednoczonymi, przy czym może to obejmować dane osobowe, które są w tranzycie między Unią a Stanami Zjednoczonymi. Gromadzenie danych osobowych poza Stanami Zjednoczonymi opiera się na rozporządzeniu wykonawczym 12333 („rozporządzenie wykonawcze 12333") ([227]) wydanym przez Prezydenta ([228]).

(123) Gromadzenie danych w ramach rozpoznania radioelektronicznego jest formą gromadzenia danych wywiadowczych najwłaściwszą dla obecnego stwierdzania odpowiedniego stopnia ochrony, ponieważ dotyczy ona gromadzenia komunikatów elektronicznych i danych z systemów informacyjnych. Takie gromadzenie danych mogą przeprowadzać amerykańskie agencje wywiadowcze zarówno w Stanach Zjednoczonych (na podstawie ustawy o kontroli wywiadu), jak i w ramach tranzytu danych do Stanów Zjednoczonych (na podstawie rozporządzenia wykonawczego 12333).

(124) 7 października 2022 r. Prezydent Stanów Zjednoczonych wydał rozporządzenie wykonawcze 14086 w sprawie wzmocnienia zabezpieczeń w odniesieniu do działań Stanów Zjednoczonych w zakresie rozpoznania radioelektronicznego, w którym określono ograniczenia i zabezpieczenia dotyczące wszystkich prowadzonych przez Stany Zjednoczone działań w zakresie rozpoznania radioelektronicznego. To rozporządzenie wykonawcze zastępuje w znacznej mierze dyrektywę polityczną Prezydenta nr 28 (PPD-28) ([229]), a jego celem jest wzmocnienie warunków, ograniczeń i zabezpieczeń mających zastosowanie do wszystkich działań w zakresie rozpoznania radioelektronicznego (tj. na podstawie ustawy o kontroli wywiadu i rozporządzenia wykonawczego 12333) na niezależnie od miejsca ich wykonywania ([230]) oraz ustanowienie nowego mechanizmu dochodzenia roszczeń, za którego pośrednictwem osoby fizyczne mogą powoływać się na te zabezpieczenia oraz je egzekwować ([231]) (więcej szczegółów podano w motywach 176–194). W ten sposób rozporządzenie to wdraża do prawa amerykańskiego wynik rozmów przeprowadzonych między UE i USA po unieważnieniu przez Trybunał Sprawiedliwości decyzji Komisji stwierdzającej odpowiedni stopień ochrony w ramach Tarczy Prywatności (zob. motyw 6). W związku z tym stanowi ono szczególnie ważny element ram prawnych będących przedmiotem oceny w niniejszej decyzji.

(125) Ograniczenia i zabezpieczenia wprowadzone rozporządzeniem wykonawczym 14086 uzupełniają ograniczenia i zabezpieczenia przewidziane w sekcji 702 ustawy o kontroli wywiadu i rozporządzeniu wykonawczym 12333. Wymogi opisane poniżej (w sekcjach 3.2.1.2 i 3.2.1.3) muszą być stosowane przez agencje wywiadowcze podczas angażowania się w działania w zakresie rozpoznania radioelektronicznego zgodnie z sekcją 702 ustawy o kontroli wywiadu i rozporządzeniem wykonawczym 12333, np. przy wyborze/identyfikowaniu kategorii danych wywiadowczych, które mają zostać pozyskane zgodnie z sekcją 702 ustawy o kontroli wywiadu; gromadzeniu danych w obszarze wywiadu lub kontrwywiadu zagranicznego zgodnie z rozporządzeniem wykonawczym 12333; oraz podejmowaniu indywidualnych decyzji o ukierunkowywaniu na podstawie sekcji 702 ustawy o kontroli wywiadu i rozporządzenia wykonawczego 12333.

(126) Wymogi określone w tym rozporządzeniu wykonawczym wydanym przez Prezydenta są wiążące dla całej Wspólnoty Wywiadowczej. Muszą one być wdrażane w ramach strategii politycznych i procedur agencji, które przekładają je na konkretne kierunki codziennej działalności. W tym względzie rozporządzenie wykonawcze 14086 zapewnia amerykańskim agencjom wywiadowczym maksymalnie rok na aktualizację ich obowiązujących strategii politycznych i procedur (tj. do 7 października 2023 r.) w celu dostosowania ich do wymogów tego rozporządzenia wykonawczego. Takie zaktualizowane strategie polityczne i procedury muszą być opracowywane w porozumieniu z prokuratorem generalnym, urzędnikiem ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych (Urząd Dyrektora Krajowych Służb Wywiadowczych Biura Wolności Obywatelskich i Ochrony Prywatności) i Radą Nadzoru nad Ochroną Danych i Wolnościami Obywatelskimi (PCLOB) – niezależnym organem nadzorczym uprawnionym do przeglądu strategii politycznych realizowanych przez władzę wykonawczą i ich wdrażania w celu ochrony prywatności i wolności obywatelskich (zob. motyw 110 w odniesieniu do roli i statusu PCLOB) – oraz muszą być podawane do wiadomości publicznej ([232]). Ponadto po wprowadzeniu zaktualizowanych

([227]) Rozporządzenie wykonawcze 12333: Działalność wywiadowcza Stanów Zjednoczonych, Rejestr Federalny t. 40, nr 235 (8 grudnia 1981 r., ze zmianami wprowadzonymi 30 lipca 2008 r.). W rozporządzeniu wykonawczym 12333 określono ogólniej cele, kierunki prac, zadania i obowiązki amerykańskich agencji wywiadowczych (w tym funkcje określonych jednostek Wspólnoty Wywiadowczej), a także ustanowiono ogólne parametry regulujące działalność agencji wywiadowczych.

([228]) Zgodnie z art. II konstytucji Stanów Zjednoczonych odpowiedzialność za zapewnienie bezpieczeństwa narodowego, w tym w szczególności gromadzenie danych wywiadowczych, spoczywa na Prezydencie, który pełni funkcję Zwierzchnika Sił Zbrojnych.

([229]) Rozporządzenie wykonawcze 14086 zastępuje poprzednią dyrektywę Prezydenta, dyrektywę polityczną Prezydenta nr 28, z wyjątkiem jej sekcji 3 i uzupełniającego ją załącznika (który nakłada na agencje wywiadowcze wymóg corocznego przeglądu ich priorytetów wywiadowczych i wymogów w zakresie rozpoznania radioelektronicznego, z uwzględnieniem korzyści płynących z działań w zakresie rozpoznania radioelektronicznego dla interesów narodowych Stanów Zjednoczonych oraz ryzyka stwarzanego przez te działania) oraz sekcji 6 (która zawiera przepisy ogólne); zob. memorandum w sprawie bezpieczeństwa narodowego, które dotyczy częściowego uchylenia dyrektywy politycznej Prezydenta nr 28, dostępne na stronie:https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/

([230]) Zob. sekcja 5 lit. f) rozporządzenia wykonawczego 14086, w której wyjaśniono, że rozporządzenie wykonawcze ma taki sam zakres stosowania jak dyrektywa polityczna Prezydenta nr 28, która – zgodnie z zawartym w niej przypisem nr 3 – ma zastosowanie do działań w zakresie rozpoznania radioelektronicznego przeprowadzanych w celu gromadzenia komunikatów lub informacji na temat komunikatów, z wyjątkiem działań w zakresie rozpoznania radioelektronicznego przeprowadzanych w celu przetestowania lub opracowania zdolności w zakresie rozpoznania radioelektronicznego.

([231]) Zob. w tym zakresie np. sekcja 5 lit. h) rozporządzenia wykonawczego 14086, w której wyjaśniono, że zabezpieczenia przewidziane w tym rozporządzeniu wykonawczym stanowią podstawę upoważnienia prawnego i że osoby fizyczne mogą je egzekwować za pośrednictwem mechanizmu dochodzenia roszczeń.

([232]) Zob. sekcja 2 lit. c) pkt (iv) ppkt C rozporządzenia wykonawczego 14086.

strategii politycznych i procedur PCLOB przeprowadzi przegląd w celu zapewnia ich zgodności z rozporządzeniem wykonawczym. W terminie 180 dni po zakończeniu takiego przeglądu przez PCLOB każda agencja wywiadowcza musi starannie rozważyć i wdrożyć wszystkie zalecenia PCLOB lub w inny sposób zastosować się do nich. 3 lipca 2023 r. rząd USA opublikował takie zaktualizowane strategie i procedury ([233]).

3.2.1.2. *Ograniczenia i zabezpieczenia odnoszące się do gromadzenia danych osobowych do celów związanych z bezpieczeństwem narodowym*

(127) W rozporządzeniu wykonawczym 14086 określono szereg nadrzędnych wymogów, które mają zastosowanie do wszystkich działań w zakresie rozpoznania radioelektronicznego (gromadzenie, wykorzystywanie, rozpowszechnianie itp. danych osobowych).

(128) Po pierwsze, podstawą takich działań muszą być przepisy ustawy lub upoważnienie wydane przez Prezydenta i takie działania muszą być podejmowane zgodnie z prawem amerykańskim, w tym zgodnie z konstytucją ([234]).

(129) Po drugie, muszą istnieć odpowiednie zabezpieczenia w celu zapewnienia, by prywatność i wolności obywatelskie miały kluczowe znaczenie w kontekście planowania takich działań ([235]).

(130) W szczególności wszystkie działania w zakresie rozpoznania radioelektronicznego mogą być prowadzone wyłącznie „po ustaleniu, na podstawie racjonalnej oceny wszystkich istotnych czynników, że działania te są niezbędne do realizacji zatwierdzonego priorytetu wywiadowczego" (w odniesieniu do terminu „zatwierdzony priorytet wywiadowczy" zob. motyw 135) ([236]).

(131) Ponadto takie działania mogą być prowadzone wyłącznie „w takim zakresie i w taki sposób, które są proporcjonalne do zatwierdzonego priorytetu wywiadowczego, w odniesieniu do którego zostały one dozwolone" ([237]). Innymi słowy, należy osiągnąć odpowiednią równowagę „między znaczeniem realizowanego priorytetu wywiadowczego a wpływem na prywatność i wolności obywatelskie osób fizycznych, których to dotyczy, niezależnie od ich narodowości lub miejsca zamieszkania" ([238]).

(132) Ponadto, aby zapewnić zgodność z tymi wymogami ogólnymi, które odzwierciedlają zasady legalności, konieczności i proporcjonalności, działania w zakresie rozpoznania radioelektronicznego podlegają nadzorowi (więcej szczegółów na ten temat podano w sekcji 3.2.2) ([239]).

(133) Te nadrzędne wymogi są ponadto uzasadnione w kontekście gromadzenia danych w ramach rozpoznania radioelektronicznego poprzez szereg warunków i ograniczeń zapewniających, aby ingerowanie w prawa osób fizycznych było ograniczone do tego, co jest niezbędne i proporcjonalne do realizacji uzasadnionego celu.

(134) Po pierwsze, w rozporządzeniu wykonawczym ogranicza się powody, dla których dane mogą być gromadzone w ramach działań w zakresie rozpoznania radioelektronicznego, na dwa sposoby. Z jednej strony w rozporządzeniu wykonawczym określono uzasadnione cele, które można realizować przez gromadzenie danych w wyniku rozpoznania radioelektronicznego, np. w celu zrozumienia lub oceny możliwości, zamiarów lub działań zagranicznych podmiotów, w tym międzynarodowych organizacji terrorystycznych, które stwarzają faktyczne lub potencjalne zagrożenie dla bezpieczeństwa narodowego Stanów Zjednoczonych, w celu ochrony przed zagranicznymi zdolnościami i działaniami wojskowymi oraz w celu zrozumienia lub oceny transgranicznych zagrożeń, które wpływają na bezpieczeństwo globalne, takich jak zmiana klimatu i inne zmiany ekologiczne, zagrożenia dla zdrowia publicznego i zagrożenia natury humanitarnej ([240]). Z drugiej strony w rozporządzeniu wykonawczym wymieniono określone

([233]) https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086.

([234]) Sekcja 2 lit. a) pkt (i) rozporządzenia wykonawczego 14086.

([235]) Sekcja 2 lit. a) pkt (ii) rozporządzenia wykonawczego 14086.

([236]) Sekcja 2 lit. a) pkt (ii) ppkt A rozporządzenia wykonawczego 14086. Nie zawsze wymaga to, aby rozpoznanie radioelektroniczne było jedynym sposobem realizacji aspektów zatwierdzonego priorytetu wywiadowczego. Na przykład gromadzenie danych w ramach rozpoznania radioelektronicznego może być wykorzystywane do zapewnienia alternatywnych ścieżek zatwierdzenia (np. w celu potwierdzenia informacji otrzymanych z innych źródeł wywiadowczych) lub do utrzymania niezawodnego dostępu do tych samych informacji (sekcja 2 lit. c) pkt (i) ppkt A rozporządzenia wykonawczego 14086).

([237]) Sekcja 2 lit. a) pkt (ii) ppkt B rozporządzenia wykonawczego 14086.

([238]) Sekcja 2 lit. a) pkt (ii) ppkt B rozporządzenia wykonawczego 14086.

([239]) Sekcja 2 lit. a) pkt (iii) w związku z sekcją 2 lit. d) rozporządzenia wykonawczego 14086.

([240]) Sekcja 2 lit. b) pkt (i) rozporządzenia wykonawczego 14086. Ze względu na ograniczony wykaz uzasadnionych celów rozporządzenia wykonawczego, który nie obejmuje ewentualnych przyszłych zagrożeń, rozporządzenie wykonawcze zapewnia Prezydentowi możliwość aktualizacji tego wykazu w przypadku zaistnienia nowych okoliczności związanych z bezpieczeństwem narodowym, takich jak nowe zagrożenia dla bezpieczeństwa narodowego. Takie aktualizacje muszą co do zasady zostać podane do wiadomości publicznej, chyba że Prezydent uzna, że takie działanie może samo w sobie stworzyć zagrożenie dla bezpieczeństwa narodowego Stanów Zjednoczonych (sekcja 2 lit. b) pkt (i) ppkt B rozporządzenia wykonawczego 14086).

cele, których nigdy nie wolno realizować za pomocą działań w zakresie rozpoznania radioelektronicznego, np. w celu wywołania krytyki lub sprzeciwu lub swobodnego wyrażania pomysłów lub opinii politycznych przez jednostki lub prasę, w celu działania na niekorzyść danej jednostki ze względu na jej pochodzenie etniczne, rasę, płeć, tożsamość płciową, orientację seksualną lub religię lub w celu przyznania przewagi konkurencyjnej amerykańskim przedsiębiorstwom ([241]).

(135) Ponadto agencje wywiadowcze nie mogą powoływać się na uzasadnione cele określone w rozporządzeniu wykonawczym 14086 same w sobie, aby uzasadnić gromadzenie danych w wyniku rozpoznania radioelektronicznego, lecz cele te muszą być dodatkowo poparte – w przypadku celów operacyjnych – bardziej konkretnymi priorytetami, w odniesieniu do których można gromadzić dane w wyniku rozpoznania radioelektronicznego. Innymi słowy, faktyczne gromadzenie danych może odbywać się wyłącznie w celu realizacji bardziej konkretnego priorytetu. Takie priorytety są ustalane za pośrednictwem specjalnego procesu, którego celem jest zapewnienie zgodności z mającymi zastosowanie wymogami prawnymi, w tym wymogami dotyczącymi prywatności i wolności obywatelskich. Ściślej rzecz ujmując, priorytety wywiadowcze są najpierw opracowywane przez Dyrektora Krajowych Służb Wywiadowczych (za pośrednictwem tak zwanych ram amerykańskich priorytetów wywiadowczych), a następnie przedstawiane Prezydentowi do zatwierdzenia ([242]). Przed zaproponowaniem priorytetów wywiadowczych Prezydentowi Dyrektor musi, zgodnie z rozporządzeniem wykonawczym 14086, uzyskać od Biura Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych ocenę każdego priorytetu pod kątem tego, czy dany priorytet 1) przyczynia się do realizacji co najmniej jednego uzasadnionego celu wymienionego w rozporządzeniu wykonawczym; 2) ani nie został zaprojektowany z myślą o gromadzeniu danych w wyniku rozpoznania radioelektronicznego, ani nie przewiduje się, że spowoduje on gromadzenie danych w wyniku rozpoznania radioelektronicznego na potrzeby realizacji zakazanego celu wymienionego w rozporządzeniu wykonawczym; oraz 3) został określony po odpowiednim uwzględnieniu prywatności i wolności obywatelskich wszystkich osób, niezależnie od ich narodowości lub miejsca zamieszkania ([243]). W przypadku gdy Dyrektor nie zgodzi się z oceną Biura Wolności Obywatelskich i Ochrony Prywatności, obie opinie muszą zostać przedstawione Prezydentowi ([244]).

(136) W związku z tym proces ten w szczególności zapewnia uwzględnienie kwestii związanych z prywatnością już na początkowym etapie, kiedy priorytety wywiadowcze są opracowywane.

(137) Po drugie, po ustaleniu priorytetu wywiadowczego szereg wymogów determinuje wydanie decyzji, czy można gromadzić dane w ramach rozpoznania radioelektronicznego w celu realizacji takiego priorytetu, a jeśli tak, to w jakim zakresie. Wymogi te zapewniają wypełnienie nadrzędnych standardów niezbędności i proporcjonalności określonych w sekcji 2 lit. a) rozporządzenia wykonawczego.

(138) W szczególności dane w ramach rozpoznania radioelektronicznego mogą być gromadzone wyłącznie „po ustaleniu, na podstawie racjonalnej oceny wszystkich istotnych czynników, że gromadzenie tych danych jest niezbędne do realizacji konkretnego priorytetu wywiadowczego" ([245]). Przy ustalaniu, czy konkretne działanie w obszarze gromadzenia danych w wyniku rozpoznania radioelektronicznego jest niezbędne do realizacji zatwierdzonego priorytetu wywiadowczego, amerykańskie agencje wywiadowcze muszą wziąć pod uwagę dostępność, wykonalność i stosowność innych, mniej inwazyjnych źródeł i metod, w tym wywodzących się ze źródeł dyplomatycznych i publicznych ([246]). Jeżeli takie alternatywne mniej inwazyjne źródła i metody są dostępne, należy stosować je w pierwszej kolejności ([247]).

(139) Jeżeli na podstawie wspomnianych kryteriów gromadzenie danych w ramach rozpoznania radioelektronicznego zostanie uznane za niezbędne, musi być ono „dostosowane do danych potrzeb" i „nie może wywierać nieproporcjonalnego wpływu na prywatność i wolności obywatelskie" ([248]). W celu zapewnienia, by na prywatność i wolności obywatelskie nie był wywierany nieproporcjonalny wpływ– tj. aby osiągnąć właściwą równowagę między potrzebami związanymi z bezpieczeństwem narodowym a ochroną prywatności i wolności obywatelskich – należy odpowiednio uwzględnić wszystkie istotne czynniki, takie jak charakter realizowanego celu, inwazyjność działania polegającego na gromadzeniu danych, w tym jego czas trwania, prawdopodobny wkład gromadzenia danych w realizację celu, konsekwencje dla osób fizycznych, które można racjonalnie przewidzieć, oraz charakter i wrażliwość danych, które mają być gromadzone ([249]).

([241]) Sekcja 2 lit. b) pkt (ii) rozporządzenia wykonawczego 14086.
([242]) Sekcja 102A ustawy o bezpieczeństwie narodowym i sekcja 2 lit. b) pkt (iii) rozporządzenia wykonawczego 14086.
([243]) W wyjątkowych przypadkach (w szczególności wówczas, gdy nie można przeprowadzić takiego procesu ze względu na konieczność zaspokojenia nowego lub nowo powstającego wymagania rozpoznawczego) takie priorytety może ustalić bezpośrednio Prezydent lub szef jednej z jednostek Wspólnoty Wywiadowczej, którzy co do zasady muszą zastosować takie same kryteria jak te opisane w sekcji 2 lit. b) pkt (iii) ppkt A części 1–3, zob. sekcja 4 lit. n) rozporządzenia wykonawczego 14086.
([244]) Sekcja 2 lit. b) pkt (iii) ppkt C rozporządzenia wykonawczego 14086.
([245]) Sekcja 2 lit. b) i c) pkt (i) ppkt A rozporządzenia wykonawczego 14086.
([246]) Sekcja 2 lit. c) pkt (i) ppkt A rozporządzenia wykonawczego 14086.
([247]) Sekcja 2 lit. c) pkt (i) ppkt A rozporządzenia wykonawczego 14086.
([248]) Sekcja 2 lit. c) pkt (i) ppkt B rozporządzenia wykonawczego 14086.
([249]) Sekcja 2 lit. c) pkt (i) ppkt B rozporządzenia wykonawczego 14086.

(140) Jeżeli chodzi o rodzaj gromadzenia danych w wyniku rozpoznania radioelektronicznego, gromadzenie danych w Stanach Zjednoczonych, które jest najistotniejsze z punktu widzenia obecnego stwierdzania odpowiedniego stopnia ochrony, ponieważ dotyczy danych, które zostały przekazane podmiotom w Stanach Zjednoczonych, powinno być zawsze ukierunkowane, jak wyjaśniono bardziej szczegółowo w motywach 142–153.

(141) „Hurtowe gromadzenie danych" ([250]) można przeprowadzić wyłącznie poza Stanami Zjednoczonymi na podstawie rozporządzenia wykonawczego 12333. Również w tym przypadku, zgodnie z rozporządzeniem wykonawczym 14086, należy nadać priorytet ukierunkowanemu gromadzeniu danych ([251]). Z kolei hurtowe gromadzenie danych jest dozwolone wyłącznie w sytuacji, w której nie można w racjonalny sposób uzyskać informacji niezbędnych do realizacji zatwierdzonego priorytetu wywiadowczego w drodze gromadzenia ukierunkowanego ([252]). Jeżeli konieczne jest przeprowadzenie hurtowego gromadzenia danych poza Stanami Zjednoczonymi, zastosowanie mają szczególne zabezpieczenia określone w rozporządzeniu wykonawczym 14086 ([253]). Po pierwsze, należy stosować metody i środki techniczne w celu ograniczenia gromadzonych danych wyłącznie do tego, co jest niezbędne do realizacji zatwierdzonego priorytetu wywiadowczego, przy jednoczesnym ograniczeniu do minimum gromadzenia informacji nieistotnych ([254]). Po drugie, w rozporządzeniu wykonawczym ogranicza się wykorzystywanie informacji zgromadzonych hurtowo (w tym w drodze zapytań) do sześciu celów szczegółowych, w tym celów dotyczących ochrony przed terroryzmem, brania zakładników oraz przetrzymywania w niewoli osób przez rząd innego państwa, podmiot lub osobę z innego państwa bądź w ich imieniu; ochrony przed szpiegostwem, sabotażem lub zamachem na rzecz obcego państwa; ochrony przed zagrożeniami wynikającymi z opracowywania, posiadania lub rozprzestrzeniania broni masowego rażenia lub powiązanych technologii i zagrożeń itp. ([255]) Ponadto wszelkie zapytania dotyczące danych zgromadzonych hurtowo w ramach rozpoznania radioelektronicznego mogą mieć miejsce, w stosownych przypadkach, wyłącznie w celu realizacji zatwierdzonego priorytetu wywiadowczego – z myślą o realizacji wspomnianych sześciu celów oraz zgodnie ze strategiami politycznymi i procedurami, w których odpowiednio uwzględniono wpływ tych zapytań na prywatność i wolności obywatelskie wszystkich osób, niezależnie od ich narodowości lub miejsca zamieszkania ([256]).

(142) Gromadzenie w wyniku rozpoznania radioelektronicznego danych, które zostały przekazane podmiotowi w Stanach Zjednoczonych, podlega nie tylko wymogom określonym w rozporządzeniu wykonawczym 14086, lecz także konkretnym ograniczeniom i zabezpieczeniom, które reguluje sekcja 702 ustawy o kontroli wywiadu ([257]). Zgodnie z przepisami sekcji 702 ustawy o kontroli wywiadu zezwala się na gromadzenie danych wywiadowczych poprzez ukierunkowywanie działań na osoby niebędące obywatelami ani rezydentami USA, w odniesieniu do których można racjonalnie założyć, że znajdują się one poza terytorium Stanów Zjednoczonych, przy obowiązkowej pomocy ze strony amerykańskich dostawców usług łączności elektronicznej ([258]). Na potrzeby gromadzenia danych

([250]) Tj. gromadzenie dużych ilości danych w ramach rozpoznania radioelektronicznego, które ze względów technicznych lub operacyjnych są pozyskiwane bez zastosowania wyróżników (na przykład bez użycia konkretnych identyfikatorów lub terminów umożliwiających selekcję), zob. sekcja 4 lit. b) rozporządzenia wykonawczego 14086. Zgodnie z rozporządzeniem wykonawczym 14086 i jak wyjaśniono dokładniej w motywie 141, hurtowe gromadzenie danych na podstawie rozporządzenia wykonawczego 12333 odbywa się wyłącznie w przypadku, gdy jest ono niezbędne do realizacji konkretnych zatwierdzonych priorytetów wywiadowczych, i podlega szeregowi ograniczeń i zabezpieczeń, które opracowano w celu uniemożliwienia powszechnego dostępu do danych. Hurtowe gromadzenie danych należy więc zestawić z gromadzeniem na zasadzie ogólnej i powszechnej („masowa inwigilacja") bez ograniczeń i zabezpieczeń.

([251]) Sekcja 2 lit. c) pkt (ii) ppkt A rozporządzenia wykonawczego 14086.

([252]) Sekcja 2 lit. c) pkt (ii) ppkt A rozporządzenia wykonawczego 14086.

([253]) Przepisy szczególne dotyczące hurtowego gromadzenia danych zawarte w rozporządzeniu wykonawczym 14086 mają również zastosowanie do ukierunkowanego gromadzenia danych w wyniku rozpoznania radioelektronicznego, w ramach którego tymczasowo wykorzystuje się dane uzyskane bez zastosowania wyróżników (np. konkretnych terminów umożliwiających selekcję lub identyfikatorów), tj. luzem (co jest możliwe jedynie poza terytorium Stanów Zjednoczonych). Nie ma to miejsca w przypadku, gdy takie dane są wykorzystywane wyłącznie do wspomagania początkowej fazy technicznej ukierunkowanego gromadzenia danych w wyniku rozpoznania radioelektronicznego, przechowywane jedynie przez krótki okres niezbędny do zakończenia tej fazy, a następnie natychmiast usuwane (sekcja 2 lit. c) pkt (ii) ppkt (D) rozporządzenia wykonawczego 14086). W tym przypadku jedynym celem wstępnego gromadzenia danych bez zastosowania wyróżników jest umożliwienie ukierunkowanego gromadzenia informacji poprzez zastosowanie konkretnego identyfikatora lub terminu umożliwiającego selekcję. W takim scenariuszu wyłącznie dane, które odzwierciedlają zastosowanie określonego wyróżnika, są wprowadzane do rządowych baz danych, podczas gdy pozostałe dane są niszczone. W związku z tym takie ukierunkowane gromadzenie danych nadal regulują przepisy ogólne, które mają zastosowanie do gromadzenia danych w wyniku rozpoznania radioelektronicznego, w tym przepisy zawarte w sekcji 2 lit. a)–b) i sekcji 2 lit. c) pkt (i) rozporządzenia wykonawczego 14086.

([254]) Sekcja 2 lit. c) pkt (ii) ppkt A rozporządzenia wykonawczego 14086.

([255]) Sekcja 2 lit. c) pkt (ii) ppkt B rozporządzenia wykonawczego 14086. W przypadku zaistnienia nowych okoliczności związanych z bezpieczeństwem narodowym, takich jak nowe zagrożenia dla bezpieczeństwa narodowego, Prezydent może zaktualizować ten wykaz. Takie aktualizacje muszą co do zasady zostać podane do wiadomości publicznej, chyba że Prezydent uzna, że takie działanie może samo w sobie stworzyć zagrożenie dla bezpieczeństwa narodowego Stanów Zjednoczonych (sekcja 2 lit. c) pkt (ii) ppkt C rozporządzenia wykonawczego 14086). W odniesieniu do zapytań dotyczących danych zgromadzonych hurtowo zob. sekcja 2 lit. c) pkt (iii) ppkt D rozporządzenia wykonawczego 14086.

([256]) Sekcja 2 lit. a) pkt (ii) ppkt A w związku z sekcją 2 lit. c) pkt (iii) ppkt D rozporządzenia wykonawczego 14086. Zob. również załącznik VII.

([257]) Tytuł 50 § 1881 U.S.C.

([258]) Tytuł 50 § 1881a lit. a) U.S.C. W szczególności, jak zauważyła PCLOB, sekcja 702 ustawy o kontroli wywiadu „w całości polega na ukierunkowywaniu działań na określone osoby [niebędące obywatelami ani rezydentami USA], w odniesieniu do których przeprowadzono zindywidualizowane rozpoznanie" (sprawozdanie Rady Nadzoru nad Ochroną Danych i Wolnościami Obywatelskimi w sprawie programu nadzoru realizowanego na podstawie sekcji 702 ustawy o kontroli wywiadu, 2 lipca 2014 r., sprawozdanie dotyczące sekcji 702 ustawy o kontroli wywiadu, s. 111). Zob. również Biuro Wolności Obywatelskich i Ochrony Prywatności w ramach Agencji Bezpieczeństwa Narodowego, Wdrażanie sekcji 702 ustawy o kontroli wywiadu przez Agencję Bezpieczeństwa Narodowego (NSA's Implementation of Foreign Intelligence Act Section 702) z dnia 16 kwietnia 2014 r. Termin „dostawca usług łączności elektronicznej" zdefiniowano w tytule 50 § 1881 lit. a) pkt 4 U.S.C.

wywiadowczych zgodnie z sekcją 702 ustawy o kontroli wywiadu prokurator generalny i Dyrektor Krajowych Służb Wywiadowczych przedkładają coroczne certyfikacje do Sądu ds. Kontroli Wywiadu, który określa kategorie danych wywiadowczych, które należy pozyskać ([259]). Certyfikacjom muszą towarzyszyć procedury ukierunkowywania, minimalizacji i zapytań, które są również zatwierdzane przez sąd i prawnie wiążące dla amerykańskich agencji wywiadowczych.

(143) Sąd ds. Kontroli Wywiadu jest niezależnym sądem ([260]) utworzonym na mocy ustawy federalnej, którego orzeczenia można zaskarżyć przed Sądem Odwoławczym ds. Kontroli Wywiadu ([261]), a ostatecznie przed Sądem Najwyższym Stanów Zjednoczonych ([262]). Sąd ds. Kontroli Wywiadu (oraz Sąd Odwoławczy ds. Kontroli Wywiadu) korzysta ze wsparcia stałego zespołu składającego się z pięciu adwokatów i pięciu ekspertów technicznych w dziedzinie bezpieczeństwa narodowego i wolności obywatelskich ([263]). Spośród tej grupy sąd powołuje jedną osobę, która będzie pełniła funkcję *amicus curiae*, tj. osoby zapewniającej wsparcie przy rozpatrywaniu wszelkich wniosków o wydanie nakazu lub wniosków o dokonanie przeglądu zawierających nową lub istotną wykładnię przepisów ustawowych, chyba że sąd stwierdzi, że powołanie takiej osoby w danym przypadku nie byłoby właściwe ([264]). Instytucja *amicus curiae* służy przede wszystkim zapewnieniu odpowiedniego uwzględnienia w ocenie przeprowadzonej przez sąd kwestii związanych z prywatnością. Sąd może również powołać osobę fizyczną lub podmiot do pełnienia funkcji *amicus curiae* i dzielenia się swoją wiedzą techniczną, jeżeli uzna to za stosowne lub – po otrzymaniu odpowiedniego wniosku – może udzielić osobie fizycznej lub podmiotowi zgody na złożenie raportu *amicus curiae* ([265]).

(144) Sąd ds. Kontroli Wywiadu dokonuje przeglądów certyfikacji i powiązanych procedur (w szczególności procedur ukierunkowywania i minimalizacji) pod względem zgodności z wymogami określonymi w ustawie o kontroli wywiadu. Jeżeli sąd ten stwierdzi, że wymogi nie zostały spełnione, może odmówić wydania certyfikatu w całości lub w części i zażądać zmiany procedur ([266]). W tym kontekście Sąd ds. Kontroli Wywiadu wielokrotnie podkreślał, że jego przegląd procedur ukierunkowywania i minimalizacji określonych w sekcji 702 nie ogranicza się wyłącznie do samych tych procedur, lecz także obejmuje sposób ich wdrażania przez rząd ([267]).

(145) Agencja Bezpieczeństwa Narodowego (agencja wywiadowcza odpowiedzialna za ukierunkowywanie, o którym mowa w sekcji 702 ustawy o kontroli wywiadu) dokonuje indywidualnych ustaleń w zakresie ukierunkowywania zgodnie z procedurami ukierunkowywania zatwierdzonymi przez Sąd ds. Kontroli Wywiadu, które nakładają na Agencję Bezpieczeństwa Narodowego obowiązek dokonania oceny, w oparciu o całokształt okoliczności, że przez ukierunkowanie działań na konkretną osobę można pozyskać dane wywiadowcze należące do kategorii wskazanej w certyfikacji ([268]). Ocena ta musi być szczegółowa i oparta na faktach, jak również musi opierać się na osądzie ana-

([259]) Tytuł 50 § 1881a lit. g) U.S.C.

([260]) W Sądzie ds. Kontroli Wywiadu zasiadają sędziowie powołani przez Prezesa Sądu Najwyższego Stanów Zjednoczonych spośród sędziów amerykańskich sądów dystryktowych, którzy zostali wcześniej mianowani przez Prezydenta za zgodą Senatu. Sędziowie, którzy sprawują swój urząd dożywotnio i mogą zostać odwołani wyłącznie z uzasadnionego powodu, orzekają w Sądzie ds. Kontroli Wywiadu w ramach siedmioletnich kadencji rozpoczynających się w różnych terminach. Zgodnie z wymogami ustawy o kontroli wywiadu sędziowie muszą zostać dobrani z co najmniej siedmiu różnych okręgów sądowych w Stanach Zjednoczonych. Zob. tytuł 50 § 1803 lit. a) U.S.C. Sędziowie korzystają ze wsparcia doświadczonych urzędników sądowych, którzy pełnią funkcję pracowników merytorycznych w sądach odpowiedzialnych za przygotowywanie analiz prawnych w odniesieniu do wniosków o wydanie zgody na gromadzenie informacji. Zob. pismo sędziego Reggiego B. Waltona, przewodniczącego składu sędziowskiego w Sądzie Stanów Zjednoczonych ds. Kontroli Wywiadu, do senatora Patricka J. Leathy'ego, przewodniczącego Komisji Sądownictwa w Senacie Stanów Zjednoczonych (z dnia 29 lipca 2013 r.) („pismo Waltona"), s. 2, dostępne pod adresem https://fas.org/irp/news/2013/07/fisc-leahy.pdf

([261]) W Sądzie Odwoławczym ds. Kontroli Wywiadu zasiadają sędziowie powołani przez prezesa Sądu Najwyższego Stanów Zjednoczonych, pochodzący z amerykańskich sądów dystryktowych lub sądów apelacyjnych, którzy sprawują swój urząd w ramach naprzemiennych siedmioletnich kadencji. Zob. tytuł 50 § 1803 lit. b) U.S.C.

([262]) Zob. tytuł 50 § 1803 lit. b), § 1861a lit. f), § 1881a lit. h), § 1881a lit. i) pkt 4 U.S.C.

([263]) Tytuł 50 § 1803 lit. i) pkt 1 i tytuł 50 § 1803 lit. i) pkt 3 ppkt A U.S.C.

([264]) Tytuł 50 § 1803 lit. i) pkt 2 ppkt A U.S.C.

([265]) Tytuł 50 § 1803 lit. i) pkt 2 ppkt B U.S.C.

([266]) Zob. np. opinia Sądu ds. Kontroli Wywiadu z dnia 18 października 2018 r. dostępna pod adresem https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, którą to opinię potwierdził Sąd Odwoławczy ds. Kontroli Wywiadu w swojej opinii z dnia 12 lipca 2019 r., która jest dostępna pod adresem https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf .

([267]) Zob. na przykład Sąd ds. Kontroli Wywiadu, opinia i zarządzenie w sprawie memorandum, s. 35 (18 listopada 2020 r.) (zatwierdzone do podania do wiadomości publicznej w dniu 26 kwietnia 2021 r.), (załącznik D).

([268]) Tytuł 50 § 1881a lit. a) U.S.C., Procedury wykorzystywane przez Agencję Bezpieczeństwa Narodowego do celów ukierunkowywania działań na osoby niebędące obywatelami ani rezydentami Stanów Zjednoczonych, co do których istnieje uzasadnione podejrzenie, że przebywają poza terytorium Stanów Zjednoczonych w celu pozyskiwania danych wywiadowczych zgodnie z sekcją 702 ustawy o kontroli wywiadu z 1978 r., z późniejszymi zmianami, z marca 2018 r. (Procedury Agencji Bezpieczeństwa Narodowego w zakresie ukierunkowania), dokument dostępny pod adresem https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, s. 1–4, wyjaśniony bardziej szczegółowo w sprawozdaniu PCLOB, s. 41–42.

litycznym, specjalistycznym szkoleniu i doświadczeniu analityka oraz na charakterze danych wywiadowczych, które mają zostać pozyskane ([269]). Ukierunkowanie przeprowadza się przez określenie tak zwanych selektorów, które pozwalają określić konkretne narzędzia komunikacyjne, takie jak adres e-mail lub numer telefonu osoby, na którą ukierunkowano działania, lecz nigdy kluczowe słowa ani imiona i nazwiska osób fizycznych ([270]).

(146) Analitycy Agencji Bezpieczeństwa Narodowego identyfikują najpierw osoby niebędące obywatelami ani rezydentami USA przebywające za granicą, których objęcie nadzorem – w ocenie analityków – umożliwi pozyskanie stosownych zagranicznych informacji wywiadowczych określonych w certyfikacji ([271]). Jak określono w procedurach Agencji Bezpieczeństwa Narodowego w zakresie ukierunkowywania, Agencja Bezpieczeństwa Narodowego może objąć nadzorem osobę, na którą ukierunkowano działania, wyłącznie pod warunkiem, że ma już pewne informacje na jej temat ([272]). Informacje te mogą pochodzić z danych uzyskanych z różnych źródeł, na przykład z wywiadu osobowego. Za pośrednictwem tych innych źródeł analityk musi również zidentyfikować konkretny selektor (tj. konto komunikacyjne) wykorzystywany przez osobę, która może być potencjalnym celem namierzania. Po zidentyfikowaniu tych poszczególnych osób i zatwierdzeniu ukierunkowywania na nie działań w ramach rozbudowanego mechanizmu przeglądu wykorzystywanego przez Agencję Bezpieczeństwa Narodowego ([273]) przydziela się (tj. opracowuje i wdraża) selektory identyfikujące narzędzia komunikacyjne (takie jak adresy e-mail), które są wykorzystywane przez osoby, na które ukierunkowano działania ([274]).

(147) Agencja Bezpieczeństwa Narodowego musi udokumentować faktyczną podstawę wyboru osoby, na którą ukierunkowano działania, ([275]) i w regularnych odstępach po wstępnym ukierunkowaniu działań na tę osobę musi potwierdzić, że norma w zakresie ukierunkowania jest cały czas spełniana ([276]). Jeżeli norma ta nie jest już spełniana, należy zaprzestać gromadzenia informacji ([277]). Urzędnicy biur ds. nadzoru nad służbami wywiadowczymi w Departamencie Sprawiedliwości, którzy mają obowiązek zgłaszać wszelkie naruszenia Sądowi ds. Kontroli Wywiadu i Kongresowi, co dwa miesiące dokonują przeglądu wyboru każdej osoby, na którą Agencja Bezpieczeństwa Narodowego ukierunkowała działania, oraz jej dokumentacji dotyczącej każdej zarejestrowanej oceny i uzasadnienia ukierunkowania w celu zapewnienia zgodności z procedurami ukierunkowywania ([278]). Dokumentacja pisemna Agencji Bezpieczeństwa Narodowego ułatwia Sądowi ds. Kontroli Wywiadu nadzorowanie tego, czy konkretne osoby fizyczne są prawidłowo namierzane na podstawie sekcji 702 ustawy o kontroli wywiadu, zgodnie z jego uprawnieniami nadzorczymi opisanymi w motywach 173–174 ([279]). Ponadto Dyrektor Krajowych Służb Wywiadowczych jest również zobowiązany do podawania co roku całkowitej liczby namierzanych osób zgodnie z sekcją 702 ustawy o kontroli wywiadu w publicznych, składanych do roku statystycznych sprawozdaniach z przejrzystości. Przedsiębiorstwa, które otrzymują dyrektywy na podstawie sekcji 702 ustawy o kontroli wywiadu, mogą publikować dane zagregowane (za pośrednictwem sprawozdań z przejrzystości) dotyczące otrzymywanych wniosków ([280]).

([269]) Procedury Agencji Bezpieczeństwa Narodowego w zakresie ukierunkowywania, s. 4.

([270]) Zob. sprawozdanie PCLOB dotyczące sekcji 702, s. 32–33, 45 z dalszymi odniesieniami. Zob. również półroczna ocena zgodności z procedurami i wytycznymi w oparciu o sekcję 702 ustawy o kontroli wywiadu złożona przez prokuratora generalnego i Dyrektora Krajowych Służb Wywiadowczych, okres sprawozdawczy: 1 grudnia 2016 r. – 31 maja 2017 r., s. 41 (październik 2018 r.); ocena dostępna pod adresem: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf

([271]) Zob. sprawozdanie PCLOB dotyczące sekcji 702, s. 42–43.

([272]) Procedury Agencji Bezpieczeństwa Narodowego w zakresie ukierunkowywania, s. 2.

([273]) Zob. sprawozdanie PCLOB dotyczące sekcji 702, s. 46. Na przykład Agencja Bezpieczeństwa Narodowego musi sprawdzić, czy istnieje związek między docelową osobą a selektorem, musi udokumentować dane wywiadowcze, które mają zostać pozyskane, dane te muszą zostać poddane przeglądowi i zatwierdzone przez dwóch starszych rangą analityków Agencji Bezpieczeństwa Narodowego, a cały proces będzie śledzony na potrzeby kolejnych przeglądów zgodności przez Urząd Dyrektora Krajowych Służb Wywiadowczych i Departament Sprawiedliwości. Zob. Biuro Wolności Obywatelskich i Ochrony Prywatności w ramach Agencji Bezpieczeństwa Narodowego, Wdrażanie sekcji 702 ustawy o kontroli wywiadu przez Agencję Bezpieczeństwa Narodowego (NSA's Implementation of Foreign Intelligence Act Section 702) z dnia 16 kwietnia 2014 r.

([274]) Tytuł 50 § 1881a lit. h) U.S.C.

([275]) Procedury Agencji Bezpieczeństwa Narodowego w zakresie ukierunkowywania, s. 8. Zob. również sprawozdanie PCLOB dotyczące sekcji 702, s. 46. Nieprzedstawienie pisemnego uzasadnienia stanowi przypadek braku zgodności z dokumentacją, który musi zostać zgłoszony Sądowi ds. Kontroli Wywiadu i Kongresowi. Zob. półroczna ocena zgodności z procedurami i wytycznymi w oparciu o sekcję 702 ustawy o kontroli wywiadu złożona przez prokuratora generalnego i Dyrektora Krajowych Służb Wywiadowczych, okres sprawozdawczy: 1 grudnia 2016 r. – 31 maja 2017 r., s. 41 (październik 2018 r.), sprawozdanie DoJ/Urzędu Dyrektora Krajowych Służb Wywiadowczych dotyczące przestrzegania zasad złożone Sądowi ds. Kontroli Wywiadu za okres od grudnia 2016 r. do maja 2017 r., s. A-6; dokument dostępny pod adresem: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf

([276]) Zob. dokument przedłożony przez rząd Stanów Zjednoczonych Sądowi ds. Kontroli Wywiadu, „2015 Summary of Notable Section 702 Requirements" („Podsumowanie najważniejszych wymogów określonych w sekcji 702, 2015 r."), s. 2–3 (15 lipca 2015 r.), oraz informacje przedstawione w załączniku VII.

([277]) Zob. dokument przedłożony przez rząd Stanów Zjednoczonych Sądowi ds. Kontroli Wywiadu, „2015 Summary of Notable Section 702 Requirements" („Podsumowanie najważniejszych wymogów określonych w sekcji 702, 2015 r."), s. 2–3 (15 lipca 2015 r.), w którym określono, że „jeżeli rząd oceni później, że dalszy przydział selektora namierzanej osoby prawdopodobnie nie doprowadzi do pozyskania danych wywiadowczych, konieczne będzie jego niezwłoczne zaniechanie, a opóźnienie tej czynności może prowadzić do wystąpienia przypadku braku zgodności, który wymaga zgłoszenia". Zob. również informacje przedstawione w załączniku VII.

([278]) Zob. sprawozdanie PCLOB dotyczące sekcji 702, s. 70–72; zasada 13 lit. b) regulaminu amerykańskiego Sądu ds. Kontroli Wywiadu, dokument dostępny pod adresem https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf

([279]) Zob. również sprawozdanie DoJ/Urzędu Dyrektora Krajowych Służb Wywiadowczych dotyczące zgodności złożone Sądowi ds. Kontroli Wywiadu za okres od grudnia 2016 r. do maja 2017 r., s. A-6.

([280]) Tytuł 50 § 1874 U.S.C.

(148) W odniesieniu do pozostałych podstaw prawnych gromadzenia danych osobowych przekazywanych podmiotom w Stanach Zjednoczonych zastosowanie mają różne ograniczenia i zabezpieczenia. Ogólnie rzecz biorąc, szczególnie zabrania się hurtowego gromadzenia danych na podstawie sekcji 402 ustawy o kontroli wywiadu (podstawa prawna do stosowania urządzeń rejestrujących wybierane numery oraz urządzeń śledzących) oraz poprzez korzystanie z wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego, a zamiast tego wymaga się stosowania konkretnych „terminów umożliwiających selekcję" ([281]).

(149) Na potrzeby prowadzenia tradycyjnego zindywidualizowanego dozoru elektronicznego (zgodnie z sekcją 105 ustawy o kontroli wywiadu) agencje wywiadowcze muszą złożyć do Sądu ds. Kontroli Wywiadu wniosek z przedstawieniem stanu faktycznego i okoliczności, na które powołały się, aby uzasadnić swoje przekonanie, że dany obiekt jest użytkowany lub wkrótce będzie użytkowany przez obce państwo lub przez agenta obcego państwa ([282]). Sąd ds. Kontroli Wywiadu oceni m.in., czy na podstawie przedstawionych faktów istnieje uzasadnione podejrzenie, że dane zdarzenie faktycznie miało miejsce ([283]).

(150) W celu przeprowadzenia przeszukania lokalu lub mienia, które ma doprowadzić do inspekcji, zajęcia itp. informacji, materiałów lub mienia (np. urządzenia komputerowego) na podstawie sekcji 301 ustawy o kontroli wywiadu, wymagane jest złożenie wniosku o wydanie nakazu do Sądu ds. Kontroli Wywiadu ([284]). W takim wniosku należy wykazać między innymi, że istnieje uzasadnione podejrzenie, że celem przeszukania jest obce państwo lub agent obcego państwa, że lokal lub mienie, które mają zostać przeszukane, można wykorzystać do pozyskania danych wywiadowczych oraz że lokal, który ma zostać przeszukany, jest własnością (agenta) obcego państwa, jest użytkowany przez obce państwo (lub jego agenta), znajduje się w posiadaniu obcego państwa (lub jego agenta) lub jest przekazywany na rzecz (agenta) obcego państwa lub przez niego ([285]).

(151) Podobnie instalacja urządzeń rejestrujących wybierane numery lub urządzeń śledzących (zgodnie z sekcją 402 ustawy o kontroli wywiadu) wymaga złożenia wniosku o wydanie nakazu do Sądu ds. Kontroli Wywiadu (lub amerykańskiego sędziego pokoju) i zastosowanie konkretnego terminu umożliwiającego selekcję, tj. terminu, który w konkretny sposób identyfikuje daną osobę, konto itd. i jest stosowany w celu ograniczenia w jak największym stopniu zakresu żądanych informacji ([286]). Ta podstawa prawna odnosi się nie do treści komunikatów, lecz raczej dotyczy informacji na temat klienta lub abonenta korzystającego z usługi (takich jak imię i nazwisko, adres, numer abonenta, okres/rodzaj otrzymywanej usługi, źródło/mechanizm płatności).

(152) W sekcji 501 ([287]) ustawy o kontroli wywiadu, która dopuszcza możliwość gromadzenia rejestrów związanych z prowadzoną działalnością wspólnego przewoźnika (tj. dowolnej osoby lub dowolnego podmiotu przewożących ludzi lub składniki majątku drogą lądową, kolejową, wodną lub powietrzną za wynagrodzeniem), publicznego obiektu noclegowego (np. hotelu, motelu lub zajazdu), wypożyczalni pojazdów lub punktu fizycznego składowania (tj. w którym udostępnia się przestrzeń lub świadczy usługi związane z przechowywaniem towarów i materiałów) ([288]), również wymaga się złożenia wniosku do Sądu ds. Kontroli Wywiadu lub sędziego pokoju. We wniosku tym należy wskazać rejestry, o które się wnosi, oraz konkretne i jasne fakty dające podstawy, by sądzić, że osoba, której rejestry dotyczą, działa na korzyść obcego państwa lub jest jego agentem ([289]).

(153) Wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego są ponadto dozwolone na mocy różnych ustaw i umożliwiają agencjom dochodzeniowo-śledczym uzyskanie określonych informacji (nieobejmujących treści komunikacji) od niektórych podmiotów (np. instytucji finansowych, biur informacji kredytowej, dostawców usług łączności elektronicznej) zawartych w sprawozdaniach kredytowych, dokumentacji finansowej i dokumentacji abonenta elektronicznego i dokumentacji dotyczącej transakcji ([290]). W ustawie dotyczącej wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego, która zezwala na dostęp do łączności elektronicznej i która może być wykorzystywana wyłącznie przez FBI, ustanowiono wymóg opatrzenia każdego wniosku elementem umożliwiającym bezpośrednią identyfikację danej osoby, podmiotu, numeru telefonicznego lub rachunku oraz poświadczenia, że informacje te są istotne w kontekście zatwierdzonego dochodzenia dotyczącego bezpieczeństwa narodowego w celu zapewnienia ochrony przed terroryzmem międzynarodowym lub tajnymi działaniami wywiadowczymi ([291]). Odbiorcy wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego mają prawo zakwestionować je przed sądem ([292]).

([281]) Tytuł 50 § 1842 lit. c) pkt 3 U.S.C. oraz, w odniesieniu do wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego, tytuł 12 § 3414 lit. a) pkt 2 U.S.C.; tytuł 15 § 1681u U.S.C.; tytuł 15 § 1681v lit. a) U.S.C. oraz tytuł 18 § 2709 lit. a) U.S.C.

([282]) Termin „agent obcego państwa" może obejmować osoby niebędące obywatelami ani rezydentami USA, które są zaangażowane w międzynarodowy terroryzm lub w rozprzestrzenianie broni masowego rażenia na szczeblu międzynarodowym (uwzględniając czynności przygotowawcze) (tytuł 50 § 1801 lit. b) pkt 1 U.S.C.).

([283]) Tytuł 50 § 1804 U.S.C. Zob. również § 1841 ust. 4 w odniesieniu do wyboru terminów umożliwiających selekcję.

([284]) Tytuł 50 §§ 1821 ust. 5 U.S.C.

([285]) Tytuł 50 § 1823 lit. a) U.S.C.

([286]) Tytuł 50 § 1842 i § 1841 ust. 2 oraz tytuł 18 sekcja 3127 U.S.C.

([287]) Tytuł 50 § 1862 U.S.C.

([288]) Tytuł 50 §§ 1861–1862 U.S.C.

([289]) Tytuł 50 § 1862 lit. b) U.S.C.

([290]) Tytuł 12 § 3414 U.S.C.; tytuł 15 §§ 1681u–1681v U.S.C. oraz tytuł 18 § 2709 U.S.C.

([291]) Tytuł 18 § 2709 lit. b) U.S.C.

([292]) Np. tytuł 18 § 2709 lit. d) U.S.C.

3.2.1.3. *Dalsze wykorzystywanie zebranych informacji*

(154) Przetwarzanie danych osobowych zgromadzonych przez amerykańskie agencje wywiadowcze za pośrednictwem rozpoznania radioelektronicznego podlega licznym zabezpieczeniom.

(155) Po pierwsze, każda agencja wywiadowcza musi zapewnić odpowiednie bezpieczeństwo danych i uniemożliwić osobom nieupoważnionym dostęp do danych osobowych zgromadzonych za pośrednictwem rozpoznania radioelektronicznego. W tym względzie w różnych instrumentach, takich jak ustawy, wytyczne i normy, dodatkowo określono minimalne wymogi w zakresie bezpieczeństwa informacji, które należy wprowadzić (np. uwierzytelnianie wieloskładnikowe, szyfrowanie itp.) ([293]). Dostęp do gromadzonych danych musi być ograniczony do upoważnionych i przeszkolonych pracowników, którzy potrzebują danych, aby wywiązywać się ze swoich obowiązków ([294]). Co do zasady agencje wywiadowcze muszą zapewnić swoim pracownikom odpowiednie szkolenia, w tym szkolenia w zakresie procedur zgłaszania naruszeń prawa i reagowania na nie (w tym w zakresie rozporządzenia wykonawczego 14086) ([295]).

(156) Po drugie, agencje wywiadowcze muszą przestrzegać standardów Wspólnoty Wywiadowczej w zakresie prawidłowości i obiektywności, w szczególności w odniesieniu do zapewnienia jakości i wiarygodności danych, uwzględniania alternatywnych źródeł informacji i obiektywności w przeprowadzaniu analiz ([296]).

(157) Po trzecie, w odniesieniu do przechowywania danych, w rozporządzeniu wykonawczym 14086 wyjaśniono, że dane osobowe osób niebędących obywatelami ani rezydentami USA podlegają okresom przechowywania takim samym jak te, które mają zastosowanie do danych obywateli i rezydentów USA ([297]). Agencje wywiadowcze są zobowiązane do określenia konkretnych okresów przechowywania danych lub czynników, które należy wziąć pod uwagę przy określaniu długości mających zastosowanie okresów przechowywania danych (np. czy informacje stanowią dowód popełnienia przestępstwa; czy informacje są danymi wywiadowczymi; czy informacje te są potrzebne do ochrony bezpieczeństwa osób lub organizacji, w tym ofiar lub celów międzynarodowego terroryzmu, określonych w różnych instrumentach prawnych ([298]).

(158) Po czwarte, w odniesieniu do rozpowszechniania danych osobowych zgromadzonych za pośrednictwem rozpoznania radioelektronicznego zastosowanie mają przepisy szczególne. Zgodnie z ogólnym wymogiem dane osobowe osób niebędących obywatelami ani rezydentami USA mogą być rozpowszechniane tylko wtedy, gdy dotyczą tego samego rodzaju informacji, które mogą być rozpowszechniane na temat obywateli i rezydentów USA, np. informacji potrzebnych do ochrony bezpieczeństwa osoby lub podmiotu (takich jak cele, ofiary lub zakładnicy międzynarodowych organizacji terrorystycznych) ([299]). Dane osobowe nie mogą być ponadto rozpowszechniane wyłącznie ze względu na obywatelstwo lub kraj zamieszkania danej osoby lub w celu obejścia wymogów rozporządzenia wykonawczego 14086 ([300]). Rozpowszechnianie danych w rządzie USA może mieć miejsce wyłącznie wówczas, gdy upo-

([293]) Sekcja 2 lit. c) pkt (iii) ppkt B pppkt 1 rozporządzenia wykonawczego 14086. Zob. także tytuł VIII ustawy o bezpieczeństwie narodowym (określający szczegółowo wymogi dotyczące dostępu do informacji niejawnych), rozporządzenie wykonawcze 12333, sekcja 1.5 (w której zobowiązuje się szefów agencji Wspólnoty Wywiadowczej do przestrzegania wytycznych dotyczących udostępniania i bezpieczeństwa informacji, prywatności informacji i innych wymogów prawnych), dyrektywa nr 42 dotycząca bezpieczeństwa narodowego, „krajowa polityka zabezpieczenia krajowych systemów telekomunikacyjnych i informacyjnych odpowiedzialnych za bezpieczeństwo narodowe" („National Policy for the Security of National Security Telecommunications and Information Systems") (w której nakazuje się Komitetowi ds. Systemów Bezpieczeństwa Narodowego przekazanie departamentom i agencjom wykonawczym wytycznych dotyczących bezpieczeństwa systemów bezpieczeństwa narodowego) oraz memorandum w sprawie bezpieczeństwa narodowego nr 8 „Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems" [„Poprawa cyberbezpieczeństwa systemów bezpieczeństwa narodowego, Departamentu Obrony i Wspólnoty Wywiadowczej"] (w którym ustanawia się terminy i wytyczne dotyczące sposobu wdrażania wymogów cyberbezpieczeństwa w odniesieniu do krajowych systemów bezpieczeństwa, w tym uwierzytelniania wieloskładnikowego, szyfrowania, technologii chmury i usług wykrywania zagrożeń na punktach końcowych).

([294]) Sekcja 2 lit. c) pkt (iii) ppkt B pppkt 2 rozporządzenia wykonawczego 14086. Ponadto dostęp do danych osobowych, w odniesieniu do których nie dokonano ostatecznego ustalenia dotyczącego zatrzymywania, można uzyskać wyłącznie w celu dokonania takiego ustalenia lub na jego poparcie lub w celu wykonywania dozwolonych funkcji administracyjnych, funkcji związanych z testowaniem, rozwojem, bezpieczeństwem lub funkcji nadzorczych (sekcja 2 lit. c) pkt (iii) ppkt B pppkt 3 rozporządzenia wykonawczego 14086).

([295]) Sekcja 2 lit. d) pkt (ii) rozporządzenia wykonawczego 14086.

([296]) Sekcja 2 lit. c) pkt (iii) ppkt C rozporządzenia wykonawczego 14086.

([297]) Sekcja 2 lit. c) pkt (iii) ppkt A pppkt 2 lit. a)–c) rozporządzenia wykonawczego 14086. Co do zasady każda agencja musi wdrożyć strategie polityczne i procedury mające na celu zminimalizowanie rozpowszechniania i zatrzymywania danych osobowych gromadzonych za pośrednictwem rozpoznania radioelektronicznego (sekcja 2 lit. c) pkt (iii) ppkt A rozporządzenia wykonawczego 14086).

([298]) Zob. np. sekcja 309 ustawy o zatwierdzeniu działań wywiadowczych na rok budżetowy 2015; procedury minimalizacji przyjęte przez poszczególne agencje wywiadowcze na podstawie sekcji 702 ustawy o kontroli wywiadu i zatwierdzone przez Sąd ds. Kontroli Wywiadu; procedury zatwierdzone przez Prokuratora Generalnego i zgodnie z ustawą o rejestrach federalnych (FRA) (wymagające od agencji federalnych Stanów Zjednoczonych, w tym agencji bezpieczeństwa narodowego, ustanowienia okresów przechowywania ich dokumentacji, które to okresy muszą zostać zatwierdzone przez Krajową Administrację Archiwów i Rejestrów).

([299]) Sekcja 2 lit. c) pkt (iii) ppkt A pppkt 1 lit. a) oraz sekcja 5 lit. d) rozporządzenia wykonawczego 14086 w związku z sekcją 2.3 rozporządzenia wykonawczego 12333.

([300]) Sekcja 2 lit. c) pkt (iii) ppkt A pppkt 1 lit. b) i e) rozporządzenia wykonawczego 14086.

ważniona i przeszkolona osoba ma uzasadnione przekonanie, że odbiorca musi znać te informacje ([301]) i będzie je odpowiednio chronił ([302]). Aby określić, czy dane osobowe mogą być rozpowszechniane odbiorcom spoza rządu amerykańskiego (w tym rządowi obcego państwa lub organizacji międzynarodowej), należy uwzględnić cel rozpowszechniania, charakter i zakres rozpowszechnianych danych oraz potencjalny szkodliwy wpływ na daną osobę lub dane osoby ([303]).

(159) Ponadto – w celu ułatwienia nadzoru nad spełnianiem obowiązujących wymogów prawnych oraz skutecznego dochodzenia roszczeń – każda agencja wywiadowcza jest zobowiązana na podstawie rozporządzenia wykonawczego 14086 do przechowywania odpowiedniej dokumentacji dotyczącej gromadzenia danych w ramach rozpoznania radioelektronicznego. Wymogi dotyczące dokumentacji obejmują elementy takie jak faktyczna podstawa oceny, że określone działanie związane z gromadzeniem danych jest niezbędne do realizacji zatwierdzonego priorytetu wywiadowczego ([304]).

(160) Oprócz wyżej wymienionych zabezpieczeń zawartych w rozporządzeniu wykonawczym 14086 dotyczących wykorzystywania informacji zgromadzonych w wyniku rozpoznania radioelektronicznego wszystkie agencje wywiadowcze Stanów Zjednoczonych podlegają bardziej ogólnym wymogom dotyczącym ograniczenia celu, minimalizacji danych, dokładności, bezpieczeństwa, przechowywania i rozpowszechniania, w szczególności na podstawie okólnika OMB nr A-130, ustawy o administracji elektronicznej, ustawy o rejestrach federalnych (zob. motywy 101–106) oraz wytycznych Komitetu ds. Systemów Bezpieczeństwa Narodowego (CNSS) ([305]).

3.2.2. ***Nadzór***

(161) Działalność amerykańskich agencji wywiadowczych podlega nadzorowi różnych organów.

(162) Po pierwsze, zgodnie z rozporządzeniem wykonawczym 14086 każda agencja wywiadowcza musi posiadać urzędników wysokiego szczebla ds. prawnych, nadzoru i zgodności, by zapewnić zgodność z mającym zastosowanie prawem amerykańskim ([306]). W szczególności muszą oni prowadzić okresowy nadzór nad działaniami w zakresie rozpoznania radioelektronicznego i zapewniać usuwanie wszelkich niezgodności. Agencje wywiadowcze muszą zapewnić takim urzędnikom dostęp do wszystkich istotnych informacji, by umożliwić im wykonywanie funkcji nadzorczych, i nie mogą podejmować żadnych działań utrudniających działania nadzorcze lub w sposób niewłaściwy wpływających na takie działania ([307]). Każdy przypadek istotnej niezgodności ([308]) stwierdzony przez urzędnika ds. nadzoru lub innego pracownika należy ponadto niezwłocznie zgłosić szefowi agencji wywiadowczej i Dyrektorowi Krajowych Służb Wywiadowczych, którzy muszą zapewnić podjęcie wszelkich niezbędnych działań, by zaradzić i zapobiec ponownemu wystąpieniu istotnej niezgodności ([309]).

(163) Tę funkcję nadzorczą pełnią urzędnicy, którym wyznaczono określone role w zakresie zgodności, jak również urzędnicy ds. prywatności i wolności obywatelskich oraz Inspektorzy Generalni ([310]).

([301]) Zob. np. AGG-DOM stanowi na przykład, że FBI może rozpowszechniać informacje tylko wtedy, gdy odbiorcy niezbędna jest ta wiedza, aby wypełniać jego misję lub chronić społeczeństwo.

([302]) Sekcja 2 lit. c) pkt (iii) ppkt A pppkt 1 lit. c) rozporządzenia wykonawczego 14086. Agencje wywiadowcze mogą na przykład rozpowszechniać informacje w okolicznościach istotnych dla postępowania przygotowawczego lub związanych z przestępstwem, w tym na przykład poprzez rozpowszechnianie ostrzeżeń o groźbach zabójstwa, poważnego uszczerbku na zdrowiu lub porwania; rozpowszechnianie informacji na temat reagowania na cyberzagrożenia, incydenty lub włamania; oraz powiadamianie ofiar lub ostrzeganie potencjalnych ofiar przestępstw.

([303]) Sekcja 2 lit. c) pkt (iii) ppkt A pppkt 1 lit. d) rozporządzenia wykonawczego 14086.

([304]) Sekcja 2 lit. c) pkt (iii) ppkt E rozporządzenia wykonawczego 14086.

([305]) Zob. polityka CNSS nr 22, polityka zarządzania ryzykiem w cyberbezpieczeństwie i instrukcja CNSS 1253, która zawiera szczegółowe wytyczne dotyczące środków bezpieczeństwa, które należy wdrożyć w odniesieniu do systemów bezpieczeństwa narodowego.

([306]) Sekcja 2 lit. d) pkt (i) ppkt A–B rozporządzenia wykonawczego 14086.

([307]) Sekcja 2 lit. d) pkt (i) ppkt B–C rozporządzenia wykonawczego 14086.

([308]) Tj. systemowego lub celowego nieprzestrzegania mającego zastosowanie prawa amerykańskiego, które może podważyć reputację lub integralność jednostki Wspólnoty Wywiadowczej lub w inny sposób zakwestionować prawidłowość działań Wspólnoty Wywiadowczej, w tym w świetle jakiegokolwiek znaczącego wpływu na interesy w zakresie ochrony prywatności i wolności obywatelskich danej osoby lub danych osób, zob. sekcja 5 lit. l) rozporządzenia wykonawczego 14086.

([309]) Sekcja 2 lit. d) pkt (iii) rozporządzenia wykonawczego 14086.

([310]) Sekcja 2 lit. d) pkt (i) ppkt B rozporządzenia wykonawczego 14086.

(164) Podobnie jak w przypadku organów egzekwowania prawa w sprawach karnych we wszystkich agencjach wywiadowczych funkcjonują urzędnicy ds. prywatności i wolności obywatelskich ([311]). Uprawnienia tych urzędników zazwyczaj obejmują nadzór nad procedurami w celu zapewnienia, aby dany departament lub dana agencja odpowiednio uwzględniały kwestie dotyczące prywatności i wolności obywatelskich oraz aby wdrażały odpowiednie procedury rozpatrywania skarg złożonych przez osoby fizyczne, które uważają, że ich prywatność lub wolności obywatelskie zostały naruszone (w niektórych przypadkach, podobnie jak Urząd Dyrektora Krajowych Służb Wywiadowczych, sami mogą mieć uprawnienia do badania skarg ([312])). Szefowie agencji wywiadowczych muszą dopilnować, aby urzędnicy ds. prywatności i wolności obywatelskich dysponowali zasobami niezbędnymi do wykonywania swoich uprawnień, mieli dostęp do wszelkich materiałów i zasobów osobowych niezbędnych do wypełniania swoich funkcji oraz byli informowani o proponowanych zmianach polityki, a także aby konsultowano się z nimi w sprawie odnośnych zmian ([313]). Urzędnicy ds. prywatności i wolności obywatelskich składają PCLOB okresowe sprawozdania dotyczące m.in. liczby i rodzaju skarg otrzymanych przez departament/agencję oraz podsumowanie sposobu rozpatrzenia takich skarg, prowadzonych przeglądów i postępowań oraz wpływu działań przeprowadzonych przez urzędnika ([314]).

(165) Po drugie, każda agencja wywiadowcza posiada niezależnego Inspektora Generalnego odpowiadającego m.in. za nadzorowanie działań wywiadowczych. Obejmuje to, w obrębie Urzędu Dyrektora Krajowych Służb Wywiadowczych, Biuro Inspektora Generalnego Wspólnoty Wywiadowczej, które sprawuje kompleksową jurysdykcję nad całą Wspólnotą Wywiadowczą i jest uprawnione do badania skarg lub informacji na temat zarzutów dotyczących postępowania niezgodnego z prawem lub nadużyć władzy w związku z programami i działaniami prowadzonymi w ramach Urzędu Dyrektora Krajowych Służb Wywiadowczych lub Wspólnoty Wywiadowczej ([315]). Tak jak w przypadku organów egzekwowania prawa w sprawach karnych (zob. motyw 109) tacy Inspektorzy Generalni są ustawowo niezależni ([316]) i odpowiedzialni za przeprowadzanie audytów i dochodzeń dotyczących programów i działań prowadzonych przez odpowiednią agencję do krajowych celów wywiadowczych, w tym w odniesieniu do nadużyć lub naruszeń prawa ([317]). Mają wgląd we wszystkie rejestry, sprawozdania, audyty, przeglądy, dokumenty, opracowa-

([311]) Zob. tytuł 42 § 2000ee-1 U.S.C. Obejmuje to np. Departament Stanu, Departament Sprawiedliwości, Departament Bezpieczeństwa Wewnętrznego, Departament Obrony, Agencję Bezpieczeństwa Narodowego, Centralną Agencję Wywiadowczą (CIA), FBI i Urząd Dyrektora Krajowych Służb Wywiadowczych.

([312]) Zob. sekcja 3 lit. c) rozporządzenia wykonawczego 14086.

([313]) Tytuł 42 § 2000ee-1 lit. d) U.S.C.

([314]) Zob. tytuł 42 § 2000ee-1 lit. f) pkt 1 i 2 U.S.C. Na przykład ze sprawozdania Biura Wolności Obywatelskich, Ochrony Prywatności i Przejrzystości przy Agencji Bezpieczeństwa Narodowego obejmującego okres od stycznia 2021 r. do czerwca 2021 r. wynika, że przeprowadziło ono 591 przeglądów dotyczących wpływu na wolności obywatelskie i prywatność w różnych kontekstach, np. w odniesieniu do działań związanych z gromadzeniem danych, uzgodnień i decyzji dotyczących wymiany informacji, decyzji dotyczących przechowywania danych itp., z uwzględnieniem różnych czynników, takich jak ilość i rodzaj informacji związanych z tymi działaniami, zaangażowane osoby, cel i przewidywane wykorzystanie danych, zabezpieczenia stosowane w celu ograniczenia potencjalnego ryzyka dla prywatności itp. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Podobnie sprawozdania Biura Ochrony Prywatności i Wolności Obywatelskich CIA za okres od stycznia do czerwca 2019 r. zawierają informacje na temat działań nadzorczych tego biura, np. przegląd zgodności z wytycznymi prokuratora generalnego na podstawie rozporządzenia wykonawczego 12333 w odniesieniu do zatrzymywania i rozpowszechniania informacji, wytyczne dotyczące wdrażania dyrektywy politycznej Prezydenta nr 28 oraz wymogi dotyczące identyfikowania i rozwiązywania problemu naruszeń ochrony danych, a także przeglądy wykorzystania danych osobowych i obchodzenia się z nimi (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Inspektora Generalnego powołuje Prezydent za zgodą Senatu; Inspektor może zostać odwołany wyłącznie przez Prezydenta.

([316]) Inspektorzy Generalni są powoływani na określoną kadencję i mogą zostać odwołani wyłącznie przez Prezydenta, który musi przedstawić Kongresowi pisemne uzasadnienie decyzji o ich odwołaniu. Nie oznacza to jednak, że inspektorzy działają w całkowicie niezależny sposób. W niektórych przypadkach dyrektor departamentu może zakazać Inspektorowi Generalnemu wszczęcia, przeprowadzania lub zakończenia audytu lub dochodzenia, w przypadku gdy uzna to za konieczne do zabezpieczenia ważnych interesów narodowych (interesów związanych z bezpieczeństwem narodowym). Kongres musi jednak zostać poinformowany o tym, że dyrektor skorzystał z tego uprawnienia, co może stanowić podstawę do pociągnięcia go do odpowiedzialności. Zob. np. w ustawie o Inspektorze Generalnym z 1978 r.: § 8 (w odniesieniu do Departamentu Obrony); § 8E (w odniesieniu do DoJ), § 8G lit. d) pkt 2 ppkt A i B (w odniesieniu do Agencji Bezpieczeństwa Narodowego); 50. § 403q lit. b) U.S.C. (w odniesieniu do CIA); sekcja 405 lit. f) ustawy o zatwierdzeniu działań wywiadowczych na rok budżetowy 2010 (w odniesieniu do Wspólnoty Wywiadowczej).

([317]) Ustawa o Inspektorze Generalnym z 1978 r., z późniejszymi zmianami, Zbiór ustaw publicznych nr L. 117–108 z dnia 8 kwietnia 2022 r. Na przykład, jak wyjaśniono w półrocznych sprawozdaniach dla Kongresu obejmujących okres od 1 kwietnia 2021 r. do 31 marca 2022 r., Inspektor Generalny Agencji Bezpieczeństwa Narodowego przeprowadził oceny przetwarzania danych dotyczących obywateli i rezydentów USA zgromadzonych na podstawie rozporządzenia wykonawczego 12333, procesu usuwania danych z rozpoznania radioelektronicznego, zautomatyzowanego narzędzia do ukierunkowywania wykorzystywanego przez Agencję Bezpieczeństwa Narodowego oraz zgodności z zasadami dotyczącymi dokumentacji i zapytań w odniesieniu do gromadzenia danych na podstawie sekcji 702 ustawy o kontroli wywiadu, a także wydał szereg zaleceń w tym kontekście (zob.https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, s. 5–8 oraz https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, s. 10–13). Zob. także niedawne audyty i dochodzenia przeprowadzone przez Inspektora Generalnego Wspólnoty Wywiadowczej w sprawie bezpieczeństwa informacji i nieuprawnionego ujawniania informacji niejawnych dotyczących bezpieczeństwa narodowego (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, s. 8, 11 i https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, s. 19–20).

nia, zalecenia lub inne istotne materiały, w razie potrzeby na mocy wezwania, oraz mogą odbierać zeznania ([318]). Inspektorzy Generalni kierują sprawy o podejrzenie popełnienia przestępstwa do organów ścigania i formułują zalecenia dotyczące działań naprawczych skierowane do szefów agencji ([319]). Chociaż ich zalecenia są niewiążące, to sprawozdania, m.in. na temat działań następczych (lub braku takich działań) ([320]), co do zasady są podawane do publicznej wiadomości i wysyłane do Kongresu, który na ich podstawie może wykonywać swoją funkcję nadzorczą (zob. motywy 168–169) ([321]).

(166) Po trzecie, Rada Nadzoru nad Służbami Wywiadowczymi, ustanowiona w ramach prezydenckiej Rady Konsultacyjnej ds. Wywiadu, jest odpowiedzialna za monitorowanie przestrzegania przepisów konstytucji i wszystkich mających zastosowanie przepisów przez amerykańskie organy wywiadowcze ([322]). Rada Konsultacyjna ds. Wywiadu jest organem doradczym Biura Wykonawczego Prezydenta. W jej skład wchodzi 16 członków spoza rządu amerykańskiego powołanych przez Prezydenta. W skład Rady Nadzoru nad Służbami Wywiadowczymi wchodzi maksymalnie pięciu członków wyznaczonych przez Prezydenta spośród członków Rady Konsultacyjnej ds. Wywiadu. Zgodnie z rozporządzeniem wykonawczym 12333 ([323]) szefowie wszystkich agencji wywiadowczych są zobowiązani do zgłaszania Radzie Nadzoru nad Służbami Wywiadowczymi wszelkich działań wywiadowczych, co do których istnieją powody, by sądzić, że mogą być niezgodne z prawem lub sprzeczne z rozporządzeniem wykonawczym lub dyrektywą prezydencką. Aby zapewnić Radzie Nadzoru nad Służbami Wywiadowczymi dostęp do informacji niezbędnych do wykonywania jej funkcji, w rozporządzeniu wykonawczym 13462 zobowiązano Dyrektora Krajowych Służb Wywiadowczych i szefów agencji wywiadowczych do przekazywania wszelkich informacji i udzielania pomocy, które Rada ta uzna za potrzebne do wykonywania swoich funkcji, w zakresie dozwolonym przez prawo ([324]). Rada Nadzoru nad Służbami Wywiadowczymi jest z kolei zobowiązana do informowania Prezydenta o działaniach wywiadowczych, które jej zdaniem mogą naruszać prawo amerykańskie (w tym rozporządzenia wykonawcze), a nie są odpowiednio traktowane przez prokuratora generalnego, Dyrektora Krajowych Służb Wywiadowczych lub szefa agencji wywiadowczej ([325]). Rada Nadzoru nad Służbami Wywiadowczymi ma ponadto obowiązek informowania prokuratora generalnego o możliwych naruszeniach prawa karnego.

(167) Po czwarte, agencje wywiadowcze podlegają nadzorowi Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi. Zgodnie ze statutem założycielskim PCLOB powierzono obowiązki w obszarze kształtowania i wdrażania polityki walki z terroryzmem, aby zapewnić ochronę prywatności i wolności obywatelskich. W swoim przeglądzie działalności agencji wywiadowczych Rada ma dostęp do wszystkich stosownych rejestrów, sprawozdań, audytów, przeglądów, dokumentów, opracowań i zaleceń agencji, z uwzględnieniem informacji niejawnych, oraz może przeprowadzać przesłuchania i odbierać zeznania ([326]). Rada otrzymuje sprawozdania od urzędników ds. wolności obywatelskich i prywatności z szeregu departamentów/agencji federalnych ([327]), może wydawać zalecenia skierowane do rządu i agencji wywiadowczych i regularnie sporządza sprawozdania dla komisji Kongresu i dla Prezydenta ([328]). Sprawozdania Rady, w tym te przedkładane Kongresowi, muszą być w możliwie największym stopniu dostępne publicznie ([329]). PCLOB wydała kilka sprawozdań dotyczących nadzoru i sprawozdań z działań następczych zawierających analizę programów prowadzonych na podstawie sekcji 702 ustawy o kontroli wywiadu i ochrony prywatności w tym kontekście, wdrożenia dyrektywy politycznej Prezydenta nr 28 i rozporządzenia wykonawczego 12333 ([330]). Zadaniem PCLOB jest również pełnienie określonych funkcji nadzorczych w odniesieniu do wdrażania

([318]) Zob. § 6 ustawy o Inspektorze Generalnym z 1978 r.

([319]) Zob. *ibid.* §§ 4, 6-5.

([320]) Jeśli chodzi o działania następcze podejmowane w związku ze sprawozdaniami i zaleceniami Inspektorów Generalnych, zob. np. odpowiedź na sprawozdanie Inspektora Generalnego DoJ, w którym stwierdzono, że FBI nie było wystarczająco przejrzyste w stosunku do Sądu ds. Kontroli Wywiadu we wnioskach składanych w latach 2014–2019, co doprowadziło do reform mających na celu poprawę przestrzegania zasad, nadzoru i rozliczalności w FBI (np. dyrektor FBI nakazał podjęcie ponad 40 działań naprawczych, w tym 12 konkretnych działań w odniesieniu do procesu na podstawie ustawy o kontroli wywiadu dotyczących dokumentacji, nadzoru, prowadzenia akt, szkoleń i audytów) (zob.https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance oraz https://oig.justice.gov/reports/2019/o20012.pdf). Zob. na przykład również audyt Inspektora Generalnego DoJ dotyczący ról i obowiązków Biura Głównego Radcy Prawnego FBI w zakresie nadzorowania przestrzegania obowiązujących przepisów, polityk i procedur dotyczących działań FBI w zakresie bezpieczeństwa narodowego oraz dodatek 2 zawierający pismo od FBI, w którym zaakceptowano wszystkie zalecenia. W tym względzie dodatek 3 zawiera przegląd działań następczych i informacji, których Inspektor Generalny wymagał od FBI, by możliwe było zakończenie realizacji jego zaleceń (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

([321]) Zob. § 4 ust. 5 i § 5 ustawy o Inspektorze Generalnym z 1978 r.

([322]) Zob. rozporządzenie wykonawcze 13462.

([323]) Sekcja 1.6 lit. c) rozporządzenia wykonawczego 12333.

([324]) Sekcja 8 lit. a) rozporządzenia wykonawczego 13462.

([325]) Sekcja 6 lit. b) rozporządzenia wykonawczego 13462.

([326]) Tytuł 42 § 2000ee lit. g) U.S.C.

([327]) Zob. tytuł 42 § 2000ee-1 lit. f) pkt 1 ppkt A pppkt (iii) U.S.C. Należy wśród nich wymienić przynajmniej Departament Sprawiedliwości, Departament Obrony, Departament Bezpieczeństwa Wewnętrznego, Dyrektora Krajowych Służb Wywiadowczych i Centralną Agencję Wywiadowczą, a także wszelkie inne departamenty, agencje lub jednostki struktury władzy wykonawczej wskazane jako właściwe przez PCLOB.

([328]) Tytuł 42 § 2000ee lit. e) U.S.C.

([329]) Tytuł 42 § 2000ee lit. f) U.S.C.

([330]) Tekst dostępny pod adresem: https://www.pclob.gov/Oversight

rozporządzenia wykonawczego 14086, w szczególności sprawdzanie, czy procedury stosowane przez agencje są zgodne z tym rozporządzeniem wykonawczym (zob. motyw 126), oraz ocena poprawności funkcjonowania mechanizmu dochodzenia roszczeń (zob. motyw 194).

(168) Po piąte, niezależnie od mechanizmów nadzoru funkcjonujących w strukturze władzy wykonawczej, specjalne komisje w Kongresie Stanów Zjednoczonych (Komisja ds. Wywiadu i Komisja ds. Sprawiedliwości w Izbie Reprezentantów i w Senacie) są zobowiązane do sprawowania nadzoru nad wszystkimi działaniami Stanów Zjednoczonych w obszarze wywiadu zagranicznego. Członkowie tych komisji są uprawnieni do uzyskania dostępu do informacji niejawnych oraz do zapoznania się z metodami i programami wywiadowczymi ([331]). Komisje sprawują funkcje nadzorcze w różnych formach, w szczególności w formie przesłuchań, dochodzeń, przeglądów i sprawozdań ([332]).

(169) Komisje Kongresu otrzymują regularne sprawozdania z działań wywiadowczych, m.in. od prokuratora generalnego, Dyrektora Krajowych Służb Wywiadowczych, agencji wywiadowczych i innych organów nadzoru (np. Inspektorów Generalnych), zob. motywy 164–165. W szczególności zgodnie z ustawą o bezpieczeństwie narodowym „Prezydent zapewnia kongresowym komisjom ds. wywiadu dostęp do pełnych i aktualnych informacji na temat działalności wywiadowczej Stanów Zjednoczonych, w tym do informacji o wszelkich istotnych planowanych działaniach wywiadowczych, zgodnie z wymogami ustanowionymi w niniejszym podrozdziale" ([333]). Ponadto „Prezydent zapewnia niezwłoczne zgłaszanie wszelkich niezgodnych z prawem działań wywiadowczych kongresowym komisjom ds. wywiadu oraz przekazywanie im informacji o wszelkich działaniach naprawczych, które zostały podjęte lub które mają zostać podjęte w związku z taką niezgodną z prawem działalnością" ([334]).

(170) Ze szczególnych ustaw wynikają ponadto dodatkowe wymogi w zakresie sprawozdawczości. W szczególności zgodnie z ustawą o kontroli wywiadu prokurator generalny jest zobowiązany do przekazywania Komisji ds. Wywiadu i Komisji ds. Sprawiedliwości w Senacie i Izbie Reprezentantów „pełnych informacji" na temat działań podejmowanych przez rząd zgodnie z określonymi sekcjami ustawy o kontroli wywiadu ([335]). Na mocy ustawy o kontroli wywiadu rząd został również zobowiązany do przekazywania komisjom Kongresu kopii wszystkich orzeczeń, zarządzeń lub opinii Sądu ds. Kontroli Wywiadu lub Sądu Odwoławczego ds. Kontroli Wywiadu, w których dokonano „istotnej interpretacji przepisów" ustawy o kontroli wywiadu lub w których dokonano „wykładni" tych przepisów. Jeżeli chodzi o sprawowanie nadzoru, o którym mowa w sekcji 702 ustawy o kontroli wywiadu, taki nadzór parlamentarny sprawuje się za pośrednictwem sprawozdań, które zgodnie z przepisami ustawy należy przekazywać Komisji ds. Wywiadu i Komisji ds. Sprawiedliwości, a także poprzez częste organizowanie odpraw i wysłuchań. Wśród tych sprawozdań należy wymienić sprawozdanie półroczne prokuratora generalnego dotyczące stosowania przepisów sekcji 702 ustawy o kontroli wywiadu wraz z dokumentami potwierdzającymi, uwzględniając sprawozdania Departamentu Sprawiedliwości i Urzędu Dyrektora Krajowych Służb Wywiadowczych dotyczące przestrzegania zasad oraz opis wszelkich przypadków nieprzestrzegania zasad ([336]), a także odrębną ocenę półroczną przeprowadzaną przez prokuratora generalnego i przygotowywany przez Departament Sprawiedliwości dokument dotyczący zgodności z procedurami ukierunkowywania i minimalizacji ([337]).

([331]) Tytuł 50 § 3091 U.S.C.

([332]) Na przykład komisje te organizują przesłuchania tematyczne (zob. na przykład niedawne przesłuchanie Komisji ds. Sprawiedliwości w Izbie Reprezentantów w sprawie „cyfrowych obław",https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983 oraz przesłuchanie Komisji ds. Wywiadu w Izbie Reprezentantów w sprawie wykorzystania sztucznej inteligencji przez Wspólnotę Wywiadowczą, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263), regularne przesłuchania nadzorcze, np. FBI i wydziału bezpieczeństwa narodowego DoJ, zob. https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 i https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899 Przykładem dochodzenia jest dochodzenie senackiej Komisji ds. Wywiadu w sprawie rosyjskiej ingerencji w wybory w USA w 2016 r., zob. https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures Jeśli chodzi o sprawozdawczość, zob. na przykład przegląd działań (nadzorczych) Komisji w sprawozdaniu senackiej Komisji ds. Wywiadu dla Senatu obejmującym okres od 4 stycznia 2019 r. do 3 stycznia 2021 r., https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4

([333]) Zob. tytuł 50 § 3091 lit. a) ppkt 1 U.S.C. W przywołanym punkcie ustanowiono ogólne wymogi dotyczące nadzoru Kongresu nad kwestiami związanymi z bezpieczeństwem narodowym.

([334]) Zob. tytuł 50 § 3091 lit. b) U.S.C.

([335]) Zob. tytuł 50 §§ 1808, 1846, 1862, 1871 i 1881f U.S.C.

([336]) Zob. tytuł 50 § 1881f U.S.C.

([337]) Zob. tytuł 50 § 1881a lit. l) pkt 1 U.S.C.

(171) Ponadto zgodnie z ustawą o kontroli wywiadu rząd Stanów Zjednoczonych jest zobowiązany do ujawniania co roku Kongresowi (i społeczeństwu) liczby nakazów na mocy ustawy o kontroli wywiadu, o które się ubiegano i które otrzymano, a także szacunków dotyczących m.in. liczby obywateli i rezydentów USA oraz liczby osób niebędących obywatelami ani rezydentami USA objętych nadzorem ([338]). W ustawie przewidziano również dodatkowy wymóg podawania do wiadomości publicznej liczby wydanych wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego, ponownie w odniesieniu do obywateli i rezydentów USA i osób niebędących obywatelami ani rezydentami USA (zapewniając jednocześnie odbiorcom nakazów i certyfikatów wydanych na podstawie ustawy o kontroli wywiadu oraz wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego możliwość opublikowania – w określonych przypadkach – sprawozdań z przejrzystości) ([339]).

(172) Ogólniej rzecz ujmując, Wspólnota Wywiadowcza Stanów Zjednoczonych podejmuje różne działania mające na celu zapewnienie przejrzystości swoich działań wywiadowczych. Na przykład w 2015 r. Urząd Dyrektora Krajowych Służb Wywiadowczych przyjął zasady przejrzystości danych wywiadowczych i plan wdrażania przejrzystości oraz zarządził, aby każda agencja wywiadowcza wyznaczała urzędnika ds. przejrzystości danych wywiadowczych w celu zwiększenia przejrzystości i prowadzenia inicjatyw w zakresie przejrzystości ([340]). W ramach tych działań Wspólnota Wywiadowcza upubliczniła i nadal upublicznia odtajnione części polityk, procedur, sprawozdań dotyczących nadzoru, sprawozdań na temat działań prowadzonych na podstawie sekcji 702 ustawy o kontroli wywiadu i rozporządzenia wykonawczego 12333, orzeczeń Sądu ds. Kontroli Wywiadu i innych materiałów, m.in. na specjalnej stronie internetowej „IC on the Record" zarządzanej przez Urząd Dyrektora Krajowych Służb Wywiadowczych ([341]).

(173) Poza nadzorem organów nadzoru wymienionych w motywach 162–168 gromadzenie danych osobowych zgodnie z sekcją 702 ustawy o kontroli wywiadu podlega ponadto nadzorowi Sądu ds. Kontroli Wywiadu ([342]). Zgodnie z zasadą 13 regulaminu Sądu ds. Kontroli Wywiadu urzędnicy ds. zgodności w amerykańskich agencjach wywiadowczych są zobowiązani do zgłaszania wszelkich naruszeń przepisów sekcji 702 ustawy o kontroli wywiadu dotyczących procedur ukierunkowywania, minimalizacji i zapytań do DoJ i Urzędu Dyrektora Krajowych Służb Wywiadowczych, które z kolei zgłaszają je do Sądu ds. Kontroli Wywiadu. DoJ i Urząd Dyrektora Krajowych Służb Wywiadowczych przedkładają ponadto Sądowi ds. Kontroli Wywiadu półroczne wspólne sprawozdania oceniające w zakresie nadzoru, w których określają tendencje dotyczące przestrzegania zasad ukierunkowywania, dostarczają danych statystycznych, opisują kategorie przypadków nieprzestrzegania zasad; opisują szczegółowo przyczyny wystąpienia niektórych przypadków niezgodności z procedurami ukierunkowywania oraz przedstawiają zastosowane przez agencje wywiadowcze środki służące uniknięciu ich ponownego wystąpienia ([343]).

(174) W stosownych przypadkach (np. w przypadku stwierdzenia naruszeń procedur ukierunkowywania) Sąd ten może nakazać odpowiedniej agencji wywiadowczej podjęcie działań zaradczych ([344]). Wspomniane działania mogą mieć różne formy: od pojedynczych środków, np. zakończenia uzyskiwania danych i usunięcia nielegalnie pozyskanych danych, po środki strukturalne, w tym zmianę praktyki gromadzenia, m.in. pod względem wytycznych i szkolenia dla pracowników ([345]). Ponadto podczas corocznego przeglądu certyfikacji na podstawie sekcji 702 Sąd ds. Kontroli

([338]) Tytuł 50 § 1873 lit. b) U.S.C. Ponadto zgodnie z sekcją 402 „Dyrektor Krajowych Służb Wywiadowczych, w porozumieniu z prokuratorem generalnym, przeprowadza przegląd w przedmiocie zniesienia klauzuli tajności w odniesieniu do poszczególnych orzeczeń, zarządzeń lub opinii wydanych przez Sąd ds. Kontroli Wywiadu lub przez Sąd Odwoławczy ds. Kontroli Wywiadu (zgodnie z sekcją 601 lit. e)), w których dokonano istotnej interpretacji lub wykładni przepisów ustawowych, uwzględniając wszelkie nowe lub istotne interpretacje lub wykładnie pojęcia »konkretnego terminu umożliwiającego selekcję«, i – zgodnie z wynikami tego przeglądu – podaje takie orzeczenie, zarządzenie lub opinię do wiadomości publicznej w jak najszerszym zakresie".

([339]) Tytuł 50 § 1873 lit. b) pkt 7 i § 1874 U.S.C.

([340]) https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic

([341]) Zob. „IC on the Record", strona dostępna pod adresem:https://icontherecord.tumblr.com/

([342]) W przeszłości Sąd ds. Kontroli Wywiadu stwierdził, że „dla Sądu jest oczywiste, że agencje wykonawcze, jak również [Urząd Dyrektora Krajowych Służb Wywiadowczych] i [wydział bezpieczeństwa narodowego DoJ] przeznaczają znaczne zasoby na wykonywanie swoich obowiązków w zakresie zapewniania zgodności i sprawowania nadzoru zgodnie z sekcją 702. Co do zasady przypadki nieprzestrzegania zasad są szybko identyfikowane i podejmowane są odpowiednie działania naprawcze, do których należy usuwanie informacji, które uzyskano w nieprawidłowy sposób lub które w inny sposób podlegały wymogom zniszczenia zgodnie z obowiązującymi procedurami". Sąd ds. Kontroli Wywiadu, opinia i zarządzenie w sprawie memorandum [podpis utajniony] (2014 r.), dostępne pod adresem https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf

([343]) Zob. np. sprawozdanie DoJ/Urzędu Dyrektora Krajowych Służb Wywiadowczych dotyczące stosowania przepisów sekcji 702 ustawy o kontroli wywiadu za okres od czerwca 2018 r. do listopada 2018 r. przedłożone Sądowi ds. Kontroli Wywiadu, s. 21–65.

([344]) Tytuł 50 § 1803 lit. h) U.S.C. Zob. również sprawozdanie PCLOB dotyczące sekcji 702, s. 76. Zob. ponadto Sąd ds. Kontroli Wywiadu, opinia i zarządzenie w sprawie memorandum z dnia 3 października 2011 r. jako przykład nakazu usunięcia uchybień zobowiązującego rząd do wyeliminowania stwierdzonych uchybień w ciągu 30 dni. Tekst dostępny pod adresem: https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf Zob. pismo Waltona, sekcja 4, s. 10–11. Zob. także opinia Sądu ds. Kontroli Wywiadu z dnia 18 października 2018 r. dostępna pod adresem https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, którą to opinię potwierdził Sąd Odwoławczy ds. Kontroli Wywiadu w swojej opinii z dnia 12 lipca 2019 r., która jest dostępna pod adresem https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf – Sąd ds. Kontroli Wywiadu m.in. nakazał w niej, aby rząd spełnił wobec niego określone wymogi w zakresie powiadamiania, dokumentacji i sprawozdawczości.

([345]) Zob. na przykład Sąd ds. Kontroli Wywiadu, opinia i zarządzenie w sprawie memorandum, s. 76 (6 grudnia 2019 r.) (zatwierdzone do podania do wiadomości publicznej w dniu 4 września 2020 r.), w którym to dokumencie Sąd ds. Kontroli Wywiadu nakazał, aby do 28 lutego 2020 r. rząd przedłożył pisemne sprawozdanie z kroków, które podjął w celu usprawnienia procesów identyfikowania i usuwania sprawozdań sporządzonych na podstawie informacji, o których mowa w art. 702 ustawy o kontroli wywiadu, które zostały wycofane ze względów dotyczących przestrzegania zasad, a także na temat innych kwestii. Zob. również załącznik VII.

Wywiadu bierze pod uwagę przypadki nieprzestrzegania zasad w celu ustalenia, czy przedstawione certyfikacje są zgodne z wymogami ustawy o kontroli wywiadu. Podobnie Sąd ds. Kontroli Wywiadu – jeśli uzna, że certyfikacje rządu nie spełniły wymogów, między innymi z powodu określonych przypadków nieprzestrzegania zasad – może wydać tak zwany „nakaz usunięcia uchybień" zobowiązujący rząd do naprawienia naruszenia w ciągu 30 dni lub do zaprzestania bądź nierozpoczynania wdrażania certyfikacji zgodnie z sekcją 702. Ponadto Sąd ds. Kontroli Wywiadu ocenia obserwowane przez siebie tendencje w zakresie przestrzegania zasad i może wymagać wprowadzenia zmian w procedurach lub dodatkowego nadzoru i sprawozdawczości w celu uwzględnienia tendencji w zakresie przestrzegania zasad ([346]).

3.2.3. ***Dochodzenie roszczeń***

(175) Jak wyjaśniono szczegółowo w niniejszej sekcji, osoby z Unii, których dane dotyczą, mogą skorzystać w Stanach Zjednoczonych z licznych możliwości wytoczenia powództwa przed niezależnym i bezstronnym sądem posiadającym odpowiednie uprawnienia. Łącznie umożliwiają one osobom fizycznym dostęp do ich danych osobowych, weryfikację zgodności z prawem dostępu organów rządowych do ich danych oraz – w przypadku stwierdzenia naruszenia – naprawienie takiego naruszenia, w tym poprzez sprostowanie lub usunięcie ich danych osobowych.

(176) Po pierwsze, na mocy rozporządzenia wykonawczego 14086 ustanowiono specjalny mechanizm dochodzenia roszczeń, uzupełniony zarządzeniem prokuratora generalnego ustanawiającym Sąd Odwoławczy ds. Ochrony Danych, w celu rozpatrywania i rozstrzygania skarg od osób fizycznych dotyczących działań USA w zakresie rozpoznania radioelektronicznego. Każda fizyczna osoba w UE jest uprawniona do złożenia skargi w ramach mechanizmu dochodzenia roszczeń dotyczącej domniemanego naruszenia amerykańskiego prawa regulującego działania w zakresie rozpoznania radioelektronicznego (np. rozporządzenia wykonawczego 14086, sekcji 702 ustawy o kontroli wywiadu, rozporządzenia wykonawczego 12333), które negatywnie wpływa na jego interesy w zakresie ochrony prywatności i wolności obywatelskich ([347]). Ten mechanizm dochodzenia roszczeń jest dostępny dla osób z krajów lub regionalnych organizacji integracji gospodarczej, które zostały wyznaczone przez prokuratora generalnego USA jako „kraje kwalifikujące się" ([348]). 30 czerwca 2023 r. prokurator generalny wyznaczył Unię Europejską i trzy państwa Europejskiego Stowarzyszenia Wolnego Handlu, które razem stanowią Europejski Obszar Gospodarczy, na podstawie sekcji 3 lit. f) rozporządzenia wykonawczego 14086 jako „kraj kwalifikujący się" ([349]). Decyzja ta pozostaje bez uszczerbku dla art. 4 ust. 2 Traktatu o Unii Europejskiej.

(177) Osoba z Unii, której dane dotyczą, chcąca złożyć taką skargę, musi złożyć ją do organu nadzorczego w państwie członkowskim właściwego w sprawach nadzoru przetwarzania danych osobowych przez organy publiczne (organu ochrony danych) ([350]). Dzięki temu osoby fizyczne mają łatwy dostęp do mechanizmu dochodzenia roszczeń, gdyż mogą zwrócić się do organu „w pobliżu miejsca zamieszkania", z którym mogą komunikować się w swoim języku ojczystym. Po zweryfikowaniu wymogów dotyczących złożenia skargi, o których mowa w motywie 178, właściwy organ ochrony danych przekaże skargę, za pośrednictwem sekretariatu Europejskiej Rady Ochrony Danych, do mechanizmu dochodzenia roszczeń.

(178) Wniesienie skargi do mechanizmu dochodzenia roszczeń podlega niskim wymogom dopuszczalności, ponieważ osoby fizyczne nie muszą wykazać, że ich dane były faktycznie amerykańskich przedmiotem działań w zakresie rozpoznania radioelektronicznego ([351]). Jednocześnie, aby zapewnić punkt wyjścia dla mechanizmu dochodzenia roszczeń w celu przeprowadzenia przeglądu, należy podać pewne podstawowe informacje, np. dotyczące danych osobowych, co do których istnieje uzasadnione przypuszczenie, że zostały przekazane do USA, oraz środków, za pomocą których zakłada się, że zostały przekazane; tożsamości jednostek rządu USA, które uważa się za zaangażowane w domniemane naruszenie (jeśli są znane); podstawy zarzutu, że doszło do naruszenia prawa amerykańskiego (chociaż to również nie wymaga wykazania, że dane osobowe zostały faktycznie zgromadzone przez amerykańskie agencje wywiadowcze), oraz charakteru żądanego zadośćuczynienia.

([346]) Zob. załącznik VII.

([347]) Zob. sekcja 4 lit. k) pkt (iv) rozporządzenia wykonawczego 14086, która stanowi, że skargę do mechanizmu dochodzenia roszczeń musi wnieść skarżący działający we własnym imieniu (tj. nie jako przedstawiciel rządu, organizacji pozarządowej lub międzyrządowej). Pojęcie „osoby dotkniętej negatywnymi skutkami" nie wymaga od skarżącego osiągnięcia określonego progu, aby mieć dostęp do mechanizmu dochodzenia roszczeń (zob. motyw 178 w tym względzie). Wyjaśniono w nim raczej, że Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych i Sąd Odwoławczy ds. Ochrony Danych są uprawnione do przeciwdziałania naruszeniom prawa Stanów Zjednoczonych regulującego działania w zakresie rozpoznania radioelektronicznego, które negatywnie wpływają na indywidualne interesy skarżącego w zakresie prywatności i wolności obywatelskich. Natomiast naruszenia wymogów wynikających z obowiązującego prawa Stanów Zjednoczonych, które nie mają na celu ochrony osób fizycznych (np. wymogów budżetowych), wykraczałyby poza jurysdykcję Biura Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych i Sądu Odwoławczego ds. Ochrony Danych.

([348]) Sekcja 3 lit. f) rozporządzenia wykonawczego 14086.

([349]) https://www.justice.gov/opcl/executive-order-14086.

([350]) Sekcja 4 lit. d) pkt (v) rozporządzenia wykonawczego 14086.

([351]) Zob. sekcja 4 lit. k) pkt (i)–(iv) rozporządzenia wykonawczego 14086.

(179) Wstępne badanie skarg kierowanych do tego mechanizmu dochodzenia roszczeń przeprowadza Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych, którego istniejącą ustawową rolę i uprawnienia rozszerzono na te konkretne działania podejmowane zgodnie z rozporządzeniem wykonawczym 14086 ([352]). W ramach Wspólnoty Wywiadowczej Biuro Wolności Obywatelskich i Ochrony Prywatności odpowiada między innymi za zapewnienie, by ochronę wolności obywatelskich i prywatności odpowiednio uwzględniono w strategiach politycznych i procedurach Urzędu Dyrektora Krajowych Służb Wywiadowczych i agencji wywiadowczych; za nadzorowanie przestrzegania przez Urząd Dyrektora Krajowych Służb Wywiadowczych obowiązujących wymogów dotyczących wolności obywatelskich i prywatności; oraz za przeprowadzanie ocen wpływu na prywatność ([353]). Odwołanie osoby pełniącej funkcję w Biurze Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych może nastąpić wyłącznie przez Dyrektora Krajowych Służb Wywiadowczych z ważnej przyczyny, tj. w przypadku uchybienia, niewłaściwego sprawowania urzędu, naruszenia bezpieczeństwa, zaniedbania obowiązków lub niezdolności do sprawowania urzędu ([354]).

(180) Przy przeprowadzaniu przeglądu Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych ma dostęp do informacji na potrzeby swojej oceny i może korzystać z pomocy urzędników ds. prywatności i wolności obywatelskich w poszczególnych agencjach wywiadowczych ([355]). Agencje wywiadowcze nie mogą utrudniać przeglądów przeprowadzanych przez Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych ani wywierać na nie niewłaściwego wpływu. Dotyczy to również Dyrektora Krajowych Służb Wywiadowczych, który nie może ingerować w przegląd ([356]). Rozpatrując skargę, Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych musi „stosować prawo bezstronnie", mając na uwadze zarówno interesy bezpieczeństwa narodowego w działaniach w zakresie rozpoznania radioelektronicznego, jak i zabezpieczenia prywatności ([357]).

(181) W ramach przeglądu Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych ustala, czy doszło do naruszenia obowiązującego prawa amerykańskiego, a jeżeli tak – podejmuje decyzję o zastosowaniu odpowiednich środków zaradczych ([358]). Są to środki, które umożliwiają pełne zrekompensowanie stwierdzonego naruszenia, takie jak zaniechanie bezprawnego pozyskiwania danych, usunięcie danych zgromadzonych niezgodnie z prawem, usunięcie wyników nieprawidłowo dokonanych zapytań odnoszących się do danych zgromadzonych zgodnie z prawem w inny sposób, ograniczenie dostępu do danych zgromadzonych zgodnie z prawem do odpowiednio przeszkolonego personelu lub wycofanie sprawozdań służb wywiadowczych zawierających dane, które pozyskano bez uzyskania prawnego upoważnienia lub które rozpowszechniano niezgodnie z prawem ([359]). Decyzje podjęte przez Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych w sprawie skarg indywidualnych (w tym decyzje w sprawie środków zaradczych) są wiążące dla zainteresowanych agencji wywiadowczych ([360]).

(182) Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych przechowuje dokumentację przeglądu oraz wydaje niejawną decyzję zawierającą podstawę dokonanych ustaleń faktycznych, ustalenia w odniesieniu do tego, czy doszło do naruszenia objętego zakresem, oraz wskazanie odpowiedniego środka zaradczego ([361]). Jeżeli w wyniku przeglądu Biura Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych ujawnione zostanie naruszenie ze strony organu podlegającego nadzorowi Sądu ds. Kontroli Wywiadu, Biuro Wolności Obywatelskich i Ochrony Prywatności musi również przedstawić niejawne sprawozdanie asystentowi prokuratora generalnego ds. bezpieczeństwa narodowego, który z kolei jest zobowiązany do zgłoszenia niezgodności Sądowi ds. Kontroli Wywiadu, który może podjąć dalsze czynności egzekucyjne (zgodnie z procedurą opisaną w motywach 173–174) ([362]).

(183) Po zakończeniu przeglądu Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych informuje skarżącego za pośrednictwem organu krajowego, że „kontrola nie wykazała żadnych naruszeń objętych zakresem albo [że] Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych wydało decyzję nakazującą wdrożenie odpowiednich środków zaradczych" ([363]). Umożliwia to zapewnienie ochrony poufności działań prowadzonych w celu ochrony bezpieczeństwa narodowego, przy jednoczesnym zapewnieniu osobom fizycznym decyzji potwierdzającej, że ich skarga została należycie zbadana i rozpatrzona. Osoba fizyczna może ponadto zakwestionować tę decyzję. W tym celu zostanie ona poinformowana o możliwości odwołania się do Sądu Odwoławczego ds. Ochrony Danych w celu dokonania przeglądu ustaleń Biura Wolności Obywatelskich i Ochrony Prywatności (zob. motyw 184 i dalsze) oraz o tym, że w przypadku wszczęcia postępowania przez Sąd zostanie wybrany rzecznik specjalny, który będzie reprezentował interesy skarżącego ([364]).

([352]) Sekcja 3 lit. c) pkt (iv) rozporządzenia wykonawczego 14086. Zob. również ustawa o bezpieczeństwie narodowym z 1947 r., tytuł 50 § 403–3d U.S.C., sekcja 103D dotycząca roli Biura Wolności Obywatelskich i Ochrony Prywatności w Urzędzie Dyrektora Krajowych Służb Wywiadowczych.

([353]) Tytuł 50 § 3029 lit. b) U.S.C.

([354]) Sekcja 3 lit. c) pkt (iv) rozporządzenia wykonawczego 14086.

([355]) Sekcja 3 lit. c) pkt (iii) rozporządzenia wykonawczego 14086.

([356]) Sekcja 3 lit. c) pkt (iv) rozporządzenia wykonawczego 14086.

([357]) Sekcja 3 lit. c) pkt (i) ppkt B pppkt (i) oraz (iii) rozporządzenia wykonawczego 14086.

([358]) Sekcja 3 lit. c) pkt (i) rozporządzenia wykonawczego 14086.

([359]) Sekcja 4 lit. a) rozporządzenia wykonawczego 14086.

([360]) Sekcja 3 lit. c) i d) rozporządzenia wykonawczego 14086.

([361]) Sekcja 3 lit. c) pkt (i) ppkt F–G rozporządzenia wykonawczego 14086.

([362]) Zob. również sekcja 3 lit. c) pkt (i) ppkt D rozporządzenia wykonawczego 14086.

([363]) Sekcja 3 lit. c) pkt (i) ppkt E pppkt 1 rozporządzenia wykonawczego 14086.

([364]) Sekcja 3 lit. c) pkt (i) ppkt E pppkt 2–3 rozporządzenia wykonawczego 14086.

(184) Każdy skarżący oraz każda jednostka Wspólnoty Wywiadowczej mogą wnieść o przegląd decyzji Biura Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych przed Sądem Odwoławczym ds. Ochrony Danych. Takie wnioski o przegląd należy złożyć w ciągu 60 dni od otrzymania od Biura Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych powiadomienia o zakończeniu przeglądu oraz muszą one zawierać wszystkie informacje, które osoba fizyczna chce przekazać Sądowi Odwoławczemu ds. Ochrony Danych (np. argumenty dotyczące kwestii prawnych lub zastosowania prawa do okoliczności faktycznych sprawy) ([365]). Osoby z Unii, których dane dotyczą, mogą ponownie złożyć wniosek do właściwego organu ochrony danych (zob. motyw 177).

(185) Sąd Odwoławczy ds. Ochrony Danych jest niezależnym sądem ustanowionym przez prokuratora generalnego na podstawie rozporządzenia wykonawczego 14086 ([366]). W jego skład wchodzi co najmniej sześciu sędziów powołanych przez prokuratora generalnego w porozumieniu z PCLOB, sekretarza handlu i Dyrektora Krajowych Służb Wywiadowczych na czteroletnią odnawialną kadencję ([367]). Przy powoływaniu sędziów prokurator generalny opiera się na kryteriach stosowanych przez władzę wykonawczą przy ocenie kandydatów na sędziów federalnych, nadając istotne znaczenie wcześniejszemu doświadczeniu sędziowskiemu ([368]). Sędziowie muszą być ponadto prawnikami praktykami (tj. aktywnymi członkami palestry o nieposzlakowanej opinii oraz muszą być należycie uprawnieni do wykonywania zawodu) i mieć odpowiednie doświadczenie w dziedzinie prawa dotyczącego prywatności i bezpieczeństwa narodowego. Prokurator generalny musi dołożyć starań, by co najmniej połowa sędziów w danym czasie miała wcześniejsze doświadczenie sędziowskie, a wszyscy sędziowie muszą mieć poświadczenia bezpieczeństwa, aby móc uzyskać dostęp do informacji niejawnych dotyczących bezpieczeństwa narodowego ([369]).

(186) Do Sądu Odwoławczego ds. Ochrony Danych mogą zostać powołane wyłącznie osoby, które spełniają kwalifikacje, o których mowa w motywie 185, oraz które w chwili powołania ani w ciągu ostatnich dwóch lat nie były zatrudnione przez instytucje władzy wykonawczej. Podobnie podczas kadencji na stanowiskach sędziów Sądu Odwoławczego ds. Ochrony Danych nie mogą oni również pełnić żadnych oficjalnych funkcji ani nie mogą być zatrudnieni w rządzie Stanów Zjednoczonych (na innym stanowisku niż sędziowie Sądu Odwoławczego ds. Ochrony Danych) ([370]).

(187) Niezależność procesu orzekania osiąga się za pomocą szeregu gwarancji. W szczególności jednostki władzy wykonawczej (prokurator generalny i agencje wywiadowcze) nie mogą ingerować w kontrolę prowadzoną przez Sąd Odwoławczy ds. Ochrony Danych ani wywierać na nią niewłaściwego wpływu ([371]). Sam Sąd Odwoławczy ds. Ochrony Danych jest zobowiązany do bezstronnego rozpoznawania spraw ([372]) i działa zgodnie z własnym regulaminem (przyjętym większością głosów). Ponadto sędziowie Sądu Odwoławczego ds. Ochrony Danych mogą zostać odwołani jedynie przez prokuratora generalnego i wyłącznie z podaniem przyczyny (tj. niewłaściwe postępowanie, niewłaściwe sprawowanie urzędu, naruszenie bezpieczeństwa, zaniedbanie obowiązków lub niezdolność do orzekania), po należytym uwzględnieniu norm mających zastosowanie do sędziów federalnych, określonych w regulaminie prowadzenia postępowań sądowych i niezdolności do prowadzenia postępowań sądowych ([373]).

([365]) § 201.6 lit. a)–b) zarządzenia prokuratora generalnego.

([366]) Sekcja 3 lit. d) pkt (i) oraz zarządzenie prokuratora generalnego. Sąd Najwyższy Stanów Zjednoczonych uznał możliwość powołania przez prokuratora generalnego niezależnych organów posiadających uprawnienia decyzyjne, w tym do orzekania w indywidualnych sprawach, zob. w szczególności Stany Zjednoczone ex rel. Accardi/Shaughnessy, 347 U.S. 260 (1954 r.) oraz Stany Zjednoczone/Nixon, 418 U.S. 683, 695 (1974 r.). Zgodność z różnymi wymogami rozporządzenia wykonawczego 14086, np. kryteriami i procedurą powoływania i odwoływania sędziów Sądu Odwoławczego ds. Ochrony Danych, podlega w szczególności nadzorowi Generalnego Inspektora Departamentu Sprawiedliwości (zob. również motyw 109 dotyczący ustawowej władzy inspektorów generalnych).

([367]) Sekcja 3 lit. d) pkt (i) ppkt A rozporządzenia wykonawczego 14086 i § 201.3 lit. a) zarządzenia prokuratora generalnego.

([368]) § 201.3 lit. b) zarządzenia prokuratora generalnego.

([369]) Sekcja 3 lit. d) pkt (i) ppkt B rozporządzenia wykonawczego 14086.

([370]) Sekcja 3 lit. d) pkt (i) ppkt A rozporządzenia wykonawczego 14086 i § 201.3 lit. a) i c) zarządzenia prokuratora generalnego. Osoby powołane do Sądu Odwoławczego ds. Ochrony Danych mogą uczestniczyć w działalności pozasądowej, w tym w działalności gospodarczej, działalności finansowej, działalności charytatywnej nienastawionej na zysk, działalności powierniczej oraz działalności prawniczej, jeżeli taka działalność nie zakłóca bezstronnego wykonywania ich obowiązków ani nie ogranicza skuteczności lub niezależności Sądu Odwoławczego ds. Ochrony Danych (§ 201.7 lit. c) zarządzenia prokuratora generalnego).

([371]) Sekcja 3 lit. d) pkt (iii)–(iv) rozporządzenia wykonawczego 14086 i § 201.7 lit. d) zarządzenia prokuratora generalnego.

([372]) Sekcja 3 lit. d) pkt (i) ppkt D rozporządzenia wykonawczego 14086 i § 201.9 zarządzenia prokuratora generalnego.

([373]) Sekcja 3 lit. d) pkt (iv) rozporządzenia wykonawczego 14086 i § 201.7 lit. d) zarządzenia prokuratora generalnego. Zob. również wyrok w sprawie Bumap/Stany Zjednoczone, 252 U.S. 512, 515 (1920), w którym potwierdzono długoletnią zasadę prawa amerykańskiego, zgodnie z którą uprawnienie do usunięcia jest zależne od uprawnienia do powoływania (co zostało również przypomniane przez Biuro Radców Prawnych Departamentu Sprawiedliwości w Konstytucyjnym oddzieleniu władzy między Prezydentem a Kongresem, 20 Op. O.L.C.). 124, 166 (1996)).

(188) Wnioski składane do Sądu Odwoławczego ds. Ochrony Danych są rozpatrywane przez panel składający się z trzech sędziów, w tym z prezesa sądu, którzy muszą postępować zgodnie z kodeksem postępowania sędziów amerykańskich ([374]). Każdy panel wspiera rzecznik specjalny ([375]), który ma dostęp do wszystkich informacji dotyczących danej sprawy, w tym informacji niejawnych ([376]). Rola rzecznika specjalnego polega na dopilnowaniu, aby interesy skarżącego były odpowiednio reprezentowane i aby panel Sądu Odwoławczego ds. Ochrony Danych był dobrze poinformowany o wszystkich istotnych okolicznościach prawnych i faktycznych ([377]). Aby uzyskać więcej informacji na temat wniosku o kontrolę złożonego przez osobę fizyczną do Sądu Odwoławczego ds. Ochrony Danych i móc zająć stanowisko w tej sprawie, rzecznik specjalny może zwrócić się do skarżącego o przekazanie dodatkowych informacji, kierując do niego pytania na piśmie ([378]).

(189) Sąd Odwoławczy ds. Ochrony Danych przeprowadza przegląd ustaleń dokonanych przez Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych (zarówno pod kątem tego, czy doszło do naruszenia obowiązującego prawa amerykańskiego, jak i pod kątem odpowiednich środków zaradczych) na podstawie co najmniej protokołu dochodzenia prowadzonego przez to biuro, jak również wszelkich informacji i uwag przedstawionych przez skarżącego, rzecznika specjalnego lub agencję wywiadowczą ([379]). Panel Sądu Odwoławczego ds. Ochrony Danych ma dostęp do wszystkich informacji niezbędnych do przeprowadzenia kontroli, które to informacje może uzyskać za pośrednictwem Biura Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych (panel może na przykład zwrócić się do tego biura o uzupełnienie dokumentacji o dodatkowe informacje lub ustalenia faktyczne, jeżeli jest to niezbędne do przeprowadzenia kontroli) ([380]).

(190) Przeprowadzając kontrolę, Sąd Odwoławczy ds. Ochrony Danych może 1) stwierdzić, że nie ma żadnych dowodów wskazujących na to, że prowadzone były działania w zakresie rozpoznania radioelektronicznego, które obejmowały dane osobowe skarżącego, 2) stwierdzić, że ustalenia Biura Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych są prawidłowe pod względem prawnym i poparte istotnymi dowodami, lub 3) dokonać swoich własnych ustaleń, jeżeli nie zgadza się z ustaleniami tego biura (w kwestii tego, czy doszło do naruszenia obowiązującego prawa amerykańskiego, lub w kwestii odpowiednich środków zaradczych) ([381]).

([374]) Sekcja 3 lit. d) pkt (i) ppkt B rozporządzenia wykonawczego 14086 i § 201.7 lit. a)–c) zarządzenia prokuratora generalnego. Biuro Ochrony Prywatności i Wolności Obywatelskich przy Departamencie Sprawiedliwości, które odpowiada za udzielanie wsparcia administracyjnego Sądowi Odwoławczemu ds. Ochrony Danych i rzecznikom specjalnym (zob. § 201.5 zarządzenia prokuratora generalnego), wybiera w systemie rotacyjnym trzyosobowy panel, dopilnowując przy tym, aby w skład każdego panelu wchodził co najmniej jeden sędzia mający wcześniejsze doświadczenie orzecznicze (w przypadku gdy żaden z sędziów wchodzących w skład panelu nie ma takiego doświadczenia, Biuro Ochrony Prywatności i Wolności Obywatelskich jako pierwszego sędziego wybiera prezesa sądu).

([375]) § 201.4 zarządzenia prokuratora generalnego. Prokurator generalny – w porozumieniu z sekretarzem handlu, Dyrektorem Krajowych Służb Wywiadowczych i PCLOB – wybiera co najmniej dwóch rzeczników specjalnych na dwie odnawialne kadencje. Rzecznicy specjalni muszą mieć odpowiednie doświadczenie w dziedzinie prawa dotyczącego prywatności i bezpieczeństwa narodowego, muszą być doświadczonymi adwokatami i aktywnymi członkami palestry o nieposzlakowanej opinii oraz muszą być należycie uprawnieni do wykonywania zawodu. Ponadto w chwili ich pierwotnego powołania nie mogą oni mieć historii zatrudnienia w strukturach władzy wykonawczej w ciągu ostatnich dwóch lat. Na potrzeby rozpatrzenia wniosku prezes sądu wybiera rzecznika specjalnego, którego zadaniem jest wspieranie panelu, zob. § 201.8 lit. a) zarządzenia prokuratora generalnego.

([376]) § 201.8 lit. c) i § 201.11 zarządzenia prokuratora generalnego.

([377]) Sekcja 3 lit. d) pkt (i) ppkt C rozporządzenia wykonawczego 14086 i § 201.8 lit. e) zarządzenia prokuratora generalnego. Rzecznik specjalny nie pełni funkcji przedstawiciela skarżącego ani nie pozostaje w relacji adwokat-klient ze skarżącym.

([378]) Zob. § 201.8 lit. d) i e) zarządzenia prokuratora generalnego. Takie pytania są najpierw analizowane przez Biuro Ochrony Prywatności i Wolności Obywatelskich w porozumieniu z odpowiednią jednostką Wspólnoty Wywiadowczej w celu zidentyfikowania i wyłączenia wszelkich informacji niejawnych, poufnych lub chronionych, zanim pytania te zostaną przekazane skarżącemu. Dodatkowe informacje otrzymane przez rzecznika specjalnego w odpowiedzi na takie pytania uwzględnia się w uwagach przekazywanych Sądowi Odwoławczemu ds. Ochrony Danych przez rzecznika specjalnego.

([379]) Sekcja 3 lit. d) pkt (i) ppkt D rozporządzenia wykonawczego 14086.

([380]) Sekcja 3 lit. d) pkt (iii) rozporządzenia wykonawczego 14086 i § 201.9 lit. b) zarządzenia prokuratora generalnego.

([381]) Sekcja 3 lit. d) pkt (i) ppkt E rozporządzenia wykonawczego 14086 i § 201.9 lit. c)–e) zarządzenia prokuratora generalnego. Zgodnie z definicją „odpowiednich środków zaradczych" zawartą w sekcji 4 lit. a) rozporządzenia wykonawczego 14086 Sąd Odwoławczy ds. Ochrony Danych musi uwzględnić „sposób, w jaki zwyczajowo zaradzono stwierdzonym naruszeniu" przy podejmowaniu decyzji w sprawie środka zaradczego w celu pełnego zaradzenia naruszeniu, tj. Sąd Odwoławczy ds. Ochrony Danych rozważy między innymi, w jaki sposób podobne problemy związane z przestrzeganiem przepisów zostały w przeszłości usunięte, aby zapewnić skuteczność i stosowność środka zaradczego.

(191) We wszystkich przypadkach Sąd Odwoławczy ds. Ochrony Danych wydaje orzeczenie na piśmie, przyjęte większością głosów. Jeżeli w wyniku kontroli ujawnione zostanie naruszenie obowiązujących przepisów, w orzeczeniu należy określić wszelkie odpowiednie środki zaradcze, które obejmują usunięcie bezprawnie zgromadzonych danych, usunięcie wyników nieprawidłowo przeprowadzonych zapytań, ograniczenie dostępu do danych zgromadzonych zgodnie z prawem do odpowiednio przeszkolonego personelu lub wycofanie sprawozdań służb wywiadowczych zawierających dane, które zostały pozyskane bez upoważnienia prawnego lub które były rozpowszechniane niezgodnie z prawem ([382]). Orzeczenie Sądu Odwoławczego ds. Ochrony Danych jest wiążące i ostateczne w odniesieniu do wniesionej do niego skargi ([383]). Ponadto, jeżeli w wyniku kontroli ujawnione zostanie naruszenie ze strony jakiegokolwiek organu podlegającego nadzorowi Sądu ds. Kontroli Wywiadu, Sąd Odwoławczy ds. Ochrony Danych musi również przedstawić niejawne sprawozdanie asystentowi prokuratora generalnego ds. bezpieczeństwa narodowego, który z kolei jest zobowiązany do zgłoszenia niezgodności Sądowi ds. Kontroli Wywiadu, który może podjąć dalsze czynności egzekucyjne (zgodnie z procedurą opisaną w motywach 173–174) ([384]).

(192) Każde orzeczenie panelu Sądu Odwoławczego ds. Ochrony Danych przekazuje się Biuru Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych ([385]). W przypadkach, w których kontrola prowadzona przez Sąd Odwoławczy ds. Ochrony Danych została wszczęta na podstawie wniosku skarżącego, organ krajowy informuje skarżącego, że sąd ten zakończył przeprowadzanie kontroli i że „kontrola nie wykazała żadnych naruszeń objętych zakresem albo [że] Sąd Odwoławczy ds. Ochrony Danych wydał orzeczenie nakazujące wdrożenie odpowiednich środków zaradczych" ([386]). Biuro Ochrony Prywatności i Wolności Obywatelskich przy DoJ prowadzi rejestr wszystkich informacji poddanych kontroli przez Sąd Odwoławczy ds. Ochrony Danych i wszystkich wydanych orzeczeń, który to rejestr zostaje udostępniony przyszłym panelom tego sądu jako niewiążący precedens ([387]).

(193) DoC jest również zobowiązany do prowadzenia rejestru w odniesieniu do każdego skarżącego, który złożył skargę ([388]). Aby zwiększyć przejrzystość, DoC musi co najmniej co pięć lat kontaktować się z odpowiednimi agencjami wywiadowczymi w celu zweryfikowania, czy informacje dotyczące kontroli przeprowadzonej przez Sąd Odwoławczy ds. Ochrony Danych zostały odtajnione ([389]). Jeżeli tak, osoba fizyczna zostanie powiadomiona o tym, że takie informacje mogą być dostępne zgodnie z obowiązującym prawem (tj. że osoba ta może złożyć wniosek o uzyskanie dostępu do tych informacji na podstawie ustawy o swobodnym dostępie do informacji, zob. motyw 199).

(194) Ponadto prawidłowe funkcjonowanie tego mechanizmu dochodzenia roszczeń będzie podlegało regularnej i niezależnej ocenie. Dokładniej rzecz ujmując, zgodnie z rozporządzeniem wykonawczym 14086 funkcjonowanie mechanizmu dochodzenia roszczeń podlega corocznemu przeglądowi przez PCLOB, który jest niezależnym organem (zob. motyw 110) ([390]). W ramach tego przeglądu PCLOB oceni m.in., czy Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych i Sąd Odwoławczy ds. Ochrony Danych rozpatrzyli skargi w odpowiednim terminie; czy uzyskali pełny dostęp do niezbędnych informacji; czy materialne zabezpieczenia przewidziane w rozporządzeniu wykonawczym 14086 zostały prawidłowo uwzględnione w procesie przeglądu oraz czy Wspólnota Wywiadowcza zastosowała się do wszystkich ustaleń dokonanych przez Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych i Sąd Odwoławczy ds. Ochrony Danych. PCLOB sporządzi sprawozdanie z wyniku swojego przeglądu, skierowane do Prezydenta, prokuratora generalnego, Dyrektora Krajowych Służb Wywiadowczych, szefów agencji wywiadowczych, Biura Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych i kongresowych komisji ds. wywiadu, które zostanie upublicznione również w wersji jawnej, jak również zostanie uwzględnione w okresowym przeglądzie funkcjonowania niniejszej decyzji, który zostanie przeprowadzony przez Komisję. Prokurator generalny, Dyrektor Krajowych Służb Wywiadowczych, Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych i szefowie agencji wywiadowczych są zobowiązani do wdrożenia lub uwzględnienia w inny sposób wszystkich zaleceń przedstawionych w takich sprawozdaniach. Oprócz tego PCLOB przeprowadzi coroczną certyfikację publiczną w celu ustalenia, czy mechanizm dochodzenia roszczeń jest wykorzystywany do rozpatrywania skarg zgodnie z wymogami określonymi w rozporządzeniu wykonawczym 14086.

([382]) Sekcja 4 lit. a) rozporządzenia wykonawczego 14086.

([383]) Sekcja 3 lit. d) pkt (ii) rozporządzenia wykonawczego 14086 i § 201.9 lit. g) zarządzenia prokuratora generalnego. Ponieważ decyzja Sądu Odwoławczego ds. Ochrony Danych jest ostateczna i wiążąca, żadna inna instytucja/organ wykonawczy lub administracyjny (w tym Prezydent Stanów Zjednoczonych) nie może jej uchylić. Potwierdziło to również orzecznictwo Sądu Najwyższego, w którym wyjaśniono, że delegując wyjątkową odpowiedzialność prokuratora generalnego w ramach struktury władzy wykonawczej do wydawania wiążących decyzji na niezależny organ, prokurator generalny odmawia sobie w jakikolwiek sposób zdolności wywarcia decydującego wpływu na ten organ (zob. United States ex rel. Accardi/Shaughnessy, 347 U.S. 260 (1954)).

([384]) Sekcja 3 lit. d) pkt (i) ppkt F rozporządzenia wykonawczego 14086 i § 201.9 lit. i) zarządzenia prokuratora generalnego.

([385]) § 201.9 lit. h) zarządzenia prokuratora generalnego.

([386]) Sekcja 3 lit. d) pkt (i) ppkt H rozporządzenia wykonawczego 14086 i § 201.9 lit. h) zarządzenia prokuratora generalnego. Jeżeli chodzi o charakter zgłoszenia, zob. sekcja 201.9 lit. h) pkt 3 zarządzenia prokuratora generalnego.

([387]) § 201.9 lit. j) zarządzenia prokuratora generalnego.

([388]) Sekcja 3 lit. d) pkt (v) ppkt A rozporządzenia wykonawczego 14086.

([389]) Sekcja 3 lit. d) pkt (v) rozporządzenia wykonawczego 14086.

([390]) Sekcja 3 lit. e) rozporządzenia wykonawczego 14086. Zob. również https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf

(195) Oprócz szczególnego mechanizmu dochodzenia roszczeń ustanowionego na mocy rozporządzenia wykonawczego 14086 wszystkim osobom fizycznym (niezależnie od obywatelstwa lub miejsca pobytu) dostępne są również środki dochodzenia roszczeń przed amerykańskimi sądami powszechnymi ([391]).

(196) W szczególności w ustawie o kontroli wywiadu i powiązanej ustawie przewidziano możliwość wytoczenia powództwa cywilnego przez osoby fizyczne o odszkodowanie pieniężne przeciwko Stanom Zjednoczonym, w przypadku gdy informacje na ich temat zostały bezprawnie i umyślnie wykorzystane lub ujawnione ([392]); pozwania amerykańskich urzędników rządowych działających we własnym imieniu o odszkodowanie pieniężne ([393]) oraz zakwestionowania legalności dozoru (i wystąpienia o ograniczenie rozpowszechniania informacji), w przypadku gdy rząd zamierza wykorzystać lub ujawnić jakiekolwiek informacje uzyskane lub pochodzące z dozoru elektronicznego przeciwko danej osobie w postępowaniu sądowym lub administracyjnym w Stanach Zjednoczonych ([394]). Mówiąc bardziej ogólnie, jeżeli rząd zamierza wykorzystywać informacje uzyskane podczas działań wywiadowczych przeciwko podejrzanemu w postępowaniu karnym, w wymogach konstytucyjnych i ustawowych ([395]) przewidziane są obowiązki ujawnienia określonych informacji, tak aby oskarżony mógł zakwestionować legalność gromadzenia i wykorzystywania dowodów przez rząd.

(197) Ponadto istnieje szereg konkretnych możliwości uzyskania ochrony prawnej przeciwko urzędnikom rządowym ze względu na bezprawny dostęp administracji rządowej do danych osobowych lub ich bezprawne wykorzystanie przez administrację rządową, w tym rzekomo do celów bezpieczeństwa narodowego (tj. ustawa o oszustwach i nadużyciach komputerowych ([396]); ustawa o ochronie danych w łączności elektronicznej ([397]) oraz ustawa o prawie do prywatności w kwestiach finansowych ([398])). Wszystkie te kroki prawne dotyczą określonych danych, celów lub rodzajów dostępu (np. zdalnego dostępu za pomocą komputera i internetu) i można z nich skorzystać pod pewnymi warunkami (np. celowe/umyślne postępowanie, postępowanie wykraczające poza kompetencje, powstała szkoda).

(198) W ustawie o postępowaniu administracyjnym ([399]) przewiduje się bardziej ogólną możliwość dochodzenia roszczeń, zgodnie z którą „każda osoba doznająca krzywdy w świetle prawa w wyniku działania agencji lub dotknięta negatywnymi skutkami takiego działania lub poszkodowana w wyniku działań prowadzonych przez agencję" może wystąpić o kontrolę sądową ([400]). Obejmuje to możliwość wystąpienia do sądu o „uznanie za bezprawne i uchylenie działań, ustaleń i wniosków agencji, w przypadku których okazało się, że są […] arbitralne, nieprzemyślane, stanowią nadużycie uprawnień lub w inny sposób są niezgodne z prawem" ([401]). Na przykład w 2015 r. federalny sąd apelacyjny orzekł w przedmiocie roszczenia na podstawie ustawy o postępowaniu administracyjnym, że hurtowe gromadzenie telefonicznych metadanych przez rząd Stanów Zjednoczonych nie jest dozwolone na mocy sekcji 501 ustawy o kontroli wywiadu ([402]).

([391]) Aby uzyskać dostęp do tych środków, należy wykazać legitymację procesową. Norma ta, która ma zastosowanie do wszystkich osób fizycznych niezależnie od ich narodowości, wywodzi się z wymogu istnienia „sprawy lub sporu" (ang. *case or controversy*) z art. III konstytucji USA. Zdaniem Sądu Najwyższego wymóg ten obejmuje następujące przesłanki: 1) osoba fizyczna doznała „faktycznej szkody" (tj. konkretnej, specyficznej i rzeczywistej lub nieuchronnej szkody dotyczącej interesu prawnie chronionego), 2) istnieje związek przyczynowy między szkodą i zachowaniem zaskarżonym przed sądem oraz 3) prawdopodobne jest (nie jest spekulacją), że korzystne orzeczenie sądu pozwoli wyeliminować tę szkodę (zob. Lujan/Defenders of Wildlife, t. 504 rejestru United States Reports, s. 555 (1992)).

([392]) Tytuł 18 § 2712 U.S.C.

([393]) Tytuł 50 § 1810 U.S.C.

([394]) Tytuł 50 § 1806 U.S.C.

([395]) *Zob*., odpowiednio, Brady/Maryland, t. 373 rejestru United States Reports, s. 83 (1963) i ustawa Jencksa, tytuł 18 § 3500 U.S.C.

([396]) Tytuł 18 § 1030 U.S.C.

([397]) Tytuł 18 §§ 2701–2712 U.S.C.

([398]) Tytuł 12 § 3417 U.S.C.

([399]) Tytuł 5 § 702 U.S.C.

([400]) Zasadniczo przedmiotem kontroli sądowej może być wyłącznie „końcowe" działanie agencji, a nie jej „wstępne, procesowe lub pośrednie" działanie. Zob. tytuł 5 § 704 U.S.C.

([401]) Tytuł 5 § 706 ust. 2 pkt A U.S.C.

([402]) ACLU/Clapper, 785 F.3d 787 (2d Cir. 2015), program hurtowego gromadzenia danych telefonicznych, zaskarżony w tych sprawach, został zakończony na mocy amerykańskiej ustawy o wolności w 2015 r.

(199) Ponadto oprócz środków dochodzenia roszczeń, o których mowa w motywach 176–198, każda osoba fizyczna ma prawo uzyskać dostęp do istniejących rejestrów agencji federalnej na podstawie ustawy o dostępie do informacji publicznej, w tym jeżeli rejestry te zawierają dane osobowe tej osoby fizycznej ([403]). Uzyskanie takiego dostępu może również ułatwić wnoszenie spraw do sądów powszechnych, w tym wykazywanie legitymacji procesowej. Agencje mogą zachować informacje, które wchodzą w zakres zamkniętej listy pewnych wyjątków, obejmujących dostęp do informacji niejawnych dotyczących bezpieczeństwa narodowego i informacji dotyczących badania egzekwowania prawa ([404]), lecz skarżący, którzy nie są usatysfakcjonowani odpowiedzią, mogą ją zaskarżyć, wnosząc o kontrolę administracyjną i, następnie, sądową (przed sądami federalnymi) ([405]).

(200) Z powyższego wynika, że gdy organy ścigania i organy bezpieczeństwa narodowego Stanów Zjednoczonych uzyskują dostęp do danych osobowych objętych zakresem niniejszej decyzji, dostęp taki jest regulowany ramami prawnymi które określają warunki, na jakich dostęp ten może mieć miejsce, i zapewniają ograniczenie dostępu do danych i ich dalszego wykorzystywania do tego, co jest niezbędne i proporcjonalne do realizowanego celu interesu publicznego. Na te zabezpieczenia mogą powołać się osoby fizyczne, którym przysługują prawa do skutecznego dochodzenia roszczeń.

4. **WNIOSEK**

(201) Komisja uważa, że Stany Zjednoczone – za pośrednictwem zasad wydanych przez DoC Stanów Zjednoczonych – zapewniają stopień ochrony danych osobowych przekazywanych z Unii do certyfikowanych podmiotów w Stanach Zjednoczonych na podstawie ram ochrony danych UE–USA, który zasadniczo odpowiada stopniowi ochrony zagwarantowanemu w rozporządzeniu (UE) 2016/679.

(202) Ponadto Komisja stwierdza, że zobowiązania w zakresie przejrzystości oraz zarządzanie DPF przez DoC gwarantują skuteczne stosowanie zasad. Oprócz tego mechanizmy nadzoru i możliwości dochodzenia roszczeń przewidziane w prawie Stanów Zjednoczonych – rozumiane jako całość – zapewniają możliwość identyfikowania przypadków naruszenia przepisów o ochronie danych i w praktyce nakładania kar za te naruszenia oraz oferują osobom, których dane dotyczą, możliwość skorzystania ze środków ochrony prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych, a także – ostatecznie – sprostowania lub usunięcia takich danych.

(203) Co więcej, na podstawie dostępnych informacji na temat amerykańskiego porządku prawnego, w tym informacji zawartych w załącznikach VI i VII, Komisja uważa, że wszelkie ingerencje w interes publiczny, w szczególności do celów ścigania przestępstw oraz bezpieczeństwa narodowego, jakich dopuszczają się amerykańskie organy publiczne w odniesieniu do praw podstawowych osób fizycznych, których dane osobowe są przekazywane z Unii do Stanów Zjednoczonych na podstawie ram ochrony danych UE–USA, będą ograniczać się do tego, co jest ściśle niezbędne do osiągnięcia danego uzasadnionego celu, oraz że istnieje skuteczna ochrona prawna przed takimi ingerencjami. W świetle powyższych ustaleń należy zatem uznać, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony w rozumieniu art. 45 rozporządzenia (UE) 2016/679, interpretowanego w świetle Karty praw podstawowych Unii Europejskiej, danych osobowych przekazywanych z Unii do podmiotów certyfikowanych na podstawie ram ochrony danych UE–USA.

(204) Biorąc pod uwagę to, że ograniczenia, zabezpieczenia i mechanizm dochodzenia roszczeń ustanowione na mocy rozporządzenia wykonawczego 14086 są zasadniczymi elementami amerykańskich ram prawnych, na których opiera się ocena Komisji, przyjęcie niniejszej decyzji jest mianowicie uzależnione od przyjęcia zaktualizowanych strategii politycznych i procedur wdrażania rozporządzenia wykonawczego 14086 przez wszystkie amerykańskie agencje wywiadowcze oraz od wskazania Unii jako kwalifikującego się podmiotu do celów mechanizmu dochodzenia roszczeń, które to przyjęcia miały odpowiednio miejsce 3 lipca 2023 r. (zob. motyw 126) i 30 czerwca 2023 r. (zob. motyw 176).

([403]) Tytuł 5 § 552 U.S.C. Podobne przepisy obowiązują na szczeblu stanowym.

([404]) Jeżeli ma to miejsce, osoba fizyczna otrzyma zazwyczaj tylko standardową odpowiedź, w której agencja odmówi potwierdzenia istnienia jakichkolwiek rejestrów tego rodzaju lub zaprzeczenia istnieniu takich rejestrów. Zob. wyrok w sprawie ACLU/CIA, 710 F.3d 422 (D.C. Cir. 2014). Kryteria i czas trwania klauzuli tajności określono w dekrecie 13526, który stanowi co do zasady, że należy ustalić konkretną datę lub zdarzenie dla odtajnienia w oparciu o okres wrażliwości informacji pod względem bezpieczeństwa narodowego, w którym to momencie informacje muszą zostać automatycznie odtajnione (zob. sekcja 1.5 rozporządzenia wykonawczego 13526).

([405]) Sąd na nowo ustala, czy udostępnienie rejestrów zostało wstrzymane zgodnie z prawem, oraz może nakazać rządowi zapewnienie dostępu do rejestrów (tytuł 5 § 552 lit. a) ust. 4 pkt B U.S.C.).

5. SKUTKI NINIEJSZEJ DECYZJI I DZIAŁANIA ORGANÓW OCHRONY DANYCH

(205) Państwa członkowskie i ich organy mają obowiązek stosować środki niezbędne do zapewnienia zgodności z aktami instytucji unijnych, ponieważ domniemywa się, że akty te są zgodne z prawem, a zatem wywołują skutki prawne do chwili ich uchylenia, stwierdzenia ich nieważności w postępowaniu o stwierdzenie nieważności lub orzeczenia o ich nieważności w następstwie wniosku o wydanie orzeczenia w trybie prejudycjalnym lub zarzutu niezgodności z prawem.

(206) Decyzja stwierdzająca odpowiedni stopień ochrony danych osobowych przyjęta przez Komisję na podstawie art. 45 ust. 3 rozporządzenia (UE) 2016/679 jest zatem wiążąca dla wszystkich organów państw członkowskich, do których jest skierowana, w tym ich niezależnych organów nadzorczych. W szczególności przekazywanie danych przez administratora lub podmiot przetwarzający w Unii certyfikowanym podmiotom w Stanach Zjednoczonych może odbywać się bez konieczności uzyskania jakiegokolwiek dodatkowego zezwolenia.

(207) Należy przypomnieć, że zgodnie z art. 58 ust. 5 rozporządzenia (UE) 2016/679 i jak wyjaśnił Trybunał Sprawiedliwości w wyroku w sprawie Schrems ([406]), jeżeli krajowy organ ochrony danych kwestionuje, w tym na podstawie skargi, zgodność wydanej przez Komisję decyzji stwierdzającej odpowiedni stopień ochrony z przysługującymi osobie fizycznej prawami podstawowymi do prywatności i ochrony danych, należy zapewnić w prawie krajowym drogę prawną umożliwiającą tej osobie podniesienie tych zarzutów przed sądem krajowym, który może być zobowiązany do wystąpienia z odesłaniem prejudycjalnym do Trybunału Sprawiedliwości ([407]).

6. MONITOROWANIE I PRZEGLĄD NINIEJSZEJ DECYZJI

(208) Zgodnie z orzecznictwem Trybunału Sprawiedliwości ([408]), a także jak wskazano w art. 45 ust. 4 rozporządzenia (UE) 2016/679, Komisja powinna ciągle monitorować istotne zmiany zachodzące w państwie trzecim po przyjęciu decyzji stwierdzającej odpowiedni stopień ochrony, aby ocenić, czy państwo trzecie nadal zapewnia zasadniczo równoważny stopień ochrony. Taka kontrola jest wymagana w każdym przypadku, gdy Komisja otrzyma informacje budzące uzasadnione wątpliwości w tym względzie.

(209) W związku z powyższym Komisja powinna na bieżąco monitorować sytuację w zakresie ram prawnych i rzeczywistej praktyki w Stanach Zjednoczonych w odniesieniu do przetwarzania danych osobowych, podlegających ocenie w niniejszej decyzji. Aby ułatwić ten proces, władze Stanów Zjednoczonych powinny niezwłocznie informować Komisję o istotnych zmianach w porządku prawnym Stanów Zjednoczonych, które mają wpływ na ramy prawne będące przedmiotem niniejszej decyzji, a także o wszelkich zmianach praktyk związanych z przetwarzaniem danych osobowych poddanych ocenie w niniejszej decyzji, zarówno w odniesieniu do przetwarzania danych osobowych przez certyfikowane podmioty w Stanach Zjednoczonych, jak i ograniczeń i zabezpieczeń dotyczących dostępu do danych osobowych przez organy publiczne.

(210) Ponadto, aby Komisja mogła skutecznie realizować funkcję monitorowania, państwa członkowskie powinny informować ją o wszelkich istotnych działaniach podejmowanych przez organy ochrony danych państw członkowskich, zwłaszcza w odniesieniu do zapytań lub skarg osób z Unii, których dane dotyczą, dotyczących przekazywania danych osobowych z Unii certyfikowanym podmiotom w Stanach Zjednoczonych. Komisja powinna być również informowana o wszelkich sygnałach świadczących o tym, że działania amerykańskich organów publicznych odpowiedzialnych za zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych, lub za bezpieczeństwo narodowe, w tym wszelkich organów nadzoru, nie gwarantują wymaganego stopnia ochrony.

([406]) Schrems, pkt 65.

([407]) Schrems, pkt 65: „W tym względzie do krajowego ustawodawcy należy ustanowienie drogi prawnej umożliwiającej krajowemu organowi nadzorczemu podniesienie zarzutów, które uważa on za zasadne, przed sądami krajowymi, po to, aby te ostatnie, jeśli podzielają wątpliwości tego organu co do ważności decyzji Komisji, wystąpiły z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w celu zbadania ważności tej decyzji".

([408]) Schrems, pkt 76.

(211) W zastosowaniu art. 45 ust. 3 rozporządzenia (UE) 2016/679 ([409]) Komisja po przyjęciu niniejszej decyzji powinna okresowo sprawdzać, czy ustalenia odnoszące się do adekwatności stopnia ochrony gwarantowanego przez Stany Zjednoczone zgodnie z DPF UE–USA są nadal faktycznie i prawnie uzasadnione. Biorąc pod uwagę to, że w szczególności w rozporządzeniu wykonawczym 14086 i zarządzeniu prokuratora generalnego nałożono wymóg utworzenia nowych mechanizmów i wdrożenia nowych zabezpieczeń, niniejsza decyzja powinna zostać poddana pierwszemu przeglądowi w ciągu jednego roku od jej wejścia w życie w celu zweryfikowania, czy wszystkie istotne elementy zostały w pełni wdrożone i czy funkcjonują one skutecznie w praktyce. Po przeprowadzeniu tego pierwszego przeglądu oraz w zależności od jego wyników Komisja, w ścisłym porozumieniu z komitetem powołanym na podstawie art. 93 ust. 1 rozporządzenia (UE) 2016/679 i Europejską Radą Ochrony Danych, podejmie decyzję w sprawie częstotliwości przyszłych przeglądów ([410]).

(212) W celu przeprowadzenia przeglądów Komisja powinna spotkać się z przedstawicielami DoC, FTC i DoT oraz – w stosownych przypadkach – z przedstawicielami innych departamentów i agencji zaangażowanych we wdrażanie DPF UE–USA oraz, w sprawach związanych z dostępem organów rządowych do danych, z przedstawicielami DoJ, Urzędu Dyrektora Krajowych Służb Wywiadowczych (w tym Biura Wolności Obywatelskich i Ochrony Prywatności), innych jednostek Wspólnoty Wywiadowczej i Sądu Odwoławczego ds. Ochrony Danych oraz rzecznikami specjalnymi. Uczestnictwo w tym spotkaniu powinno być otwarte dla przedstawicieli członków Europejskiej Rady Ochrony Danych.

(213) Przeglądy powinny uwzględniać wszystkie aspekty funkcjonowania niniejszej decyzji w odniesieniu do przetwarzania danych osobowych w Stanach Zjednoczonych, w szczególności stosowanie i wdrażanie zasad, przy czym szczególną uwagę należy poświęcić środkom ochronnym w związku z dalszym przekazywaniem danych; nowym rozstrzygnięciom w orzecznictwie w tej dziedzinie; skuteczności korzystania z praw indywidualnych; monitorowaniu i egzekwowaniu zgodności z zasadami, a także ograniczeniom i zabezpieczeniom w odniesieniu do dostępu rządu, w szczególności wdrażaniu i stosowaniu zabezpieczeń wprowadzonych rozporządzeniem wykonawczym 14086, w tym poprzez polityki i procedury opracowane przez agencje wywiadowcze; wzajemnym powiązaniom między rozporządzeniem wykonawczym 14086 a sekcją 702 ustawy o kontroli wywiadu i rozporządzeniem wykonawczym 12333; oraz skuteczności mechanizmów nadzoru i możliwości dochodzenia roszczeń (w tym funkcjonowania nowego mechanizmu dochodzenia roszczeń ustanowionego na mocy rozporządzenia wykonawczego 14086). W kontekście takich przeglądów uwaga zostanie również poświęcona współpracy między organami ochrony danych a właściwymi organami Stanów Zjednoczonych, w tym opracowaniu wytycznych i innych narzędzi interpretacyjnych dotyczących stosowania zasad, a także innych aspektów funkcjonowania ram.

(214) Na podstawie przeglądu Komisja powinna przygotować ogólnodostępne sprawozdanie, które przedłoży Parlamentowi Europejskiemu i Radzie.

7. **ZAWIESZENIE, UCHYLENIE LUB ZMIANA NINIEJSZEJ DECYZJI**

(215) W przypadku gdy z dostępnych informacji, w szczególności informacji uzyskanych w wyniku monitorowania niniejszej decyzji lub przedstawionych przez władze Stanów Zjednoczonych lub państw członkowskich, wynika, że zapewniany stopień ochrony danych przekazywanych na podstawie niniejszej decyzji może nie być już odpowiedni, Komisja powinna powiadomić o tym właściwe organy Stanów Zjednoczonych i zwrócić się o zastosowanie właściwych środków w określonym, rozsądnym terminie.

(216) Jeśli po upływie tego określonego terminu właściwe organy Stanów Zjednoczonych nie zastosują tych środków lub w inny zadowalający sposób nie wykażą, że niniejsza decyzja jest nadal oparta na odpowiednim stopniu ochrony, Komisja rozpocznie procedurę, o której mowa w art. 93 ust. 2 rozporządzenia (UE) 2016/679, w celu częściowego lub całkowitego zawieszenia lub uchylenia niniejszej decyzji.

(217) Ewentualnie Komisja rozpocznie tę procedurę w celu zmiany decyzji, zwłaszcza uzależniając przekazywanie danych od spełnienia dodatkowych warunków lub ograniczając zakres stwierdzenia odpowiedniego stopnia ochrony wyłącznie do przekazywania danych, co do których zapewniono ciągłość odpowiedniego stopnia ochrony.

([409]) Zgodnie z art. 45 ust. 3 rozporządzenia (UE) 2016/679 „[w] akcie wykonawczym przewiduje się mechanizm okresowego przeglądu [...], podczas którego uwzględnia się wszelkie mające znaczenie zmiany w państwie trzecim lub organizacji międzynarodowej".

([410]) Zgodnie z art. 45 ust. 3 rozporządzenia (UE) 2016/679 okresowy przegląd musi odbywać się „przynajmniej raz na cztery lata". Zob. również Europejska Rada Ochrony Danych, dokument w sprawie odpowiedniego stopnia ochrony, WP 254 rev.01.

(218) W szczególności Komisja powinna rozpocząć procedurę zawieszenia lub uchylania w przypadku:

a) oznak, że podmioty, które otrzymały dane osobowe z Unii na podstawie niniejszej decyzji, nie przestrzegają zasad oraz że właściwe organy ds. nadzoru i egzekwowania przepisów nie zajęły się skutecznie takimi przypadkami niezgodności;

b) oznak, że organy Stanów Zjednoczonych nie przestrzegają obowiązujących warunków i ograniczeń dostępu amerykańskich organów publicznych do danych osobowych przekazywanych zgodnie z DPF UE–USA do celów egzekwowania prawa i bezpieczeństwa narodowego; lub

c) nieskutecznego rozpatrywania skarg wnoszonych przez osoby z Unii, których dane dotyczą, w tym przez Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych lub Sąd Odwoławczy ds. Ochrony Danych.

(219) Komisja powinna również rozważyć wszczęcie procedury prowadzącej do zmiany, zawieszenia lub uchylenia niniejszej decyzji, jeżeli właściwe organy amerykańskie nie przedłożą informacji lub wyjaśnień wymaganych w związku z oceną stopnia ochrony zapewnianego w odniesieniu do danych osobowych przekazywanych z Unii do Stanów Zjednoczonych albo w odniesieniu do oceny zgodności z niniejszą decyzją. W tej kwestii Komisja powinna uwzględnić również zakres, w jakim właściwe informacje można uzyskać z innych źródeł.

(220) W należycie uzasadnionych, szczególnie pilnych przypadkach, na przykład gdyby rozporządzenie wykonawcze 14086 lub zarządzenie prokuratora generalnego zostało zmienione w taki sposób, który zmniejsza stopień ochrony opisany w niniejszej decyzji lub gdyby wskazanie przez prokuratora generalnego Unii jako kwalifikującego się podmiotu do celów mechanizmu dochodzenia roszczeń zostało wycofane, Komisja skorzysta z możliwości przyjęcia zgodnie z procedurą, o której mowa w art. 93 ust. 3 rozporządzenia (UE) 2016/679, mających natychmiastowe zastosowanie aktów wykonawczych zawieszających, uchylających lub zmieniających niniejszą decyzję.

8. **UWAGI KOŃCOWE**

(221) Europejska Rada Ochrony Danych opublikowała swoją opinię ([411]), która została uwzględniona podczas przygotowywania niniejszej decyzji.

(222) Parlament Europejski przyjął rezolucję w sprawie adekwatności ochrony zapewnianej przez ramy ochrony danych UE–USA ([412]).

(223) Środki przewidziane w niniejszej decyzji są zgodne z opinią Komitetu ustanowionego na podstawie art. 93 ust. 1 rozporządzenia (UE) 2016/679,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Do celów art. 45 rozporządzenia (UE) 2016/679 Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do podmiotów w Stanach Zjednoczonych, które są wymienione w „wykazie DPF" prowadzonym i udostępnianym publicznie przez Departament Handlu Stanów Zjednoczonych, zgodnie z załącznikiem I sekcja I pkt 3.

Artykuł 2

W każdym przypadku, gdy właściwe organy w państwach członkowskich, w celu ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, wykonują swoje uprawnienia na podstawie art. 58 rozporządzenia (UE) 2016/679 w odniesieniu do przekazywania danych, o którym mowa w art. 1 niniejszej decyzji, dane państwo członkowskie niezwłocznie informuje o tym fakcie Komisję.

([411]) Opinia 5/2023 w sprawie projektu decyzji wykonawczej Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony danych w odniesieniu do ram ochrony danych UE-USA z dnia 28 lutego 2023 r.

([412]) Rezolucja Parlamentu Europejskiego z dnia 11 maja 2023 r. w sprawie adekwatności ochrony zapewnianej przez ramy ochrony danych UE–USA (2023/2501(RSP).

Artykuł 3

1. Komisja stale monitoruje stosowanie ram prawnych, które są przedmiotem niniejszej decyzji, w tym warunków, na jakich odbywa się dalsze przekazywanie danych, wykonywanie praw indywidualnych oraz uzyskiwanie przez organy publiczne Stanów Zjednoczonych dostępu do danych przekazywanych na podstawie niniejszej decyzji, w celu ustalenia, czy Stany Zjednoczone nadal zapewniają odpowiedni stopień ochrony, o którym mowa w art. 1.

2. Państwa członkowskie i Komisja informują się nawzajem o przypadkach, w których wydaje się, że organy w Stanach Zjednoczonych posiadające ustawowe uprawnienia do egzekwowania zasad przedstawionych w załączniku I nie wdrożyły skutecznych mechanizmów wykrywania i nadzoru umożliwiających identyfikowanie przypadków naruszenia zasad określonych w załączniku I faktyczne nakładanie kar za takie naruszenia.

3. Państwa członkowskie i Komisja informują się nawzajem o wszelkich przesłankach wskazujących, że ingerencje organów publicznych Stanów Zjednoczonych, które odpowiadają za zapewnienie bezpieczeństwa narodowego, egzekwowanie prawa lub realizację innych celów interesu publicznego, w prawo osób fizycznych do ochrony ich danych osobowych wykraczają poza to, co jest niezbędne i proporcjonalne, lub że nie zapewniono żadnej skutecznej ochrony prawnej przed takimi ingerencjami.

4. Po roku od dnia powiadomienia państw członkowskich o wydaniu niniejszej decyzji, a następnie z częstotliwością, o której Komisja zdecyduje w ścisłym porozumieniu z komitetem powołanym na podstawie art. 93 ust. 1 rozporządzenia (UE) 2016/679 i Europejską Radą Ochrony Danych, Komisja ocenia ustalenie, o którym mowa w art. 1 ust. 1, na podstawie wszystkich dostępnych informacji, w tym informacji otrzymanych w ramach przeglądu przeprowadzanego wspólnie z właściwymi organami Stanów Zjednoczonych.

5. Jeżeli Komisja wejdzie w posiadanie dowodów na to, że odpowiedni stopień ochrony nie jest już zapewniony, powiadamia o tym właściwe organy Stanów Zjednoczonych. W razie potrzeby Komisja postanowi o zawieszeniu, zmianie albo uchyleniu niniejszej decyzji albo o ograniczeniu jej zakresu, zgodnie z art. 45 ust. 5 rozporządzenia (UE) 2016/679. Komisja może również przyjąć taką decyzję, jeżeli brak współpracy ze strony rządu Stanów Zjednoczonych nie pozwala Komisji ustalić, czy Stany Zjednoczone nadal zapewniają odpowiedni stopień ochrony.

Artykuł 4

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 10 lipca 2023 r.

W imieniu Komisji
Didier REYNDERS
Członek Komisji

ZAŁĄCZNIK I

ZASADY RAMOWE OCHRONY DANYCH UE–USA WYDANE PRZEZ DEPARTAMENT HANDLU STANÓW ZJEDNOCZONYCH

I. OGÓLNY ZARYS

1. Chociaż Stany Zjednoczone i Unia Europejska („UE") podzielają zaangażowanie w podniesienie poziomu ochrony prywatności, praworządności i uznania znaczenia transatlantyckich przepływów danych dla naszych obywateli, gospodarek i społeczeństw, to Stany Zjednoczone mają inne podejście do ochrony prywatności niż UE. Stany Zjednoczone stosują podejście sektorowe, które polega na połączeniu ustawodawstwa, regulacji i samoregulacji. Departament Handlu Stanów Zjednoczonych („departament") wydaje zasady ramowe ochrony danych UE–USA, w tym zasady uzupełniające (zwane łącznie „zasadami") oraz załącznik I do zasad („załącznik I"), zgodnie ze swoim uprawnieniem na mocy prawa stanowionego do ułatwiania, wspierania i rozwijania handlu międzynarodowego (tytuł 15 § 1512 U.S.C.). Zasady te zostały opracowane w porozumieniu z Komisją Europejską („Komisja"), przedstawicielami przemysłu i innymi zainteresowanymi stronami w celu ułatwienia handlu między Stanami Zjednoczonymi a UE. Zasady te stanowią kluczowy element ram ochrony danych UE–USA („DPF UE–USA") i zapewniają podmiotom w Stanach Zjednoczonych niezawodny mechanizm przekazywania danych osobowych z UE do Stanów Zjednoczonych, przy jednoczesnym zagwarantowaniu osobom, których dane dotyczą, pochodzącym z UE, że nadal będą mogły korzystać ze skutecznych gwarancji i ochrony zgodnie z wymogami prawodawstwa europejskiego w odniesieniu do przetwarzania ich danych osobowych, jeżeli przekazano je do państw trzecich. Zasady te są przeznaczone do wyłącznego użytku kwalifikujących się amerykańskich podmiotów otrzymujących dane osobowe z UE w celu zakwalifikowania ich do DPF UE–USA, a zatem przyznania im przywilejów przysługujących na mocy decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony ([1]). Zasady nie mają wpływu na stosowanie rozporządzenia (UE) 2016/679 („ogólne rozporządzenie o ochronie danych" lub „RODO") ([2]), które ma zastosowanie do przetwarzania danych osobowych w państwach członkowskich UE. Zasady nie ograniczają też obowiązków w zakresie prywatności, które mają zastosowanie na mocy prawa Stanów Zjednoczonych.

2. Aby móc skorzystać z DPF UE–USA w celu uzyskania danych osobowych z UE, podmiot musi dokonać samocertyfikacji zobowiązującej go do przestrzegania zasad w departamencie (lub wobec przez niego wyznaczonej jednostki). Chociaż decyzja podmiotu o dołączeniu do DPF UE–USA jest zatem całkowicie dobrowolna, skuteczne przestrzeganie zasad jest obowiązkowe: podmioty, które dokonają samocertyfikacji w departamencie i publicznie zadeklarują swoje zobowiązanie do przestrzegania zasad, muszą ich w pełni przestrzegać. Aby dołączyć do DPF UE–USA, podmiot musi: a) podlegać uprawnieniom dochodzeniowym i wykonawczym Federalnej Komisji Handlu („FTC"), Departamentu Transportu USA („DoT") lub innego organu ustawowego, który skutecznie zapewni przestrzeganie zasad (*wykaz innych amerykańskich organów ustawowych uznanych przez UE można w przyszłości dołączyć jako załącznik*); b) publicznie zadeklarować swoje zobowiązanie do przestrzegania zasad; c) publicznie ujawnić swoją politykę ochrony prywatności zgodną z tymi zasadami; oraz d) w pełni je wdrożyć ([3]). Nieprzestrzeganie zasad przez podmiot może być egzekwowane przez FTC na mocy sekcji 5 ustawy o Federalnej Komisji Handlu (FTC), w której zakazano nieuczciwych lub wprowadzających w błąd działań w ramach wymiany handlowej lub mających wpływ na wymianę handlową (tytuł 15 § 45 U.S.C.); przez DoT na podstawie tytułu 49 § 41712 U.S.C., w którym zakazuje się przewoźnikowi lub pośrednikowi sprzedaży biletów stosowania nieuczciwych lub wprowadzających w błąd praktyk w sprzedaży usług transportu lotniczego lub sprzedaży transportu lotniczego; lub na mocy innych przepisów ustawowych lub wykonawczych, w których zakazano takich działań.

([1]) Jeśli decyzja Komisji w sprawie adekwatności ochrony przewidzianej w DPF UE–USA ma zastosowanie do Islandii, Liechtensteinu i Norwegii, DPF UE–USA obejmie zarówno UE, jak i te trzy kraje. Z tego względu odniesienia do UE i jej państw członkowskich należy rozumieć jako obejmujące Islandię, Liechtenstein i Norwegię.

([2]) 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 danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

([3]) Zasady ramowe Tarczy Prywatności UE–USA zostały zmienione i zastąpione „zasadami ramowymi ochrony danych UE–USA". (*Zob*. zasada uzupełniająca dotycząca samocertyfikacji).

3. Departament będzie prowadził i publicznie udostępniał oficjalny wykaz amerykańskich podmiotów, które dokonały samocertyfikacji w departamencie i zadeklarowały swoje zobowiązanie do przestrzegania zasad („wykaz podmiotów objętych DPF"). Przywileje wynikające z DPF UE–USA przysługują od dnia, w którym departament umieści podmiot w wykazie DPF. Departament usunie z wykazu DPF te podmioty, które dobrowolnie wycofają się z DPF UE–USA lub które nie dokonają corocznej ponownej certyfikacji w departamencie; podmioty te muszą albo nadal stosować zasady do danych osobowych, które otrzymały zgodnie z DPF UE–USA, i corocznie potwierdzać departamentowi swoje zobowiązanie do stosowania zasad (tj. dopóki przechowują takie dane), zapewniać „odpowiednią" ochronę danych za pomocą innych zatwierdzonych środków (na przykład stosując umowę w pełni odzwierciedlającą wymogi odpowiednich standardowych klauzul umownych przyjętych przez Komisję), albo zwrócić lub usunąć dane. Departament usunie również z wykazu DPF te podmioty, które uporczywie nie przestrzegały zasad; podmioty te muszą zwrócić lub usunąć dane osobowe, które otrzymały zgodnie z DPF UE–USA. Usunięcie podmiotu z wykazu DPF oznacza, że nie może on już korzystać z przywilejów przysługujących na mocy decyzji Komisji stwierdzającej odpowiedni stopień ochrony, aby uzyskiwać dane osobowe z UE.

4. Departament będzie również prowadził i publicznie udostępniał oficjalny rejestr amerykańskich podmiotów, które wcześniej dokonały samocertyfikacji w departamencie, ale które usunięto z wykazu DPF. Departament wystosuje jasne ostrzeżenie, w którym poda, że te podmioty nie są uczestnikami DPF UE–USA; że usunięcie z wykazu DPF oznacza, iż nie mogą się one prezentować jako podmioty przestrzegające zasad DPF UE–USA ani nie mogą wygłaszać jakichkolwiek oświadczeń czy też stosować wprowadzających w błąd praktyk, które sugerowałyby ich uczestnictwo w DPF UE–USA; oraz że takie podmioty nie mogą już korzystać z przywilejów przysługujących na mocy decyzji Komisji stwierdzającej odpowiedni stopień ochrony, aby uzyskiwać dane osobowe z UE. Wobec podmiotu, który twierdzi, że nadal jest objęty DPF UE–USA, lub który podaje inne fałszywe informacje na temat swojego uczestnictwa w DPF UE–USA po jego usunięciu z wykazu DPF, FTC, DoT lub inne organy egzekwowania prawa mogą wszcząć odpowiednie postępowanie.

5. Przestrzeganie tych zasad może być ograniczone: a) w zakresie niezbędnym do wykonania orzeczenia sądowego lub do spełnienia wymogów interesu publicznego, egzekwowania prawa lub bezpieczeństwa narodowego (w tym w przypadku gdy ustawa lub rozporządzenie rządowe nakładają sprzeczne obowiązki); b) ustawą, orzeczeniem sądu lub rozporządzeniem rządu, którymi udzielono wyraźnego upoważnienia, pod warunkiem że działając na mocy jakiegokolwiek upoważnienia tego rodzaju, podmiot potrafi wykazać, że nieprzestrzeganie przez niego zasad jest ograniczone do zakresu koniecznego do zaspokojenia nadrzędnych uzasadnionych interesów wspieranych tym upoważnieniem; lub c) jeżeli na mocy RODO dopuszcza się wyjątki lub odstępstwa zgodnie z określonymi w nim warunkami, pod warunkiem że takie wyjątki lub odstępstwa stosuje się w porównywalnych okolicznościach. W tym kontekście obowiązujące w prawie amerykańskim zabezpieczenia mające na celu ochronę prywatności i wolności obywatelskich obejmują te wymagane na mocy rozporządzenia wykonawczego nr 14086 ([4]) zgodnie z określonymi w nim warunkami (w tym wymogami dotyczącymi konieczności i proporcjonalności). Zgodnie z celem zakładającym zwiększenie ochrony prywatności podmioty powinny dążyć do pełnego wdrożenia tych zasad w sposób przejrzysty, w tym przez podejmowanie działań mających na celu wskazanie w swoich politykach ochrony prywatności przypadków, w których stosowane będą wyjątki od zasad wskazane w lit. b) powyżej. Z tego samego powodu – w przypadku gdy zasady lub prawo amerykańskie dopuszczają taką możliwość – oczekuje się, że w miarę możliwości podmioty będą decydować się na wyższy poziom ochrony.

6. Po przystąpieniu do DPF UE–USA podmioty mają obowiązek stosować zasady zawsze, gdy przekazują dane osobowe zgodnie z DPF UE–USA. Podmiot, który chce rozszerzyć przywileje wynikające z DPF UE–USA na dane osobowe o zasobach ludzkich przekazywane z UE do wykorzystania w związku ze stosunkiem pracy, musi to zaznaczyć, kiedy dokonuje samocertyfikacji w departamencie, i musi spełnić wymagania podane w zasadzie uzupełniającej dotyczącej samocertyfikacji.

([4]) Rozporządzenie wykonawcze z dnia 7 października 2022 r. w sprawie poprawy zabezpieczeń dotyczących działań Stanów Zjednoczonych w zakresie rozpoznania radioelektronicznego.

7. Prawo amerykańskie będzie miało zastosowanie do wykładni i zagadnień związanych z przestrzeganiem zasad oraz odpowiednimi politykami ochrony prywatności podmiotów uczestniczących w DPF UE–USA z wyjątkiem przypadków, gdy takie podmioty zobowiązały się współpracować z organami ochrony danych UE. O ile nie stwierdzono inaczej, wszystkie przepisy zasad stosuje się, gdy są one właściwe w określonych okolicznościach.

8. Definicje:

   a. „dane osobowe" są to dane dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, wchodzące w zakres RODO, otrzymane z UE przez podmiot w Stanach Zjednoczonych i zapisane w dowolnej formie;

   b. „przetwarzanie" danych osobowych oznacza każdą operację lub każdy zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych środków, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, dostosowanie lub modyfikacja, odzyskiwanie, przeszukiwanie, wykorzystywanie, ujawnianie lub rozpowszechnianie, a także usuwanie lub niszczenie;

   c. „administrator" oznacza osobę fizyczną lub podmiot, które samodzielnie lub wspólnie z innymi podmiotami określają cele i sposoby przetwarzania danych osobowych.

9. Datą wejścia w życie zasad i załącznika I do zasad jest data wejścia w życie decyzji stwierdzającej odpowiedni stopień ochrony przez Komisję Europejską.

II. ZASADY

1. ZAWIADOMIENIE

a. Podmiot musi poinformować osoby fizyczne o:

   i. swoim uczestnictwie w DPF UE–USA i podać link do strony internetowej zawierającej wykaz DPF lub adres tej strony,

   ii. rodzajach gromadzonych danych osobowych i, w stosownych przypadkach, o amerykańskich jednostkach lub amerykańskich jednostkach zależnych podmiotu, które również przestrzegają zasad,

   iii. swoim zobowiązaniu do stosowania zasad do wszystkich danych osobowych otrzymanych z UE zgodnie z DPF UE–USA,

   iv. celach, dla których gromadzi i wykorzystuje dane osobowe dotyczące tych osób,

   v. sposobach kontaktowania się z podmiotem w razie jakichkolwiek zapytań lub skarg, w tym o wszelkich odpowiednich podmiotach w UE, które mogą odpowiadać na takie zapytania lub skargi,

   vi. rodzaju lub tożsamości stron trzecich, którym ujawnia ona dane osobowe, oraz o celach, dla których to czyni,

   vii. prawie dostępu do własnych danych osobowych, które przysługuje osobom fizycznym,

   viii. wyborach i środkach, jakie podmiot oferuje osobom fizycznym, których dane dotyczą, w celu ograniczenia wykorzystywania i ujawniania ich danych osobowych,

   ix. niezależnym organie ds. rozstrzygania sporów wyznaczonym do celów rozpatrywania skarg i zagwarantowania odpowiednich możliwości ochrony prawnej, z których osoby fizyczne mogą korzystać nieodpłatnie, i niezależnie od tego, czy jest to: 1) panel ustanowiony przez organy ochrony danych, 2) organ pozasądowego rozstrzygania sporów z siedzibą w UE lub 3) organ pozasądowego rozstrzygania sporów z siedzibą w Stanach Zjednoczonych,

   x. podleganiu uprawnieniom dochodzeniowym i wykonawczym FTC, DoT lub jakiegokolwiek innego amerykańskiego uprawnionego organu ustawowego,

   xi. możliwości wystąpienia przez osobę fizyczną – pod pewnymi warunkami – o arbitraż ([5]),

   xii. wymogu ujawnienia danych osobowych na zgodny z prawem wniosek organów publicznych, w tym w celu spełnienia wymogów bezpieczeństwa narodowego lub na potrzeby egzekwowania prawa, oraz

   xiii. swojej odpowiedzialności w razie dalszego przekazywania danych stronom trzecim.

([5]) *Zob*. np. sekcja c) zasady dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności.

b. Powiadomienie to musi być sformułowane jasno i jednoznacznie z chwilą, gdy osoby fizyczne zostały po raz pierwszy poproszone o przekazanie danych osobowych podmiotowi, lub w najbliższym możliwym terminie po zwróceniu się do tych osób o dane osobowe po raz pierwszy, ale w każdym przypadku przed użyciem przez podmiot takich danych w celu innym niż ten, w którym były one pierwotnie gromadzone lub przetwarzane przez podmiot przekazujący, lub też zanim podmiot ujawni je po raz pierwszy stronie trzeciej.

2. **WYBÓR**

a. Podmiot musi dać osobom fizycznym możliwość wyboru (tj. klauzula *opt-out*), czy dane osobowe ich dotyczące mają: (i) zostać ujawnione stronie trzeciej lub (ii) zostać wykorzystane w celu niezgodnym z celem lub celami, dla których były pierwotnie gromadzone lub na które osoba fizyczna wyraziła później zgodę. Osobom fizycznym należy zagwarantować jasne, jednoznaczne i łatwo dostępne mechanizmy dokonywania wyboru.

b. Na zasadzie odstępstwa od poprzedniego ustępu zagwarantowanie wyboru nie jest konieczne, jeżeli dane ujawnia się stronie trzeciej, która działa jako przedstawiciel upoważniony do wykonywania czynności w imieniu i zgodnie z instrukcjami podmiotu. Podmiot powinien jednak zawsze zawrzeć umowę z przedstawicielem.

c. W przypadku informacji szczególnie chronionych (tj. danych osobowych dotyczących informacji medycznych lub stanu zdrowia, pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych, członkostwa w związkach zawodowych lub danych związanych z życiem seksualnym danej osoby) podmioty muszą uzyskać wyraźną zgodę (tj. zezwolenie) osób fizycznych, jeżeli takie dane mają zostać (i) ujawnione stronie trzeciej lub (ii) użyte w celu innym niż cele, dla których były pierwotnie gromadzone lub na które osoba fizyczna wyraziła później zgodę poprzez udzielenie zezwolenia. Ponadto podmiot powinien traktować wszelkie dane osobowe przekazane przez stronę trzecią jako dane wrażliwe, w przypadku gdy strona trzecia określa i traktuje je jako wrażliwe.

3. **ODPOWIEDZIALNOŚĆ ZA DALSZE PRZEKAZYWANIE**

a. Przekazując dane osobowe stronie trzeciej działającej jako administrator, podmioty muszą stosować zasady powiadomienia i wyboru. Podmioty muszą również zawrzeć z administratorem będącym stroną trzecią umowę, która przewiduje, że dane te można przetwarzać wyłącznie do ograniczonych i określonych celów, na które osoba fizyczna wyraziła zgodę, i że odbiorca zapewni ten sam poziom ochrony co poziom wymagany zasadami oraz poinformuje podmiot, jeżeli ustali, że nie może dłużej wypełniać tego obowiązku. Umowa przewiduje, że gdy takie ustalenie zostanie dokonane, strona trzecia będąca administratorem zaprzestaje przetwarzania lub podejmuje inne właściwe uzasadnione środki w celu zaradzenia tej sytuacji.

b. Przekazując dane osobowe stronie trzeciej działającej jako przedstawiciel, podmioty muszą: (i) przekazywać takie dane wyłącznie do ograniczonych i określonych celów; (ii) upewnić się, że przedstawiciel ma obowiązek zapewnienia przynajmniej takiego samego poziomu ochrony prywatności co poziom wymagany w zasadach; (iii) podjąć zasadne i odpowiednie kroki w celu zagwarantowania, że przedstawiciel będzie efektywnie przetwarzać dane osobowe przekazane mu w sposób zgodny z zobowiązaniami podmiotu wynikającymi z zasad; (iv) nałożyć na przedstawiciela obowiązek powiadomienia podmiotu, jeżeli ustali, że nie może dłużej wypełniać swojego obowiązku polegającego na zapewnieniu takiego samego poziomu ochrony, jaki jest wymagany w zasadach; (v) na wezwanie, w tym na podstawie ppkt (iv), podjąć zasadne i odpowiednie kroki w celu zatrzymania niedozwolonego przetwarzania i naprawienia szkód z niego wynikłych; oraz (vi) na wezwanie departamentu przedstawić streszczenie lub poświadczoną kopię odpowiednich postanowień dotyczących prywatności zawartych w umowie z tym przedstawicielem.

4. **BEZPIECZEŃSTWO**

a. Podmioty tworzące, przechowujące, wykorzystujące lub rozpowszechniające dane osobowe muszą wprowadzać zasadne i odpowiednie środki ostrożności w celu ochrony ich przed utratą, niewłaściwym wykorzystaniem oraz nieuprawnionym dostępem, ujawnieniem, zmianą i zniszczeniem, biorąc w szczególności pod uwagę zagrożenia związane z przetwarzaniem danych osobowych i ich charakterem.

5. **INTEGRALNOŚĆ DANYCH I OGRANICZENIE CELU**

a. Zgodnie z zasadami dane osobowe muszą ograniczać się do danych, które są istotne do celów przetwarzania ([6]). Podmiotom nie wolno przetwarzać danych osobowych w sposób niezgodny z celami, dla których były one zbierane lub na które osoba fizyczna wyraziła później zgodę. W zakresie niezbędnym do osiągnięcia tych celów podmiot musi podjąć zasadne działania w celu zapewnienia, aby dane osobowe były zgodne ze swoim przeznaczeniem, prawidłowe, kompletne i aktualne. Podmiot musi przestrzegać zasad dopóty, dopóki przechowuje takie dane.

b. Informacje mogą być przechowywane w formie identyfikującej osobę fizyczną lub umożliwiającej jej identyfikację ([7]) jedynie tak długo, jak długo służy to celowi przetwarzania w rozumieniu pkt 5 lit a). Obowiązek ten nie uniemożliwia podmiotom przetwarzania danych osobowych przez dłuższe okresy do chwili i w zakresie, w jakim przetwarzanie takie w sposób racjonalny służy do celów archiwizacji w interesie publicznym, oraz do celów dziennikarskich, literackich i artystycznych, naukowych, badań historycznych i analizy statystycznej. W tych przypadkach przetwarzanie danych podlega pozostałym zasadom i przepisom DPF UE–USA. Podmioty powinny przyjmować zasadne i stosowne środki w celu dostosowania się do niniejszego przepisu.

6. **DOSTĘP**

a. Osoby fizyczne muszą mieć dostęp do własnych danych osobowych przechowywanych przez podmiot i możliwość poprawiania, zmieniania lub usuwania takich danych, gdy są one nieprawidłowe lub zostały przetworzone z naruszeniem zasad, z wyjątkiem przypadków, gdy obciążenie związane z udostępnianiem lub koszty udostępniania danych byłyby nieproporcjonalne w stosunku do zagrożenia dla ochrony prywatności danej osoby fizycznej, lub w przypadku gdy naruszone zostałyby prawa innych osób.

7. **OCHRONA PRAWNA, EGZEKWOWANIE PRAWA ORAZ ODPOWIEDZIALNOŚĆ**

a. Skuteczna ochrona prywatności musi obejmować solidne mechanizmy zapewniające przestrzeganie zasad, ochronę prawną osób fizycznych, które poniosły skutki nieprzestrzegania zasad, oraz konsekwencje, jakie musi ponieść dany podmiot, jeżeli nie przestrzega zasad. Takie mechanizmy muszą obejmować przynajmniej:

i. łatwo dostępne niezależne mechanizmy ochrony prawnej, dzięki którym bada się i szybko rozstrzyga skargi oraz spory poszczególnych osób fizycznych, bez konieczności ponoszenia przez nie jakichkolwiek kosztów i poprzez odniesienie do zasad, a także przyznaje odszkodowanie, w przypadku gdy przewidziano to w prawie właściwym lub w ramach inicjatywy sektora prywatnego;

ii. procedury kontrolne mające na celu sprawdzenie, że poświadczenia i zapewnienia składane przez podmioty w odniesieniu do ich praktyk ochrony prywatności są prawdziwe oraz że praktyki te zostały wdrożone zgodnie z deklaracjami, szczególnie w sprawach dotyczących nieprzestrzegania zasad; oraz

iii. zobowiązania do rozwiązania problemów wynikających z nieprzestrzegania zasad przez podmioty deklarujące, że ich przestrzegają, oraz konsekwencje ponoszone przez takie podmioty. Sankcje muszą być dostatecznie surowe, by zapewnić przestrzeganie zasad przez podmioty.

b. Podmioty i wskazane przez nie niezależne mechanizmy ochrony prawnej będą bezzwłocznie reagowały na złożone przez departament zapytania i wnioski o informacje dotyczące DPF UE–USA. Wszystkie podmioty muszą sprawnie reagować na skargi dotyczące przestrzegania zasad złożone przez organy państwa członkowskiego UE za pośrednictwem departamentu. Podmioty, które zdecydowały się na współpracę z organami ochrony danych, w tym podmioty przetwarzające dane dotyczące zasobów ludzkich, muszą bezpośrednio udzielać odpowiedzi tym organom w związku z badaniem i rozpatrywaniem skarg.

([6]) W zależności od okoliczności przykładami dopuszczalnych celów przetwarzania mogą być cele służące w sposób zasadny relacjom z klientami, zgodność i względy prawne, audyt, bezpieczeństwo i zapobieganie oszustwom, zachowanie praw podmiotu i ich obrona, lub inne cele zgodne z oczekiwaniami, jakie może mieć racjonalna osoba pod względem gromadzenia danych.

([7]) W tym kontekście, jeśli biorąc pod uwagę środki, jakimi można się racjonalnie posłużyć w celu identyfikacji (uwzględniając m.in. koszty i czas potrzebny do zidentyfikowania danej osoby oraz technologię dostępną w momencie przetwarzania danych), a także formę, w jakiej dane są zachowywane, osoba fizyczna może być racjonalnie zidentyfikowana przez podmiot lub stronę trzecią – gdyby ta osoba trzecia miała dostęp do danych – wówczas osoba fizyczna jest „możliwa do zidentyfikowania".

c. Podmioty są zobowiązane do przeprowadzenia arbitrażu w sprawie roszczeń i przestrzegania warunków określonych w załączniku I, pod warunkiem że osoba fizyczna wystąpiła o arbitraż, przekazując zawiadomienie zainteresowanemu podmiotowi oraz postępując zgodnie z procedurami i warunkami określonymi w załączniku I.

d. W kontekście dalszego przekazywania danych uczestniczący podmiot jest odpowiedzialny za przetwarzanie danych osobowych, które otrzymuje zgodnie z DPF UE–USA, a następnie przekazuje je stronie trzeciej działającej jako przedstawiciel w jej imieniu. Uczestniczący podmiot ponosi odpowiedzialność zgodnie z zasadami, jeżeli jego przedstawiciel przetwarza tego rodzaju dane osobowe w sposób niezgodny z zasadami, chyba że udowodni, iż nie jest odpowiedzialny za zdarzenie, które spowodowało szkodę.

e. Gdy podmiot stanie się przedmiotem orzeczenia sądu w związku z nieprzestrzeganiem zasad lub nakazu wydanego przez amerykański organ ustawowy (np. FTC lub DoT) wymieniony w zasadach lub w przyszłym załączniku do zasad w związku z nieprzestrzeganiem zasad, upublicznia on wszelkie istotne części sprawozdań dotyczących przestrzegania zasad lub oceny związane z DPF UE–USA, które przedłożył sądowi lub amerykańskiemu organowi sądowemu w zakresie zgodnym z wymogami poufności. Departament utworzył specjalne stanowisko ds. kontaktów z organami ochrony danych na wypadek jakichkolwiek problemów z przestrzeganiem zasad przez uczestniczące podmioty. FTC i DoT będą priorytetowo traktować zgłoszenia dotyczące nieprzestrzegania zasad przekazane przez departament i organy państwa członkowskiego UE oraz będzie terminowo dokonywać wymiany informacji na temat zgłoszeń z organami państwowymi dokonującymi zgłoszenia, z zastrzeżeniem istniejących ograniczeń poufności.

III. ZASADY UZUPEŁNIAJĄCE

1. Dane wrażliwe

a. Nie wymaga się od podmiotu uzyskania wyraźnej zgody (tj. zezwolenia) w odniesieniu do danych wrażliwych, jeżeli przetwarzanie tych danych:

i. leży w żywotnym interesie osoby, której dane dotyczą, lub innej osoby;

ii. jest konieczne do ustalenia roszczeń prawnych lub obrony;

iii. jest wymagane do udzielenia opieki zdrowotnej lub postawienia diagnozy;

iv. jest wykonywane w toku prawomocnych działań przez fundację, stowarzyszenie albo jakąkolwiek organizację non-profit prowadzącą działalność polityczną, filozoficzną, religijną lub związkową, a także pod warunkiem że przetwarzanie danych dotyczy wyłącznie członków tej jednostki albo osób mających z nią stały kontakt wynikający z celów jej działalności, a dane nie są ujawnione stronom trzecim bez zgody osób, których te dane dotyczą;

v. jest konieczne do wykonania zobowiązań podmiotu w dziedzinie prawa pracy; lub

vi. jest związane z danymi, które osoba fizyczna w sposób oczywisty ujawnia publicznie.

2. Wyjątki dziennikarskie

a. Biorąc pod uwagę konstytucyjną ochronę wolności prasy w Stanach Zjednoczonych, w przypadku gdy prawo do wolnej prasy zawarte w pierwszej poprawce do konstytucji Stanów Zjednoczonych koliduje z ochroną prywatności, interesy te w odniesieniu do działań amerykańskich obywateli i rezydentów lub podmiotów należy wyważyć na podstawie pierwszej poprawki.

b. Dane osobowe zebrane w celu ich publikacji w prasie, radiu lub telewizji albo w innej formie publicznego rozpowszechnienia materiału dziennikarskiego, niezależnie od tego, czy informacje te wykorzystano czy nie, a także informacje znajdujące się w uprzednio opublikowanym materiale rozpowszechnionym z archiwów środków masowego przekazu, nie podlegają wymaganiom zasad.

3. Odpowiedzialność pośrednia

a. Dostawcy usług internetowych, operatorzy telekomunikacyjni i inne podmioty nie podlegają odpowiedzialności w ramach zasad, gdy w imieniu innego podmiotu jedynie przekazują, kierują, przełączają lub przechowują informacje. DPF UE–USA nie powoduje odpowiedzialności pośredniej. W zakresie, w jakim podmiot działa jedynie jako kanał dla danych przekazywanych przez strony trzecie, i o ile nie decyduje on o celach oraz sposobach przetwarzania tych danych osobowych, podmiot ten nie ponosi odpowiedzialności.

4. **Przeprowadzanie badań *due diligence* oraz audytów**

a. Działania audytorów i bankierów inwestycyjnych mogą wiązać się z przetwarzaniem danych osobowych bez zgody lub wiedzy osoby fizycznej, której dane dotyczą. Jest to dozwolone w świetle zasad powiadomienia, wyboru i dostępu w przypadkach opisanych poniżej.

b. Publiczne spółki akcyjne oraz spółki o niewielkiej liczbie inwestorów, w tym uczestniczące podmioty, są regularnie poddawane audytom. Skuteczność tego rodzaju audytów, szczególnie tych dotyczących potencjalnych naruszeń, może być zagrożona w razie przedwczesnego ujawnienia. Podobnie uczestniczący podmiot, który bierze udział w potencjalnym połączeniu lub przejęciu, będzie musiał przeprowadzić badanie *due diligence* lub poddać się takiemu badaniu. Często będzie się to wiązało z gromadzeniem i przetwarzaniem danych osobowych, takich jak informacje na temat członków kadry kierowniczej wyższego szczebla oraz innych pracowników zajmujących najważniejsze stanowiska. Przedwczesne ujawnienie mogłoby zakłócić transakcję, a nawet naruszyć mające zastosowanie przepisy dotyczące papierów wartościowych. Bankierzy inwestycyjni i prawnicy biorący udział w badaniu *due diligence* lub audytorzy przeprowadzający audyt mogą przetwarzać informacje bez wiedzy osoby fizycznej tylko w takim zakresie i przez taki okres, jaki jest konieczny do spełnienia wymogów ustawowych lub wymogów interesu publicznego oraz w innych okolicznościach, w których stosowanie niniejszych zasad naruszałoby uzasadnione interesy podmiotów. Tego rodzaju uzasadnione interesy obejmują monitorowanie przestrzegania przez podmioty spoczywających na nich obowiązków prawnych i uzasadnionych operacji księgowych, a także konieczność zachowania poufności w związku z możliwymi przejęciami, połączeniami, spółkami *joint venture* albo innymi podobnymi transakcjami przeprowadzanymi przez bankierów inwestycyjnych lub audytorów.

5. **Rola organów ochrony danych**

a. Podmioty będą wypełniały swoje zobowiązanie do współpracy z organami ochrony danych w sposób opisany poniżej. W DPF UE–USA podmioty amerykańskie otrzymujące dane osobowe z UE muszą zobowiązać się do stosowania skutecznych mechanizmów w celu zapewnienia przestrzegania zasad. W szczególności zgodnie z zasadą dotyczącą ochrony prawnej, egzekwowania prawa oraz odpowiedzialności uczestniczące podmioty muszą zapewnić: a)(i) środki odwoławcze dla osób, których dane dotyczą; a)(ii) procedury kontrolne mające na celu sprawdzenie, czy dokonywane przez nie poświadczenia i zapewnienia związane z praktyką ochrony prywatności są prawdziwe; oraz a)(iii) zobowiązania polegające na zaradzeniu problemom powstałym wskutek nieprzestrzegania zasad oraz konsekwencje dla takich podmiotów. Podmiot może spełniać wymagania określone w lit. a) ppkt (i) i (iii) zasady dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności, jeżeli przestrzega wymagań określonych w niniejszym dokumencie w zakresie współpracy z organami ochrony danych.

b. Podmiot zobowiązuje się do współpracy z organami ochrony danych przez oświadczenie w zgłoszeniu samocertyfikacji na potrzeby DPF UE–USA złożonym w departamencie (*zob*. zasada uzupełniająca dotycząca samocertyfikacji), że podmiot:

i. zamierza spełnić wymóg określony w lit. a) ppkt (i) i (iii) zasady dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności przez zobowiązanie się do współpracy z organami ochrony danych;

ii. będzie współpracował z organami ochrony danych przy badaniu i rozstrzyganiu skarg wniesionych w ramach zasad; oraz

iii. będzie postępować zgodnie z poradami udzielonymi przez organy ochrony danych, w przypadku gdy organy takie uznają, że podmiot powinien podjąć szczególne działania w celu zapewnienia zgodności z zasadami, włącznie ze stosowaniem środków naprawczych lub odszkodowawczych na rzecz osób poszkodowanych z tytułu jakiegokolwiek przypadku nieprzestrzegania zasad, i przekaże organom ochrony danych pisemne potwierdzenie, iż takie działanie zostało podjęte.

c. Działanie grupy zrzeszającej organy ochrony danych

i. Współpraca ze strony organów ochrony danych będzie polegała na udzielaniu informacji i wskazówek w następujący sposób:

1. wskazówki organów ochrony danych będą przekazywane za pośrednictwem nieformalnej grupy zrzeszającej organy ochrony danych ustanowionej na poziomie UE, która między innymi pomoże zapewnić skoordynowane i spójne podejście;

2. grupa będzie przekazywać wskazówki zainteresowanym podmiotom amerykańskim w sprawie nierozstrzygniętych skarg osób fizycznych dotyczących posługiwania się danymi osobowymi przekazanymi z UE zgodnie z DPF UE–USA. Wskazówki te będą miały na celu zapewnienie prawidłowego stosowania zasad i będą obejmować wszelkie środki ochrony prawnej dla zainteresowanej osoby fizycznej lub zainteresowanych osób fizycznych, jakie organy ochrony danych uznają za właściwe;

3. grupa będzie przekazywać tego typu wskazówki w następstwie wniesienia odwołania przez zainteresowane podmioty lub w odpowiedzi na skargi otrzymane bezpośrednio od osób fizycznych na podmioty, które zobowiązały się współpracować z organami ochrony danych na potrzeby DPF UE–USA, jednocześnie zachęcając i w razie potrzeby pomagając takim osobom wykorzystać w pierwszej kolejności wewnętrzne procedury rozpatrywania skarg, które wprowadził dany podmiot;

4. wskazówki zostaną przekazane dopiero wówczas, gdy obie strony sporu miały należytą możliwość wypowiedzenia się i przedstawienia wszystkich dowodów zgodnie z własnym uznaniem. Grupa będzie starała się przekazywać wskazówki tak szybko, jak pozwala niniejszy wymóg należytej procedury. Jako ogólną zasadę przyjmuje się, że grupa będzie się starała się je przekazać w ciągu 60 dni od otrzymania skargi lub zgłoszenia, a w miarę możliwości wcześniej;

5. jeżeli grupa uzna to za stosowne, poda do publicznej wiadomości wyniki rozpatrywania otrzymanych skarg;

6. przekazywanie wskazówek za pośrednictwem grupy nie będzie skutkowało powstaniem żadnej odpowiedzialności po stronie grupy lub poszczególnych organów ochrony danych.

ii. Jak wspomniano powyżej, podmioty wybierające ten sposób rozstrzygania sporów muszą zobowiązać się do przestrzegania wskazówek organów ochrony danych. Jeżeli podmiot nie zastosuje się do wskazówek w ciągu 25 dni od ich otrzymania i nie poda zadowalającego usprawiedliwienia tego opóźnienia, grupa zawiadomi go o swoim zamiarze albo przekazania sprawy FTC, DoT lub innemu federalnemu lub stanowemu organowi Stanów Zjednoczonych posiadającemu ustawowe uprawnienia do wszczęcia postępowania w przypadku wprowadzenia w błąd lub podania fałszywych informacji, albo o zamiarze stwierdzenia, że porozumienie o współpracy zostało poważnie naruszone i musi tym samym zostać uznane za nieważne. W tym ostatnim przypadku grupa poinformuje departament, tak aby wykaz DPF mógł zostać odpowiednio zmieniony. Każdy przypadek niewypełnienia zobowiązania do współpracy z organami ochrony danych, a także przypadki nieprzestrzegania zasad będą podlegały zaskarżeniu jako praktyka wprowadzająca w błąd na mocy sekcji 5 ustawy o FTC (15 § 45 U.S.C.), 49 § 41712 U.S.C. lub innej podobnej ustawy.

d. Podmiot, który chce, aby przywileje wynikające z DPF UE–USA miały zastosowanie do danych dotyczących zasobów ludzkich przekazywanych z UE w związku ze stosunkiem pracy, musi zobowiązać się do współpracy z organami ochrony danych w zakresie tego rodzaju danych (*zob*. zasada uzupełniająca dotycząca danych o zasobach ludzkich).

e. Podmioty wybierające ten wariant będą musiały zapłacić roczną składkę, która zostanie przeznaczona na sfinansowanie kosztów operacyjnych grupy. Mogą również zostać poproszone o pokrycie koniecznych wydatków związanych z tłumaczeniami wynikających z rozpatrywania przez grupę zgłoszeń lub skarg złożonych przeciwko nim. Wysokość składki zostanie określona przez departament po konsultacji z Komisją. Poboru składki może dokonywać strona trzecia wybrana przez departament na depozytariusza środków zebranych w tym celu. Departament będzie ściśle współpracować z Komisją i organami ochrony danych w zakresie ustanowienia odpowiednich procedur dystrybucji środków zebranych w ramach poboru składki, a także innych aspektów proceduralnych i administracyjnych grupy. Departament i Komisja mogą porozumieć się co do zmiany częstotliwości pobierania składki.

6. **Samocertyfikacja**

a. Przywileje wynikające z DPF UE–USA przysługują od dnia, w którym departament umieści podmiot w wykazie DPF. Departament umieści podmiot w wykazie DPF dopiero po ustaleniu, że złożone przez niego wstępne zgłoszenie samocertyfikacji jest kompletne i usunie podmiot z tego wykazu, jeśli ten dobrowolnie się wycofa, nie dokona corocznej ponownej certyfikacji lub jeśli uporczywie nie będzie przestrzegać zasad (*zob*. zasada uzupełniająca dotycząca rozstrzygania sporów i egzekwowania prawa).

b. W celu dokonania wstępnej samocertyfikacji lub ponownej certyfikacji do celów DPF UE–USA podmiot musi każdorazowo złożyć w departamencie zgłoszenie sporządzone przez członka zarządu w imieniu podmiotu, który dokonuje samocertyfikacji lub ponownej certyfikacji, potwierdzające przestrzeganie zasad ([8]) i zawierające przynajmniej następujące dane:

([8]) Zgłoszenia musi dokonać – za pośrednictwem strony internetowej departamentu dotyczącej ram ochrony danych – przedstawiciel podmiotu upoważniony do składania oświadczeń w imieniu podmiotu i dowolnej z jednostek objętych przez podmiot obowiązkiem przestrzegania zasad.

i. nazwę amerykańskiego podmiotu, który dokonuje samocertyfikacji lub ponownej certyfikacji, a także nazwę (nazwy) wszystkich jego amerykańskich jednostek lub amerykańskich jednostek zależnych, które również przestrzegają zasad określonych przez podmiot;

ii. opis działalności podmiotu w odniesieniu do danych osobowych, które mają być otrzymywane z UE na podstawie DPF UE–USA;

iii. opis odpowiedniej obowiązującej w podmiocie polityki (polityk) ochrony prywatności dotyczącej tego typu danych osobowych obejmujący:

1. w przypadku gdy podmiot prowadzi ogólnodostępną stronę internetową – odpowiedni adres strony internetowej, na której dostępna jest polityka ochrony prywatności, lub, jeśli podmiot nie prowadzi ogólnodostępnej strony internetowej – informację, gdzie polityka ochrony prywatności jest udostępniona do wglądu publicznego; oraz

2. datę jej wdrożenia;

iv. biuro kontaktowe w ramach podmiotu odpowiednie do rozpatrywania skarg, wniosków o udostępnienie danych oraz wszelkich innych kwestii wynikających z wprowadzenia zasad ([9]), w tym:

1. (odpowiednio) imię i nazwisko (imiona i nazwiska), stanowisko (stanowiska), adres (adresy) e-mail i numer (numery) telefonu odpowiedniej osoby (osób) lub odpowiedniego biura kontaktowego (biur kontaktowych) w ramach podmiotu; oraz

2. odpowiedni amerykański adres pocztowy podmiotu;

v. określony organ ustawowy właściwy do rozpatrywania wszelkich skarg na podmiot dotyczących możliwych nieuczciwych lub wprowadzających w błąd praktyk oraz naruszenia przepisów ustawowych lub wykonawczych regulujących ochronę prywatności (wymienionych w zasadach lub w przyszłym załączniku do zasad);

vi. nazwy wszelkich programów ochrony prywatności, których podmiot jest członkiem;

vii. metodę weryfikacji (tj. samoocena; lub zewnętrzne przeglądy zgodności, w tym wskazanie strony trzeciej, która przeprowadza takie przeglądy) ([10]); oraz

viii. odpowiedni(e) niezależny(-e) mechanizm(y) ochrony prawnej, który(e) umożliwia(ją) badanie nierozstrzygniętych skarg dotyczących zasad ([11]).

c. W przypadku gdy podmiot chce, aby jego przywileje wynikające z DPF UE–USA miały także zastosowanie do informacji o zasobach ludzkich przekazywanych z UE do wykorzystania w związku ze stosunkiem pracy, może tak uczynić, gdy organowi ustawowemu wymienionemu w zasadach lub przyszłym załączniku do zasad przysługuje właściwość do rozpoznawania skarg na podmiot wynikających z przetwarzania informacji o zasobach ludzkich. Ponadto podmiot musi zaznaczyć to we wstępnym zgłoszeniu samocertyfikacji i w zgłoszeniach ponownej certyfikacji, a także zobowiązać się do współpracy z zainteresowanym organem lub zainteresowanymi organami UE zgodnie z obowiązującymi zasadami uzupełniającymi dotyczącymi odpowiednio: danych o zasobach ludzkich i roli organów ochrony danych oraz do działania zgodnie ze wskazówkami przekazanymi przez takie organy. Podmiot musi także złożyć w departamencie kopię swojej polityki ochrony prywatności w zakresie zasobów ludzkich i udzielić informacji, w jakim miejscu polityka ta jest udostępniona do wglądu dla objętych nią pracowników.

([9]) Główna „osoba do kontaktu w imieniu podmiotu" lub „członek zarządu podmiotu" nie może być osobą spoza podmiotu (np. zewnętrznym doradcą lub zewnętrznym konsultantem).

([10]) *Zob*. zasada uzupełniająca dotycząca weryfikacji.

([11]) *Zob*. zasada uzupełniająca dotycząca rozstrzygania sporów i egzekwowania prawa.

d. Departament będzie prowadzić i udostępniać publicznie wykaz podmiotów objętych DPF, które złożyły wypełnione wstępne zgłoszenie samocertyfikacji, i będzie również aktualizować ten wykaz na podstawie wypełnionych corocznych zgłoszeń ponownej certyfikacji, a także zawiadomień otrzymanych na podstawie zasady uzupełniającej dotyczącej rozstrzygania sporów i egzekwowania prawa. Tego rodzaju zgłoszenia ponownej certyfikacji muszą być składane co najmniej raz w roku; w przeciwnym razie podmiot zostanie wykreślony z wykazu DPF i pozbawiony przywilejów wynikających z DPF UE–USA. Wszystkie podmioty, które departament umieścił w wykazie DPF, muszą posiadać odpowiednie polityki prywatności, które są zgodne z zasadą powiadomienia, a także podać w tych politykach ochrony prywatności informację o tym, że przestrzegają zasad ([12]). Jeśli polityka ochrony prywatności jest dostępna na stronie internetowej podmiotu, musi znaleźć się w niej link do strony internetowej departamentu dotyczącej ram ochrony danych oraz link do strony internetowej lub formularza skargi w ramach niezależnego mechanizmu ochrony prawnej, który umożliwia rozpoznanie nierozstrzygniętych skarg dotyczących zasad bez powstania z tego tytułu kosztów dla danej osoby fizycznej.

e. Zasady mają zastosowanie niezwłocznie po samocertyfikacji. Uczestniczące podmioty, które dotychczas dokonywały samocertyfikacji zgodnie z zasadami ramowymi Tarczy Prywatności UE–USA, muszą zaktualizować swoje polityki prywatności, aby zamiast tego odnosić się do „zasad ramowych ochrony danych UE–USA". Podmioty te uwzględniają to odniesienie tak szybko, jak to możliwe, a w każdym razie nie później niż trzy miesiące od daty wejścia w życie „zasad ramowych ochrony danych UE–USA".

f. Podmiot musi objąć zobowiązaniem do stosowania zasad wszystkie dane osobowe otrzymane z UE zgodnie z DPF UE–USA. Zobowiązanie do przestrzegania zasad nie jest ograniczone czasowo w odniesieniu do danych osobowych otrzymanych w okresie, w którym podmiot korzysta z przywilejów wynikających z DPF UE–USA; jego zobowiązanie oznacza, że będzie w dalszym ciągu stosować zasady w odniesieniu do tych danych tak długo, jak będzie je przechowywać, wykorzystywać lub ujawniać, nawet jeżeli w późniejszym terminie z jakiegokolwiek powodu zrezygnuje z uczestnictwa w DPF UE–USA. Podmiot, który chce wycofać się z DPF UE–USA, musi z wyprzedzeniem powiadomić o tym departament. W zawiadomieniu tym należy również wskazać, w jaki sposób podmiot postąpi z danymi osobowymi, które otrzymał w oparciu o DPF UE–USA (tj. zachowa, zwróci lub usunie dane, a jeśli zachowa dane, zatwierdzone środki, za pomocą których zapewni ochronę danych). Podmiot, który wycofuje się z DPF UE–USA, lecz chce zachować tego rodzaju dane, musi albo corocznie potwierdzać departamentowi swoje zobowiązanie do stosowania zasad w odniesieniu do danych, albo zapewnić „odpowiednią" ochronę danych za pomocą innych zatwierdzonych środków (na przykład stosując umowę w pełni odzwierciedlającą wymogi odpowiednich standardowych klauzul umownych przyjętych przez Komisję); w przeciwnym razie podmiot musi zwrócić lub usunąć dane ([13]). Podmiot, który wycofuje się z DPF UE–USA, musi usunąć z każdej odpowiedniej polityki ochrony prywatności wszelkie odniesienia do DPF UE–USA, które sugerują, że podmiot wciąż uczestniczy w DPF UE–USA i jest uprawniony do wynikających z niego przywilejów.

([12]) Podmiot dokonujący samocertyfikacji po raz pierwszy nie może deklarować uczestnictwa w DPF UE–USA w swojej ostatecznej polityce prywatności, dopóki departament nie powiadomi go, że może to zrobić. Przy składaniu wstępnej samocertyfikacji podmiot musi przedstawić departamentowi projekt polityki prywatności, która jest zgodna z zasadami. Po ustaleniu przez departament, że wstępne zgłoszenie samocertyfikacji złożone przez podmiot jest kompletne, departament powiadomi podmiot, że powinien on sfinalizować (np. – w stosownych przypadkach – opublikować) swoją politykę prywatności zgodną z DPF UE–USA. Podmiot musi niezwłocznie powiadomić departament z chwilą, gdy odpowiednia polityka prywatności zostanie sfinalizowana; departament umieści wówczas ten podmiot w wykazie DPF.

([13]) Jeśli w momencie wycofania się podmiot zdecyduje się zachować dane osobowe, które otrzymał w oparciu o DPF UE–USA, i corocznie potwierdzać departamentowi, że nadal stosuje zasady do takich danych, podmiot musi udokumentować departamentowi raz w roku po wycofaniu się (tj. chyba że i dopóki podmiot nie zapewni „odpowiedniej" ochrony takich danych za pomocą innych zatwierdzonych środków lub zwróci lub usunie wszystkie takie dane i powiadomi o tym departament), w jaki sposób postąpił z tymi danymi osobowymi, w jaki sposób postąpi z wszelkimi danymi osobowymi, które nadal przechowuje, oraz wskazać stałą osobę odpowiedzialną za kontakty w sprawie pytań związanych z zasadami.

g. Podmiot, który przestanie istnieć jako odrębny podmiot prawny z powodu zmiany statusu spółki, takiej jak połączenie lub przejęcie, upadłość lub rozwiązanie, musi z wyprzedzeniem powiadomić o tym departament. W zawiadomieniu tym należy również wskazać, czy podmiot powstały w wyniku zmiany statusu spółki będzie (i) nadal uczestniczył w DPF UE–USA, korzystając z istniejącej samocertyfikacji; (ii) dokona samocertyfikacji jako nowy uczestnik DPF UE–USA (np. w przypadku gdy nowy podmiot lub podmiot, który kontynuuje działalność po zmianie, nie posiada jeszcze samocertyfikacji, która mogłaby być podstawą jego uczestnictwa w DPF UE–USA); lub (iii) wdroży inne zabezpieczenia, takie jak pisemna umowa, która zapewni ciągłe stosowanie zasad do wszelkich danych osobowych, które podmiot otrzymał zgodnie z DPF UE–USA i zachowa. W przypadku gdy ppkt (i), (ii) ani (iii) nie ma zastosowania, wszelkie dane osobowe otrzymane zgodnie z DPF UE–USA muszą zostać bezzwłocznie zwrócone lub usunięte.

h. Podmiot, który z jakiegokolwiek powodu wycofuje się z DPF UE–USA, musi usunąć wszelkie oświadczenia, które sugerują, że podmiot wciąż uczestniczy w DPF UE–USA lub jest uprawniony do wynikających z niego przywilejów. Znak certyfikacyjny DPF UE–USA, jeżeli jest stosowany, musi także zostać usunięty. Każde podanie do publicznej wiadomości fałszywej informacji dotyczącej przestrzegania przez podmiot zasad może stanowić podstawę wszczęcia postępowania przez FTC, DoT lub inny odpowiedni organ rządowy. Podanie fałszywych informacji departamentowi może stanowić podstawę wszczęcia postępowania na podstawie ustawy o fałszywych oświadczeniach (tytuł 18 § 1001 U.S.C.).

7. **Kontrola**

a. Podmioty muszą zapewnić procedury kontrolne pozwalające sprawdzić, czy ich poświadczenia i zapewnienia dotyczące praktyk ochrony prywatności zgodnie z DPF UE–USA są prawdziwe oraz czy praktyki te zostały wdrożone tak, jak zostało to przedstawione, oraz zgodnie z zasadami.

b. W celu spełnienia wymogów kontrolnych określonych w zasadzie dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności podmiot musi kontrolować takie poświadczenia i zapewnienia w drodze samooceny albo zewnętrznych przeglądów zgodności.

c. W przypadku gdy podmiot wybrał samoocenę, kontrola taka musi wykazać, że polityka podmiotu w zakresie ochrony prywatności dotycząca danych osobowych otrzymanych z UE jest prawidłowa, całościowa, łatwo dostępna, zgodna z zasadami oraz w pełni wdrożona (tj. że jest przestrzegana). Kontrola ta musi również wykazać, że osoby fizyczne są informowane o wszelkich wewnętrznych mechanizmach rozpatrywania skarg oraz niezależnych mechanizmach ochrony prawnej, którymi mogą posłużyć się w celu składania skarg; że podmiot stosuje odpowiednie procedury szkoleń pracowników we wprowadzaniu w życie polityki ochrony prywatności i karania pracowników w przypadku jej nieprzestrzegania; oraz że podmiot stosuje wewnętrzne procedury okresowego przeprowadzania przedmiotowych przeglądów zgodności z powyższym. Oświadczenie potwierdzające przeprowadzenie samooceny musi zostać podpisane przez członka zarządu lub innego upoważnionego przedstawiciela podmiotu co najmniej raz w roku i musi zostać udostępnione na żądanie osobom fizycznym w toku dochodzenia bądź badania skargi dotyczącej nieprzestrzegania zasad.

d. W przypadku gdy podmiot wybrał zewnętrzny przegląd zgodności, kontrola taka musi wykazać, że polityka podmiotu w zakresie ochrony prywatności dotycząca danych osobowych otrzymanych z UE jest prawidłowa, całościowa, łatwo dostępna, zgodna z zasadami oraz w pełni wdrożona (tj. że jest przestrzegana). Kontrola ta musi również wykazać, że osoby fizyczne są informowane o wszelkich mechanizmach ochrony prawnej, którymi mogą posłużyć się w celu składania skarg. Metody przeglądu mogą obejmować między innymi audyty, wyrywkowe przeglądy, używanie „przynęt" albo w stosownych przypadkach wykorzystanie narzędzi technologicznych. Oświadczenie potwierdzające przeprowadzenie z pozytywnym wynikiem zewnętrznego przeglądu zgodności musi zostać podpisane przez osobę dokonującą przeglądu, członka zarządu albo innego upoważnionego przedstawiciela podmiotu co najmniej raz w roku i musi zostać udostępnione na żądanie osobom fizycznym w toku dochodzenia bądź badania skargi dotyczącej nieprzestrzegania zasad.

e. Podmioty muszą zachowywać dokumenty dotyczące wdrażania praktyk ochrony prywatności zgodnie z DPF UE–USA oraz udostępniać je na żądanie, w toku dochodzenia bądź badania skargi dotyczącej nieprzestrzegania zasad, niezależnemu organowi ds. rozstrzygania sporów, odpowiedzialnemu za badanie skarg bądź organowi mającemu w zakresie właściwości badanie nieuczciwych i wprowadzających w błąd praktyk. Podmioty muszą również szybko reagować na przekazywane przez departament zapytania i inne wnioski o udzielenie informacji dotyczących przestrzegania zasad przez podmiot.

8. **Dostęp**

a. Zasada dostępu w praktyce

i. Zgodnie z zasadami prawo dostępu ma kluczowe znaczenie dla ochrony prywatności. W szczególności zapewnia ono osobom fizycznym możliwość zweryfikowania prawidłowości przechowywanych informacji na ich temat. Zgodnie z zasadą dostępu osoby fizyczne są uprawnione do:

1. uzyskania od stosownego podmiotu potwierdzenia, czy podmiot ten przetwarza dane osobowe na ich temat ([14]);

2. otrzymania odpowiednich danych, aby mieć możliwość zweryfikowania ich prawidłowości oraz zgodności ich przetwarzania z prawem; oraz

3. zażądania poprawienia, zmiany lub usunięcia danych w przypadku, gdy będą one nieprawidłowe lub gdy będą przetwarzane niezgodnie z zasadami.

ii. Osoby fizyczne nie muszą uzasadniać składanych przez siebie wniosków o udostępnienie danych osobowych, które ich dotyczą. Rozpatrując składane przez osoby fizyczne wnioski o udostępnienie danych, podmioty powinny mieć na uwadze przede wszystkim powód złożenia takiego wniosku. Jeżeli na przykład wniosek o udostępnienie danych jest niejasny albo ma bardzo szeroki zakres, podmiot może nawiązać kontakt z daną osobą fizyczną, aby lepiej zrozumieć powód, dla którego zdecydowała się złożyć wniosek, oraz łatwiej zlokalizować właściwe informacje. Podmiot może zapytać osobę fizyczną, z którymi jednostkami w jego ramach miała ona styczność lub jakiego rodzaju charakter miały informacje stanowiące przedmiot wniosku lub ich wykorzystanie.

iii. Zgodnie z podstawową zasadą dostępu podmioty powinny zawsze podejmować w dobrej wierze wysiłki na rzecz zapewnienia dostępu do informacji. Na przykład jeżeli zachodzi konieczność objęcia określonych informacji ochroną oraz zapewnienia możliwości ich łatwego odseparowania od innych danych osobowych będących przedmiotem wniosku o udostępnienie danych, podmiot powinien utajnić informacje chronione oraz udostępnić pozostałe informacje. Jeżeli podmiot stwierdzi, że w danym przypadku należy ograniczyć dostęp do informacji, powinien przedstawić osobie fizycznej zwracającej się o udzielenie dostępu przyczyny podjęcia takiej decyzji oraz wskazać punkt kontaktowy, do którego może ona kierować wszelkie dalsze zapytania.

b. Obciążenia związane z udzieleniem dostępu lub koszty udzielenia dostępu

i. W wyjątkowych okolicznościach prawo dostępu do danych osobowych może zostać ograniczone, jeżeli istnieje ryzyko naruszenia uzasadnionych praw osób innych niż dana osoba fizyczna lub jeżeli obciążenia związane z udzieleniem dostępu lub koszty udzielenia dostępu byłyby nieproporcjonalne w stosunku do zagrożeń dla prywatności osoby fizycznej w danym przypadku. Koszty i obciążenia stanowią istotne czynniki, które należy wziąć pod uwagę, ale nie mają one decydującego znaczenia przy ustalaniu, czy udzielenie dostępu jest w danym przypadku zasadne.

ii. Na przykład jeżeli dane osobowe są wykorzystywane przy podejmowaniu decyzji, które wywrą istotny wpływ na daną osobę fizyczną (np. odmowa przyznania lub przyznanie istotnych korzyści, takich jak ubezpieczenie, kredyt hipoteczny lub praca), wówczas zgodnie z pozostałymi przepisami niniejszych zasad uzupełniających podmiot byłby zobowiązany do ujawnienia tych informacji, nawet jeżeli byłoby to stosunkowo trudne lub wiązałoby się z koniecznością poniesienia stosunkowo wysokich kosztów. Jeżeli dane osobowe będące przedmiotem wniosku nie są danymi wrażliwymi ani nie są wykorzystywane przy podejmowaniu decyzji, które wywrą istotny wpływ na daną osobę fizyczną, są łatwo dostępne, a ich przekazanie nie wiąże się z koniecznością poniesienia znacznych kosztów, podmiot będzie zobowiązany do zapewnienia dostępu do takich informacji.

c. Poufne informacje handlowe

i. Poufne informacje handlowe to informacje, w odniesieniu do których podmiot podjął kroki w celu zapewnienia ich ochrony przed ujawnieniem, jeżeli takie ujawnienie przyniosłoby korzyść konkurentowi na rynku. Podmioty mogą odmówić dostępu do informacji lub ograniczyć dostęp do informacji, jeżeli udzielenie pełnego dostępu do informacji doprowadziłoby do ujawnienia ich własnych poufnych informacji handlowych, takich jak sporządzane przez nie ustalenia dotyczące funkcjonowania rynku lub klasyfikacje, lub poufnych informacji handlowych innego podmiotu, z którym podmioty wiąże zobowiązanie umowne do zachowania poufności.

([14]) Podmiot powinien udzielać odpowiedzi na zapytania osoby fizycznej dotyczące celów przetwarzania danych, kategorii przetwarzanych danych osobowych oraz odbiorców lub kategorii odbiorców, którym dane osobowe są ujawniane.

ii. Jeżeli poufne informacje handlowe można łatwo oddzielić od innych danych osobowych będących przedmiotem wniosku o udostępnienie danych, podmiot powinien utajnić poufne informacje handlowe i udostępnić informacje niemające poufnego charakteru.

d. Organizowanie baz danych

i. Podmiot może zapewnić dostęp do stosownych danych osobowych, ujawniając je odpowiedniej osobie fizycznej, jeżeli takie ujawnienie nie wiąże się z koniecznością uzyskania przez tę osobę dostępu do bazy danych podmiotu.

ii. Dostęp musi zostać udzielony wyłącznie w zakresie, w jakim dany podmiot przechowuje dane osobowe. Zasada dostępu jako taka nie nakłada na podmioty obowiązku zatrzymywania, utrzymywania, reorganizacji lub restrukturyzacji plików zawierających dane osobowe.

e. Przypadki, w których prawo dostępu może zostać ograniczone

i. Ponieważ podmioty muszą zawsze podejmować w dobrej wierze wysiłki na rzecz zapewnienia osobom fizycznym dostępu do danych osobowych, które ich dotyczą, podmioty mogą ograniczyć takie prawo dostępu w niewielkiej liczbie przypadków, a wszelkie powody ograniczenia dostępu muszą zostać precyzyjnie określone. Zgodnie z postanowieniami RODO podmiot może ograniczyć dostęp do informacji, jeżeli ich ujawnienie mogłoby utrudnić zapewnienie ochrony istotnego nadrzędnego interesu publicznego, takiego jak bezpieczeństwo narodowe; obronność; lub bezpieczeństwo publiczne. Ponadto dostępu można odmówić w przypadku, gdy dane osobowe przetwarza się wyłącznie w celach naukowych lub statystycznych. Wśród innych powodów odmowy lub ograniczenia dostępu należy wymienić:

1. ingerencję w wykonywanie lub egzekwowanie prawa lub ściganie przestępstw z oskarżenia prywatnego, w tym przeciwdziałanie przestępstwom, prowadzenie dochodzeń w ich sprawie lub ich wykrywanie oraz prawo do rzetelnego procesu sądowego;

2. ujawnienie danych w sytuacji, w której mogłoby się to wiązać z naruszeniem uzasadnionych lub istotnych interesów innych osób;

3. naruszenie poufności wymiany informacji między prawnikiem a klientem lub innej tajemnicy zawodowej lub obowiązku zawodowego;

4. niekorzystny wpływ na przebieg postępowań sprawdzających pracowników lub postępowań dotyczących skarg wniesionych przez pracowników lub niekorzystny wpływ na przebieg procedur związanych z planowaniem zmian kadrowych lub reorganizacją przedsiębiorstwa; lub

5. naruszenie poufności niezbędnej do pełnienia funkcji kontrolnych, nadzorczych lub regulacyjnych związanych z prawidłowym zarządzaniem lub poufności w ramach przyszłych lub obecnie prowadzonych negocjacji z udziałem podmiotu.

ii. Podmiot, który powoła się na jeden z przedstawionych powyżej wyjątków, jest zobowiązany do wykazania, że było to konieczne, a także do przedstawienia powodów ograniczenia dostępu oraz do wskazania punktu kontaktowego, do którego osoby fizyczne powinny kierować dalsze pytania.

f. Prawo do uzyskania potwierdzenia oraz do pobierania opłaty na pokrycie kosztów udzielenia dostępu

i. Osoba fizyczna jest uprawniona do uzyskania potwierdzenia, że dany podmiot dysponuje danymi osobowymi, które jej dotyczą. Osoba fizyczna jest również uprawniona do uzyskania dostępu do dotyczących jej danych osobowych przechowywanych przez dany podmiot. Podmiot jest uprawniony do pobierania opłaty z tego tytułu, o ile nie będzie ona nadmiernie wysoka.

ii. Pobieranie opłaty może być uzasadnione na przykład w przypadku, gdy wnioski o udostępnienie danych są ewidentnie nadużywane, w szczególności ze względu na ich powtarzalność.

iii. Dostępu nie można odmówić ze względu na koszty, jeżeli osoba fizyczna wyraża gotowość ich pokrycia.

g. Powtarzające się lub uporczywe składanie wniosków o udostępnienie danych

i. Podmiot może wyznaczyć rozsądne ograniczenia co do liczby wniosków o udostępnienie danych składanych przez daną osobę fizyczną, które zostaną rozpatrzone w określonym okresie. Ustanawiając takie ograniczenia, podmiot powinien wziąć pod uwagę takie czynniki jak częstotliwość aktualizowania informacji, cel, w jakim dane mają zostać wykorzystane, oraz charakter informacji.

h. Oszukańcze wnioski o udostępnienie danych

i. Podmiot nie jest zobowiązany do zapewnienia dostępu, jeżeli nie otrzyma informacji pozwalających mu na potwierdzenie tożsamości wnioskodawcy.

i. Termin na odpowiedź

i. Podmioty powinny odpowiedzieć na wnioski o udostępnienie danych w rozsądnym terminie, w odpowiedni sposób oraz w formie zrozumiałej dla danej osoby fizycznej. Podmiot regularnie przekazujący informacje osobom, których dane dotyczą, może odpowiedzieć na wniosek o udostępnienie danych złożony przez osobę fizyczną w ramach podejmowanych przez siebie regularnie działań w zakresie ujawniania informacji, pod warunkiem że nie będzie to stanowić nadmiernego opóźnienia.

9. **Dane o zasobach ludzkich**

a. Zakres DPF UE–USA

i. Jeżeli podmiot w UE przekazuje dane osobowe na temat swoich pracowników (byłych lub obecnych) gromadzone w ramach stosunku pracy dominującemu, powiązanemu lub niepowiązanemu dostawcy usług w Stanach Zjednoczonych objętemu DPF UE–USA, przekazanie takich danych jest objęte ochroną zapewnioną zgodnie z DPF UE–USA. W takich przypadkach kwestie związane z gromadzeniem informacji i ich przetwarzaniem przed przekazaniem będą regulowały przepisy prawa krajowego państwa członkowskiego UE, w którym dane te zostały zgromadzone, a przy ich przekazywaniu konieczne będzie zapewnienie zgodności z wszelkimi warunkami lub ograniczeniami przewidzianymi w tych przepisach.

ii. Zasady mają zastosowanie wyłącznie w przypadku przekazywania indywidualnie zidentyfikowanych lub możliwych do zidentyfikowania zbiorów danych lub uzyskiwania dostępu do takich zbiorów. Prowadzenie sprawozdawczości statystycznej w oparciu o zagregowane dane dotyczące zatrudnienia, które nie zawierają żadnych danych osobowych lub które nie wiążą się z wykorzystaniem zanonimizowanych danych, nie wzbudza obaw związanych z ochroną prywatności.

b. Stosowanie zasad powiadomienia i wyboru

i. Amerykański podmiot, który otrzymał informacje na temat pracownika z UE zgodnie z DPF UE–USA, może ujawnić takie informacje stronom trzecim lub korzystać z nich w innych celach wyłącznie zgodnie z zasadami powiadomienia i wyboru. Na przykład, jeżeli podmiot zamierza wykorzystać dane osobowe zgromadzone w ramach stosunku pracy do celów niezwiązanych z pracą, takich jak publikacje handlowe, podmiot w Stanach Zjednoczonych musi zwrócić się do zainteresowanych osób fizycznych o udzielenie zgody na wykorzystanie dotyczących ich danych osobowych w tym celu, chyba że osoby te już wcześniej wyraziły na to zgodę. Takie wykorzystanie nie może być niezgodne z celami, dla których dane osobowe zostały zgromadzone lub na które osoba fizyczna wyraziła później zgodę. Ponadto decyzja o udzieleniu lub nieudzieleniu zgody nie może stanowić podstawy do ograniczania możliwości zatrudnienia tych pracowników lub nakładania na nich jakichkolwiek sankcji.

ii. Należy zwrócić uwagę na fakt, że część ogólnie obowiązujących warunków dotyczących przekazywania danych pochodzących z niektórych państw członkowskich UE może uniemożliwiać wykorzystanie takich informacji nawet po ich przekazaniu poza terytorium UE – w takiej sytuacji należy zapewnić poszanowanie tych warunków.

iii. Ponadto pracodawcy powinni dokładać starań, aby należycie uwzględnić preferencje pracowników w obszarze ochrony prywatności. Działania w tym obszarze mogą obejmować np. ograniczenie dostępu do danych osobowych, anonimizowanie określonych danych lub przypisywanie kodów lub pseudonimów, w przypadku gdy korzystanie z faktycznych imion i nazwisk pracowników nie jest konieczne w ramach danego procesu zarządzania.

iv. W okresie i w stopniu, w którym będzie to niezbędne do uniknięcia negatywnego wpływu na zdolność podmiotu do dokonywania awansów, powoływania na stanowiska lub do podejmowania podobnych decyzji dotyczących zatrudnienia, podmiot nie musi stosować zasad ogłoszenia i wyboru.

c. Stosowanie zasady dostępu

i. Zasada uzupełniająca dotycząca dostępu zawiera wskazówki na temat przyczyn, które mogą uzasadniać odrzucenie wniosku o udzielenie dostępu do danych dotyczących zasobów ludzkich lub ograniczenie dostępu do takich danych. Pracodawcy w UE muszą oczywiście przestrzegać przepisów krajowych w tym obszarze i zapewnić pracownikom z UE dostęp do tego rodzaju informacji zgodnie z przepisami obowiązującymi w danym państwie, niezależnie od miejsca, w którym takie dane są przetwarzane i przechowywane. Zgodnie z DPF UE–USA podmiot przetwarzający takie dane w Stanach Zjednoczonych jest zobowiązany do współpracy w zakresie udzielenia bezpośredniego dostępu do takich danych albo udostępniania ich za pośrednictwem pracodawcy w UE.

d. Egzekwowanie prawa

i. Jeżeli dane osobowe są wykorzystywane wyłącznie w związku ze stosunkiem pracy, główna odpowiedzialność za te dane względem pracownika spoczywa na podmiocie w UE. Oznacza to, że w przypadku, gdy pracownicy w Europie złożą skargi dotyczące przypadków naruszenia przysługującego im prawa do ochrony danych osobowych i nie będą zadowoleni z rezultatów procedur przeglądu wewnętrznego, wnoszenia skarg i procedur odwoławczych (lub wszelkich podobnych procedur skargowych przewidzianych w umowie ze związkiem zawodowym), powinni zostać skierowani do państwowego lub krajowego organu ochrony danych lub organu ds. prawa pracy właściwego dla miejsca ich zatrudnienia. Dotyczy to również przypadków, w których odpowiedzialność za domniemane nieprawidłowe wykorzystanie danych osobowych spoczywa na podmiocie w Stanach Zjednoczonych, który otrzymał stosowne informacje od pracodawcy, co stanowi przypadek domniemanego naruszenia zasad. Stanowi to najskuteczniejszą metodę rozstrzygania kwestii związanych z często pokrywającymi się prawami i obowiązkami przewidzianymi w krajowym prawie pracy i w umowach o pracę, a także w przepisach dotyczących ochrony danych.

ii. Podmiot amerykański objęty DPF UE–USA, który korzysta z danych o unijnych zasobach ludzkich przekazanych przez UE w kontekście stosunku pracy i który zamierza objąć transfery takich danych programem DPF UE–USA, musi zobowiązać się do współpracy w stosownych dochodzeniach oraz do przestrzegania wskazówek organów UE w tym zakresie.

e. Stosowanie zasady odpowiedzialności za dalsze przekazywanie

i. W przypadku wystąpienia sporadycznych, związanych z zatrudnieniem potrzeb operacyjnych uczestniczącego podmiotu dotyczących danych osobowych przekazywanych zgodnie z DPF UE–USA, takich jak konieczność rezerwacji biletu lotniczego lub pokoju hotelowego lub konieczność wykupienia polisy ubezpieczeniowej, dopuszcza się możliwość przekazywania danych osobowych niewielkiej liczby pracowników administratorom danych bez konieczności stosowania zasady dostępu lub zawarcia umowy z administratorem będącym stroną trzecią, pomimo że w normalnych warunkach byłoby to wymagane zgodnie z zasadą odpowiedzialności za dalsze przekazywanie, pod warunkiem że uczestniczący podmiot zapewnił zgodność z zasadami powiadomienia i wyboru.

10. **Obowiązkowe umowy dotyczące dalszego przekazywania**

a. Umowy dotyczące przetwarzania danych

i. Jeżeli dane osobowe są przekazywane z UE do Stanów Zjednoczonych wyłącznie w celach związanych z ich przetwarzaniem, konieczne jest podpisanie stosownej umowy w tym zakresie, niezależnie od tego, czy podmiot przetwarzający jest objęty DPF UE–USA.

ii. Administratorzy danych w UE są zobowiązani do podpisania umowy za każdym razem, gdy dochodzi do przekazania danych wyłącznie w celach związanych z ich zwykłym przetwarzaniem, niezależnie od tego, czy przetwarzanie będzie odbywało się na terytorium UE czy poza tym terytorium oraz czy podmiot przetwarzający jest objęty DPF UE–USA, czy też nie. Celem umowy jest zagwarantowanie, by podmiot przetwarzający:

1. podejmował działania wyłącznie zgodnie z instrukcjami administratora danych;

2. zapewniał odpowiednie środki techniczne i organizacyjne pozwalające zapewnić ochronę danych osobowych przed przypadkowym lub bezprawnym zniszczeniem lub przypadkową utratą, modyfikacją, nieuprawnionym ujawnieniem lub uzyskaniem do nich nieuprawnionego dostępu oraz dysponował wiedzą na temat tego, kiedy może dopuścić możliwość dalszego przekazania danych; oraz

3. brał pod uwagę charakter przetwarzania danych i wspierał administratora danych w udzielaniu odpowiedzi osobom fizycznym korzystającym z praw przysługujących im zgodnie z zasadami.

iii. Ponieważ uczestniczące podmioty zapewniają odpowiednią ochronę, umowy z takimi podmiotami dotyczące samego przetwarzania nie wymagają uprzedniego zatwierdzenia.

b. Przekazywanie danych w ramach kontrolowanej grupy korporacji lub jednostek

i. Jeżeli chodzi o przekazywanie danych osobowych między dwoma administratorami danych w ramach kontrolowanej grupy korporacji lub jednostek, zgodnie z zasadą odpowiedzialności za dalsze przekazywanie umowa nie zawsze jest wymagana. Administratorzy danych w ramach kontrolowanej grupy korporacji lub jednostek mogą przeprowadzać tego rodzaju przekazania danych w oparciu o inne instrumenty, takie jak wiążące reguły korporacyjne UE lub inne instrumenty wewnątrzgrupowe (np. programy zgodności i kontroli), przy jednoczesnym zapewnieniu ciągłości ochrony danych osobowych zgodnie z zasadami. W przypadku takich transferów uczestniczący podmiot pozostaje odpowiedzialny za zapewnienie zgodności z zasadami.

c. Transfery między administratorami danych

i. Jeżeli chodzi o transfery między administratorami danych, administrator danych będący odbiorcą nie musi być podmiotem uczestniczącym ani nie musi zapewniać możliwości skorzystania z niezależnego mechanizmu ochrony prawnej. Uczestniczący podmiot musi podpisać umowę z odbiorcą będącym stroną trzecią – administratorem danych – który zapewnia poziom ochrony równoważny poziomowi zapewnianemu zgodnie z DPF UE–USA, przy czym administrator będący stroną trzecią nie musi być uczestniczącym podmiotem ani nie musi zapewniać możliwości skorzystania z niezależnego mechanizmu ochrony prawnej, o ile zapewni możliwość skorzystania z równoważnego mechanizmu.

11. **Rozstrzyganie sporów i egzekwowanie prawa**

a. W zasadzie dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności ustanowiono wymogi w zakresie egzekwowania zasad DPF UE–USA. W zasadzie uzupełniającej dotyczącej kontroli opisano, w jaki sposób należy spełniać wymogi przewidziane w lit. a) ppkt (ii) tej zasady. We wspomnianej zasadzie uzupełniającej odniesiono się do postanowień lit. a) ppkt (i) i (iii) – w obydwu tych podpunktach ustanowiono wymóg zapewnienia możliwości skorzystania z niezależnych mechanizmów ochrony prawnej. Mechanizmy te mogą mieć różną postać, ale muszą spełniać wymogi zasady dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności. Podmioty przestrzegają obowiązujących wymogów poprzez: (i) zapewnienie zgodności z programami prywatności opracowanymi przez podmioty sektora prywatnego, w które wkomponowano zasady i w których przewidziano możliwość skorzystania ze skutecznych mechanizmów egzekwowania przepisów zbliżonych do mechanizmów opisanych w zasadzie dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności; (ii) zapewnienie zgodności z aktami ustawowymi lub regulacyjnymi wydanymi przez organy nadzorcze, stanowiącymi podstawę prawną rozpatrywania skarg wnoszonych przez osoby fizyczne i rozstrzygania sporów; lub (iii) podjęcie zobowiązania do współpracy z organami ochrony danych mającymi swoją siedzibę w UE lub z ich upoważnionymi przedstawicielami.

b. Wykaz ten ma w założeniu charakter ilustracyjny i nie jest zawężający. Sektor prywatny może opracować dodatkowe mechanizmy na rzecz egzekwowania przepisów, o ile będą one spełniały wymogi określone w zasadzie dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności i w zasadach uzupełniających. Należy pamiętać, że wymogi zasady dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności mają charakter uzupełniający w stosunku do wymogu, zgodnie z którym działania samoregulacyjne muszą być możliwe do wykonania zgodnie z sekcją 5 ustawy o FTC (tytuł 15 § 45 U.S.C.), w której ustanowiono zakaz podejmowania nieuczciwych i wprowadzających w błąd działań w ramach wymiany handlowej lub mających wpływ na wymianę handlową, na podstawie tytułu 49 § 41712 U.S.C., w którym zakazuje się przewoźnikowi lub pośrednikowi sprzedaży biletów stosowania nieuczciwych lub wprowadzających w błąd praktyk lub nieuczciwych metod konkurencji w sprzedaży usług transportu lotniczego lub sprzedaży transportu lotniczego lub na mocy innych przepisów ustawowych lub wykonawczych, w których zakazano takich działań.

c. Aby ułatwić zapewnienie zgodności z zobowiązaniami DPF UE–USA i aby wesprzeć stosowne podmioty w zarządzaniu programem, podmioty – a także stosowane przez nie niezależne mechanizmy ochrony prawnej – muszą przekazywać informacje dotyczące DPF UE–USA na żądanie departamentu. Ponadto podmioty muszą szybko rozpatrywać skargi dotyczące przestrzegania przez nie zasad przekazywane przez organy ochrony danych za pośrednictwem departamentu. W odpowiedzi na skargę należy określić, czy skarga jest zasadna, a jeśli tak – wskazać, w jaki sposób podmiot zamierza rozwiązać zaistniały problem. Departament będzie chronił poufność otrzymywanych informacji zgodnie z prawem obowiązującym w Stanach Zjednoczonych.

d. Mechanizmy ochrony prawnej

i. Osoby fizyczne należy zachęcać do przekazywania wszelkich skarg właściwym podmiotom przed podjęciem decyzji o skorzystaniu z niezależnych mechanizmów ochrony prawnej. Podmioty muszą odpowiedzieć na skargę wniesioną przez osobę fizyczną w terminie 45 dni od daty jej otrzymania. Niezależność mechanizmu ochrony prawnej można wykazać w szczególności poprzez udowodnienie, że ma on bezstronny charakter, jego części składowe i struktura jego finansowania są przejrzyste, a jego stosowanie w przeszłości przyniosło udokumentowane dobre rezultaty. Zgodnie z wymogami ustanowionymi w zasadzie dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności mechanizmy ochrony prawnej, z jakich mogą skorzystać osoby fizyczne, muszą być łatwo dostępne i nieodpłatne. Niezależne organy ds. rozstrzygania sporów powinny rozpatrzyć każdą skargę przekazaną przez osoby fizyczne, chyba że taka skarga będzie w oczywisty sposób bezpodstawna lub niepoważna. Niezależny organ ds. rozstrzygania sporów zarządzający mechanizmem ochrony prawnej może jednak przyjąć wymogi w zakresie kwalifikowalności, przy czym takie wymogi powinny być przejrzyste i uzasadnione (np. w celu zapewnienia możliwości wykluczenia skarg wykraczających poza zakres programu lub skarg, które powinny zostać rozpoznane na innym forum) i nie powinny zwalniać organu z obowiązku rozpoznania zasadnych skarg. Ponadto mechanizmy ochrony prawnej powinny dostarczać osobom fizycznym wyczerpujących i łatwo dostępnych informacji na temat przebiegu procedury rozwiązywania sporów po wniesieniu skargi. W takich informacjach należy również uwzględnić opis praktyk w obszarze prywatności stosowanych w ramach mechanizmu zgodnie z zasadami. Wspomniane mechanizmy powinny również prowadzić współpracę w zakresie opracowywania narzędzi takich jak ujednolicone formularze skargowe, aby usprawnić przebieg procedury rozpoznawania skarg.

ii. Niezależne mechanizmy ochrony prawnej muszą udostępniać na swoich ogólnodostępnych stronach internetowych informacje na temat zasad oraz na temat usług świadczonych przez siebie zgodnie z DPF UE–USA. Takie informacje muszą obejmować: 1) informacje na temat wymogów dotyczących niezależnych mechanizmów ochrony prawnej ustanowionych w zasadach lub link do takich informacji; 2) link do strony internetowej departamentu dotyczącej ram ochrony danych; 3) wyjaśnienie, że usługi rozwiązywania sporów w DPF UE–USA są świadczone na rzecz osób fizycznych nieodpłatnie; 4) opis procedury składania skargi dotyczącej kwestii związanych z zasadami; 5) wyznaczenie terminu na rozpoznanie skarg dotyczących zasad; oraz 6) opis zakresu potencjalnych środków ochrony prawnej.

iii. Niezależne mechanizmy ochrony prawnej muszą publikować sprawozdanie roczne zawierające zagregowane dane statystyczne dotyczące świadczonych przez siebie usług w zakresie rozstrzygania sporów. Sprawozdanie roczne musi zawierać następujące informacje: 1) łączną liczbę skarg związanych z zasadami otrzymanych w roku sprawozdawczym; 2) rodzaje otrzymanych skarg; 3) wskaźniki pomiaru jakości rozstrzygania sporów, np. czas niezbędny do rozpatrzenia skarg; oraz 4) wyniki rozpatrywania otrzymanych skarg, w szczególności liczbę i rodzaj zastosowanych środków ochrony prawnej lub nałożonych sankcji.

iv. Jak wskazano w załączniku I, osoby fizyczne mogą skorzystać z arbitrażu, aby ustalić – w odniesieniu do pozostałych roszczeń – czy uczestniczący podmiot naruszył zobowiązania względem danej osoby fizycznej spoczywające na niej zgodnie z zasadami oraz czy takie naruszenie pozostaje w pełni lub częściowo nienaprawione. Z arbitrażu można skorzystać wyłącznie w celach wskazanych powyżej. Z arbitrażu nie można skorzystać np. w przypadku, w którym przedmiotem sporu są wyjątki od zasad ([15]), lub w przypadku zarzutu dotyczącego adekwatności DPF UE–USA. W przypadku wszczęcia postępowania arbitrażowego panel ds. ram ochrony danych UE–USA (w którego skład wchodzi jeden arbiter lub trzech arbitrów, zgodnie z ustaleniami stron) jest uprawniony do zasądzenia godziwego środka naprawiającego szkodę w formie niepieniężnej dostosowanego do indywidualnych potrzeb (takiego jak dostęp do danych dotyczących danej osoby, prawo do ich poprawienia, usunięcia lub zwrócenia danej osobie fizycznej) niezbędnego do naprawienia naruszenia zasad wyłącznie w stosunku do tej osoby fizycznej. Osoby fizyczne i podmioty uczestniczące będą mogły wystąpić o przeprowadzenie kontroli sądowej i wykonanie orzeczeń arbitrażowych zgodnie z prawem amerykańskim, tj. federalną ustawą o arbitrażu.

e. Środki ochrony prawnej i sankcje

i. Zastosowanie jakichkolwiek środków ochrony prawnej zapewnianych przez niezależny organ ds. rozstrzygania sporów powinno skutkować – w stopniu, w jakim będzie to możliwe – uchyleniem lub skorygowaniem skutków nieprzestrzegania zasad przez podmiot oraz zagwarantowaniem, aby dany podmiot w przyszłości przetwarzał dane osobowe zgodnie z zasadami oraz, w stosownych przypadkach, aby zaprzestał przetwarzania danych osobowych osoby fizycznej, która wniosła skargę. Sankcje muszą być dostatecznie rygorystyczne, aby zapewnić przestrzeganie zasad przez podmioty. Wprowadzenie szeregu sankcji o różnym stopniu dotkliwości zapewni organom ds. rozstrzygania sporów możliwość właściwego reagowania na różne przypadki nieprzestrzegania zasad. Sankcje powinny obejmować podanie ustaleń dotyczących

([15]) Zasady, Przegląd, pkt 5.

nieprzestrzegania zasad do wiadomości publicznej oraz nakazanie usunięcia danych w określonych przypadkach ([16]). Inne sankcje mogą obejmować zawieszenie i cofnięcie zezwolenia na prowadzenie działalności, przyznanie osobom fizycznym odszkodowania z tytułu szkody poniesionej wskutek nieprzestrzegania zasad oraz zabezpieczenie roszczenia. Niezależne organy ds. rozstrzygania sporów sektora prywatnego i organy samoregulacyjne mają obowiązek zgłaszać właściwemu organowi rządowemu lub – w stosownych przypadkach – właściwym sądom przypadki niewywiązania się przez uczestniczące podmioty z obowiązku zastosowania się do wydanych przez nie orzeczeń i decyzji oraz powiadomić o tym fakcie departament.

f. Działania FTC

i. FTC zobowiązał się do priorytetowego rozpatrywania zgłoszeń dotyczących domniemanego nieprzestrzegania zasad przekazywanych przez: (i) organy samoregulacyjne ds. prywatności i inne niezależne organy ds. rozstrzygania sporów; (ii) państwa członkowskie UE; oraz (iii) departament, aby ustalić, czy doszło do naruszenia przepisów sekcji 5 ustawy o FTC, w której ustanowiono zakaz podejmowania nieuczciwych lub wprowadzających w błąd działań lub praktyk handlowych. Jeżeli FTC uzna, że istnieją podstawy, by przypuszczać, że doszło do naruszenia przepisów sekcji 5, może rozstrzygnąć tę kwestie, występując o wydanie administracyjnego nakazu zaprzestania stosowania zaskarżonych praktyk lub wnosząc skargę do federalnego sądu pierwszej instancji (ang. *federal district court*) – w przypadku jej pomyślnego rozpoznania sąd federalny może wydać nakaz o tej samej treści. Dotyczy to fałszywych oświadczeń o przestrzeganiu zasad lub udziale w DPF UE–USA składanych przez podmioty, które nie figurują już w wykazie DPF albo które nigdy nie dokonały samocertyfikacji przed departamentem. FTC może wystąpić o nałożenie kar na gruncie prawa cywilnego z tytułu naruszenia administracyjnego nakazu zaprzestania stosowania zaskarżonych praktyk oraz może wszcząć postępowanie cywilne lub karne dotyczące naruszenia nakazu wydanego przez sąd federalny. FTC powiadomi departament o wszelkich podejmowanych przez siebie działaniach w tym obszarze. Departament zachęca inne organy rządowe do powiadamiania go o treści ostatecznych postanowień dotyczących wszelkich tego rodzaju zgłoszeń lub innych orzeczeń dotyczących przestrzegania zasad.

g. Uporczywe nieprzestrzeganie zasad

i. Jeżeli dany podmiot będzie uporczywie nie przestrzegać zasad, straci możliwość dalszego korzystania z przywilejów wynikających z DPF UE–USA. Podmioty, które uporczywie nie przestrzegały zasad, zostaną usunięte przez departament z wykazu DPF i będą zobowiązane do zwrócenia lub usunięcia danych osobowych, które otrzymały zgodnie z DPF UE–USA.

ii. Z uporczywym nieprzestrzeganiem zasad mamy do czynienia w przypadku, gdy podmiot, który dokonał samocertyfikacji przed departamentem, odmówi zastosowania się do ostatecznych ustaleń jakiegokolwiek postępowania służącego rozstrzygnięciu sporu prowadzonego przed samoregulacyjnym, niezależnym organem ds. prywatności lub przed organem rządowym, lub gdy taki organ, w tym departament, uzna, że podmiot na tyle często nie wywiązuje się z zobowiązań spoczywających na nim zgodnie z zasadami, że jego deklaracji o przestrzeganiu tych zasad nie można już uznać za wiarygodną. W przypadkach gdy takiego ustalenia dokona organ inny niż departament, podmiot musi niezwłocznie powiadomić departament o zaistnieniu takiej sytuacji. Niedopełnienie tego obowiązku może stanowić podstawę dla wszczęcia postępowania zgodnie z przepisami ustawy o fałszywych oświadczeniach (tytuł 18 § 1001 U.S.C.). Wycofanie się podmiotu z udziału w programie na rzecz samoregulacji kwestii związanych z prywatnością w sektorze prywatnym lub z udziału w niezależnym mechanizmie rozstrzygania sporów nie zwalnia go z obowiązku zapewnienia zgodności z zasadami i należy je uznać za przejaw uporczywego nieprzestrzegania zasad.

iii. Departament usunie podmiot z wykazu DPF za uporczywe nieprzestrzeganie zasad, również w odpowiedzi na dowolne otrzymane powiadomienie o takim nieprzestrzeganiu zasad przekazane przez sam podmiot, samoregulacyjny organ ds. prywatności lub inny niezależny organ ds. rozstrzygania sporów lub organ rządowy, po uprzednim zapewnieniu podmiotowi możliwości ustosunkowania się do tych zarzutów w terminie 30 dni ([17]). Dlatego też prowadzony przez departament wykaz DPF będzie zawierał przejrzyste informacje na temat tego, które podmioty mogą nadal korzystać z przywilejów wynikających z DPF UE–USA.

iv. Podmiot ubiegający się o uczestnictwo w organie samoregulacyjnym w celu ponownego zakwalifikowania się do objęcia DPF UE–USA musi przedstawić temu organowi wyczerpujące informacje na temat swojego wcześniejszego udziału w DPF UE–USA.

([16]) Niezależne organy ds. rozstrzygania sporów dysponują swobodą uznania co do okoliczności, w jakich zdecydują się na nałożenie tych sankcji. Wrażliwość danych stanowi jeden z czynników, jaki należy wziąć pod uwagę przy podejmowaniu decyzji, czy w danym przypadku zachodzi konieczność usunięcia danych, a także czy podmiot gromadził informacje, korzystał z nich lub ujawniał je z rażącym naruszeniem zasad.

([17]) Departament wskaże w powiadomieniu termin, koniecznie krótszy niż 30 dni, w którym podmiot ma odpowiedzieć na powiadomienie.

12. **Wybór – termin na skorzystanie z klauzuli *opt-out***

a. Zasadniczo celem zasady wyboru jest zapewnienie wykorzystywania i ujawniania danych osobowych w sposób zgodny z oczekiwaniami i wyborami danej osoby fizycznej. Podobnie osoba fizyczna powinna mieć możliwość skorzystania z klauzuli *opt-out* i zdecydowania, czy chce wyrazić zgodę na przetwarzanie jej danych osobowych do celów marketingu bezpośredniego w dowolnym momencie i pod warunkiem ustanowienia zasadnych ograniczeń przez podmiot, np. zapewnienia podmiotowi czasu na nadanie skuteczności klauzuli *opt-out*. Podmiot może też wymagać przekazania wystarczających informacji, które pozwolą na potwierdzenie tożsamości osoby korzystającej z klauzuli *opt-out*. W Stanach Zjednoczonych osoby fizyczne mogą skorzystać z tego wariantu za pośrednictwem programu „opt-out". Niezależnie od danego przypadku osoba fizyczna powinna mieć możliwość skorzystania z łatwo dostępnego i przystępnego cenowo mechanizmu zapewniającego jej możliwość wyboru tego wariantu.

b. Podobnie podmiot może korzystać z informacji w określonych celach związanych z marketingiem bezpośrednim, jeżeli zapewnienie osobie fizycznej możliwości skorzystania z klauzuli *opt-out* przed wykorzystaniem informacji jest niemożliwe, pod warunkiem że podmiot niezwłocznie i jednocześnie (oraz w dowolnym momencie, jeżeli osoba fizyczna wystąpi ze stosownym żądaniem) zapewni danej osobie fizycznej możliwość cofnięcia zgody (bez konieczności uiszczenia jakichkolwiek opłat) na otrzymywanie jakichkolwiek dalszych materiałów marketingu bezpośredniego i spełni życzenie osoby fizycznej.

13. **Informacje dotyczące podróży**

a. Informacje gromadzone przy dokonywaniu rezerwacji przez pasażerów linii lotniczych i inne informacje dotyczące podróży, takie jak informacje gromadzone w ramach programu lojalnościowego „frequent flyer" lub informacje gromadzone przy dokonywaniu rezerwacji w hotelach, np. informacje o zamawianiu posiłków spełniających określone wymagania religijne lub informacje o wystąpieniu z żądaniem udzielenia pomocy fizycznej, mogą być w różnych przypadkach przekazywane podmiotom spoza UE. Zgodnie z RODO w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony dane osobowe mogą być przekazywane do państwa trzeciego, jeżeli zapewnione są odpowiednie zabezpieczenia służące ochronie danych zgodnie z art. 46 RODO lub, w określonych sytuacjach, jeżeli spełniony jest jeden z warunków określonych w art. 49 RODO (np. jeżeli osoba, której dane dotyczą, wyraźnie wyraziła zgodę na przekazanie danych). Podmioty amerykańskie uczestniczące w DPF UE–USA zapewniają odpowiednią ochronę danych osobowych, dlatego też mogą przyjmować transfery danych z UE na podstawie art. 45 RODO bez konieczności wprowadzania instrumentu przekazywania zgodnie z art. 46 RODO lub spełniania warunków określonych w art. 49 RODO. Ponieważ w DPF UE–USA ustanowiono przepisy szczegółowe dotyczące postępowania z informacjami szczególnie chronionymi, takie informacje (które mogą być gromadzone np. w związku z koniecznością udzielenia klientom pomocy fizycznej) mogą zostać uwzględnione w transferach przekazywanych uczestniczącym podmiotom. We wszystkich przypadkach podmiot przekazujący informacje musi jednak zapewnić poszanowanie prawa obowiązującego w państwie członkowskim UE, w którym prowadzi działalność – zgodnie z przepisami obowiązującymi w tym państwie przetwarzanie danych wrażliwych może być np. obwarowane szczególnymi warunkami.

14. **Produkty farmaceutyczne i lecznicze**

a. Stosowanie prawa UE/prawa obowiązującego w państwie członkowskim lub zasad

i. Przepisy UE/przepisy obowiązujące w państwie członkowskim mają zastosowanie przy gromadzeniu danych osobowych i przy wszelkim przetwarzaniu takich danych przed ich przekazaniem Stanom Zjednoczonym. Zasady mają zastosowanie do danych po ich przekazaniu Stanom Zjednoczonym. W stosownych przypadkach dane wykorzystywane do celów związanych z prowadzeniem badań farmaceutycznych i w innych celach powinny zostać zanonimizowane.

b. Przyszłe badania naukowe

i. Dane osobowe przetwarzane w ramach określonych badań medycznych lub farmaceutycznych niejednokrotnie odgrywają istotną rolę w przyszłych badaniach naukowych. W przypadku przekazania danych osobowych zgromadzonych w ramach jednego badania naukowego podmiotowi amerykańskiemu objętemu DPF UE–USA podmiot ten może skorzystać z tych danych do przeprowadzenia nowych badań naukowych, jeżeli wcześniej przekazał danym osobom stosowne powiadomienie i zapewnił im możliwość dokonania wyboru. W takim powiadomieniu należy zawrzeć informacje o wszelkich przyszłych sposobach korzystania z danych, np. o zamiarze wykorzystania ich do celów związanych z okresowym podejmowaniem działań następczych, prowadzeniem powiązanych badań lub podejmowaniem działań marketingowych.

ii. Ze zrozumiałych względów nie sposób przewidzieć wszystkich przyszłych zastosowań określonych danych, ponieważ decyzja o wykorzystaniu danych do celów związanych z nowymi badaniami może zostać podjęta w rezultacie wyciągnięcia nowych wniosków z pierwotnych danych, dokonania nowych odkryć naukowych i postępów w dziedzinie medycyny i zdrowia publicznego oraz zmiany obowiązujących przepisów. Dlatego też – w stosownych przypadkach – w powiadomieniu należy wyjaśnić, że dane osobowe mogą być wykorzystywane do celów związanych z przyszłymi badaniami medycznymi i farmaceutycznymi, których charakteru nie można obecnie przewidzieć. Jeżeli sposób korzystania z danych jest niezgodny z ogólnymi celami badania, na potrzeby którego dane osobowe zostały pierwotnie zgromadzone, lub niezgodne z celami, na które osoba fizyczna wyraziła następnie swoją zgodę, należy uzyskać nową zgodę.

c. Wycofanie się z badania klinicznego

i. Uczestnicy mogą w każdej chwili podjąć decyzję o wycofaniu się z badań klinicznych lub mogą zostać poproszeni o wycofanie się z takich badań. Wszelkie dane osobowe zgromadzone przed wycofaniem się danej osoby z badań klinicznych mogą być w dalszym ciągu przetwarzane razem z pozostałymi danymi zgromadzonymi w trakcie badań klinicznych, o ile uczestnik badania został w jednoznaczny sposób poinformowany o tym fakcie w powiadomieniu przekazanym mu w chwili, gdy wyraził zgodę na udział w badaniu.

d. Przekazywanie informacji do celów regulacyjnych i do celów związanych ze sprawowaniem nadzoru

i. Przedsiębiorstwa zajmujące się wytwarzaniem produktów farmaceutycznych i wyrobów medycznych są uprawnione do przekazywania danych osobowych zgromadzonych w trakcie badań klinicznych przeprowadzonych w UE regulatorom rynku w Stanach Zjednoczonych do celów regulacyjnych i do celów związanych ze sprawowaniem nadzoru. Dopuszcza się możliwość dokonywania podobnych transferów danych na rzecz podmiotów innych niż regulatorzy, takich jak siedziby przedsiębiorstw i inni badacze, zgodnie z zasadami powiadomienia i wyboru.

e. Badania ze „ślepą próbą"

i. Aby zapewnić obiektywność wyników wielu badań klinicznych, ich uczestnikom – a często również osobom prowadzącym badania – nie można udzielić dostępu do informacji o leczeniu, jakiemu może być poddawany dany uczestnik badania. Udzielenie takich informacji zagroziłoby wiarygodności badania i jego wyników. Uczestnikom badań klinicznych (określanych jako badania ze „ślepą próbą") nie należy udzielać dostępu do danych na temat ich leczenia w trakcie badania, jeżeli przekazano im stosowne informacje w tym zakresie w momencie, w którym decydowali się na udział w badaniu, a ujawnienie takich informacji zagroziłoby wiarygodności całego badania.

ii. Wyrażenie zgody na udział w badaniu na takich warunkach jest równoznaczne ze skutecznym zrzeczeniem się prawa dostępu do danych. Po zakończeniu badania i przeanalizowaniu jego wyników uczestnikom należy zapewnić dostęp do danych, które ich dotyczą, jeżeli tego zażądają. Uczestnicy badania powinni zwrócić się z żądaniem udostępnienia takich danych przede wszystkim do lekarza lub innego świadczeniodawcy, który był odpowiedzialny za ich leczenie w trakcie badania klinicznego, lub – w dalszej kolejności – do podmiotu sponsorującego badania kliniczne.

f. Monitorowanie bezpieczeństwa i skuteczności produktów

i. Przedsiębiorstwo zajmujące się wytwarzaniem produktów farmaceutycznych i wyrobów medycznych nie ma obowiązku stosowania zasad w zakresie zasad powiadomienia, wyboru, odpowiedzialności za dalsze przekazywanie danych i dostępu przy podejmowaniu działań dotyczących monitorowania bezpieczeństwa i skuteczności wytwarzanych przez siebie produktów, w tym nie ma obowiązku zgłaszania wystąpienia zdarzeń niepożądanych ani monitorowania pacjentów/podmiotów korzystających z określonych produktów leczniczych lub wyrobów medycznych, w zakresie, w jakim zapewnienie zgodności z tymi zasadami uniemożliwia spełnienie wymogów regulacyjnych. Dotyczy to zarówno sprawozdań przekazywanych przedsiębiorstwom zajmującym się wytwarzaniem produktów farmaceutycznych i wyrobów medycznych na przykład przez świadczeniodawców, jak i sprawozdań przekazywanych przez przedsiębiorstwa zajmujące się wytwarzaniem produktów farmaceutycznych i wyrobów leczniczych agencjom rządowym takim jak Urząd ds. Żywności i Leków.

g. Dane kodowane za pomocą klucza

i. Wyniki badań naukowych są zawsze kodowane przez głównego badacza w momencie ich uzyskania za pomocą niepowtarzalnego klucza, aby nie dopuścić do ujawnienia tożsamości poszczególnych osób, których dane dotyczą. Przedsiębiorstwa farmaceutyczne sponsorujące takie badania nie posiadają dostępu do tego klucza. Niepowtarzalny klucz jest znany wyłącznie badaczowi – dzięki temu badacz może ustalić tożsamość osoby biorącej udział w badaniu w wyjątkowych okolicznościach (np. w przypadku konieczności udzielenia takiej osobie pomocy medycznej po zakończeniu badania). Przekazanie danych zakodowanych w opisany powyżej sposób z UE do Stanów Zjednoczonych, które zgodnie z prawem UE stanowią unijne dane osobowe, podlegałoby zasadom.

15. **Rejestr publiczny i publicznie dostępne informacje**

a. Podmiot musi stosować zasady bezpieczeństwa, integralności danych i ograniczenia celu oraz zasadę dotyczącą ochrony prawnej, egzekwowania prawa oraz odpowiedzialności w odniesieniu do danych osobowych pochodzących z ogólnodostępnych źródeł. Zasady te mają również zastosowanie do danych osobowych pochodzących z rejestrów publicznych (tj. z ogólnodostępnych rejestrów prowadzonych przez agencje rządowe lub podmioty na poszczególnych szczeblach).

b. Stosowanie zasad powiadomienia, wyboru lub odpowiedzialności za dalsze przekazywanie w odniesieniu do informacji przechowywanych w rejestrach publicznych nie jest konieczne, o ile takie informacje nie zostaną połączone z informacjami przechowywanymi w rejestrach niepublicznych i pod warunkiem zapewnienia zgodności z wszelkimi warunkami uzyskania dostępu do takich informacji obowiązującymi w danym systemie prawnym. Ponadto stosowanie zasad powiadomienia, wyboru lub odpowiedzialności za dalsze przekazywanie w odniesieniu do ogólnodostępnych informacji nie jest co do zasady konieczne, chyba że osoba dokonująca przeniesienia z UE wskaże, że takie informacje podlegają ograniczeniom wiążącym się z koniecznością zastosowania tych zasad przez podmiot zamierzający wykorzystać te informacje w określonych celach. Podmioty nie ponoszą odpowiedzialności za sposób wykorzystywania tych informacji przez podmioty uzyskujące do nich dostęp za pośrednictwem opublikowanych materiałów.

c. Jeżeli okaże się, że podmiot umyślnie podał dane osobowe do wiadomości publicznej z naruszeniem zasad, tak aby wykorzystać te wyjątki lub umożliwić innym podmiotom skorzystanie z nich, nie będzie już uprawniony do korzystania z przywilejów wynikających z DPF UE–USA.

d. Stosowanie zasady dostępu w odniesieniu do informacji przechowywanych w rejestrze publicznym nie jest konieczne, o ile takie informacje nie zostaną połączone z innymi danymi osobowymi (nie dotyczy to niewielkich ilości informacji wykorzystywanych do indeksowania informacji przechowywanych w rejestrze publicznym lub do zarządzania tymi informacjami); należy jednak przestrzegać wszelkich warunków uzyskania dostępu do takich informacji obowiązujących w danym systemie prawnym. Natomiast w przypadku, gdy dochodzi do połączenia informacji przechowywanych w rejestrze publicznym z informacjami przechowywanymi w rejestrze niepublicznym (innymi niż informacje wskazane powyżej), podmiot musi zapewnić dostęp do wszystkich tego rodzaju informacji, o ile nie są one objęte innymi dopuszczalnymi wyjątkami.

e. Podobnie jak ma to miejsce w przypadku informacji przechowywanych w rejestrach publicznych, zapewnienie dostępu do informacji, które zostały już podane do wiadomości publicznej, nie jest konieczne, o ile takie informacje nie zostały połączone z informacjami, które nie są ogólnodostępne. Podmioty, których działalność polega na sprzedaży publicznie dostępnych informacji, mogą zażądać od podmiotu uiszczenia opłaty, jaką zwyczajowo pobierają z tytułu rozpatrzenia wniosku o udzielenie dostępu. Osoby fizyczne mogą również zwrócić się o udostępnienie im danych na ich temat do podmiotu, który pierwotnie zgromadził stosowne dane.

16. **Wnioski o udostępnienie danych składane przez organy publiczne**

a. Aby zapewnić przejrzystość w odniesieniu do wniosków o udostępnienie danych, składanych zgodnie z prawem przez organy publiczne, podmioty uczestniczące mogą dobrowolnie publikować okresowe sprawozdania z przejrzystości zawierające informacje o liczbie wniosków o udostępnienie danych osobowych na potrzeby egzekwowania prawa lub zapewnienia bezpieczeństwa narodowego, jakie otrzymują od organów publicznych, o ile ujawnienie tego rodzaju danych jest dopuszczalne w świetle obowiązujących przepisów.

b. Informacje zamieszczane w tych sprawozdaniach przez podmioty uczestniczące, informacje, które zostały ujawnione przez Wspólnotę Wywiadowczą, oraz inne informacje mogą być wykorzystywane przy przeprowadzaniu okresowego wspólnego przeglądu funkcjonowania DPF UE–USA zgodnie z zasadami.

c. Niewystosowanie powiadomienia zgodnie z lit. a) ppkt (xii) zasady powiadomienia nie uniemożliwia danemu podmiotowi udzielenia odpowiedzi na jakikolwiek złożony zgodnie z prawem wniosek ani nie utrudnia mu udzielenia odpowiedzi na taki wniosek.

ZAŁĄCZNIK I: MODEL ARBITRAŻOWY

W niniejszym załączniku I przedstawiono warunki rozpatrywania roszczeń w ramach postępowania arbitrażowego przez podmioty uczestniczące w DPF UE–USA zgodnie z zasadą dotyczącą ochrony prawnej, egzekwowania prawa oraz odpowiedzialności. Opisana poniżej możliwość przeprowadzenia arbitrażu ma zastosowanie do niektórych „pozostałych" roszczeń dotyczących danych objętych DPF UE–USA. Celem tego rozwiązania jest zapewnienie możliwości skorzystania przez osoby fizyczne na zasadzie dobrowolności z szybkiego, niezależnego i sprawiedliwego mechanizmu rozstrzygania wszelkich przypadków domniemanych naruszeń zasad, które nie zostały rozstrzygnięte w ramach żadnego z pozostałych mechanizmów DPF UE–USA.

A. **Zakres oddziaływania**

Osoba fizyczna może skorzystać z arbitrażu, aby ustalić – w odniesieniu do pozostałych roszczeń – czy podmiot uczestniczący naruszył spoczywające na nim zgodnie z zasadami zobowiązania względem danej osoby fizycznej oraz czy takie naruszenie pozostaje w pełni lub częściowo nienaprawione. Z arbitrażu można skorzystać wyłącznie w celach wskazanych powyżej. Z arbitrażu nie można skorzystać np. w przypadku, w którym przedmiotem sporu są wyjątki od zasad ([1]), lub w przypadku zarzutu dotyczącego adekwatności DPF UE–USA.

B. **Dostępne środki ochrony prawnej**

W przypadku wszczęcia postępowania arbitrażowego „panel ds. ram ochrony danych UE–USA" (panel, w którego skład wchodzi jeden arbiter lub trzech arbitrów, zgodnie z ustaleniami stron) jest uprawniony do zasądzenia godziwego środka naprawiającego szkodę w formie niepieniężnej dostosowanego do indywidualnych potrzeb (takiego jak dostęp do danych dotyczących danej osoby, prawo do ich poprawienia, usunięcia lub zwrócenia danej osobie fizycznej) niezbędnego do naprawienia naruszenia zasad wyłącznie w stosunku do tej osoby fizycznej. Są to wyłącznie uprawnienia przysługujące panelowi ds. ram ochrony danych UE–USA w odniesieniu do środków ochrony prawnej. W czasie obrad nad tym, jakie środki ochrony prawnej należy zastosować w danym przypadku, panel ds. ram ochrony danych UE–USA musi wziąć pod uwagę inne środki ochrony prawnej, które zostały już zastosowane w ramach innych mechanizmów DPF UE–USA. Nie przewidziano możliwości dochodzenia odszkodowania, zwrotu kosztów lub opłat ani stosowania innych środków ochrony prawnej. Każda strona jest zobowiązana do pokrycia honorarium swojego pełnomocnika procesowego.

C. **Wymogi, jakie muszą zostać spełnione przed wszczęciem postępowania arbitrażowego**

Osoba fizyczna, która zdecyduje się skorzystać z możliwości przeprowadzenia postępowania arbitrażowego, musi podjąć następujące działania przed wystąpieniem o wszczęcie postępowania arbitrażowego: 1) zgłosić domniemane naruszenie bezpośrednio danemu podmiotowi i zapewnić mu możliwość rozwiązania zaistniałego problemu w terminie wyznaczonym w lit. d) ppkt (i) zasady uzupełniającej dotyczącej rozstrzygania sporów i egzekwowania prawa; 2) skorzystać z bezpłatnego niezależnego mechanizmu ochrony prawnej przewidzianego w zasadach; oraz 3) przekazać stosowne informacje departamentowi za pośrednictwem właściwego dla tej osoby fizycznej organu ochrony danych i zapewnić departamentowi możliwość podjęcia działań w celu rozwiązania danego problemu w terminach określonych w piśmie Urzędu ds. Handlu Międzynarodowego w departamencie – przekazanie takich informacji nie wiąże się z koniecznością ponoszenia jakichkolwiek opłat przez osobę fizyczną.

Z wariantu zakładającego przeprowadzenie arbitrażu nie można skorzystać, jeżeli to samo domniemane naruszenie zasad 1) było już przedmiotem arbitrażu; 2) było przedmiotem prawomocnego wyroku wydanego w postępowaniu sądowym, którego stroną była dana osoba fizyczna; lub 3) zostało już wcześniej uregulowane przez strony. Ponadto z tego wariantu nie można skorzystać, jeżeli organ ochrony danych 1) jest organem właściwym zgodnie z zasadą uzupełniającą dotyczącą roli organów ochrony danych lub zasadą uzupełniającą dotycząca danych o zasobach ludzkich; lub 2) został upoważniony do rozstrzygnięcia przypadku domniemanego naruszenia bezpośrednio przez podmiot. Uprawnienie organu ochrony danych do rozpatrzenia tych samych zarzutów przeciwko unijnemu administratorowi danych nie wyklucza samo w sobie wszczęcia postępowania arbitrażowego przeciwko innemu podmiotowi prawnemu, dla którego nie wyznaczono takiego organu ochrony danych.

D. **Wiążący charakter orzeczeń**

Decyzja osoby fizycznej o skorzystaniu z arbitrażu jest całkowicie dobrowolna. Orzeczenia arbitrażowe będą wiążące dla wszystkich stron arbitrażu. Po wystąpieniu o arbitraż dana osoba fizyczna traci możliwość dochodzenia środka naprawiającego szkodę za ten sam rodzaj naruszenia przed innym organem lub sądem, przy czym jeżeli godziwy środek naprawiający szkodę w formie niepieniężnej nie rekompensuje w pełni domniemanego naruszenia, wystąpienie osoby fizycznej o arbitraż nie wyklucza wniesienia powództwa o odszkodowanie do sądu.

([1]) Zasady, przegląd, pkt 5.

E. **Kontrola i wykonanie**

Osoby fizyczne i podmioty uczestniczące będą mogły wystąpić o przeprowadzenie kontroli sądowej i wykonanie orzeczeń arbitrażowych zgodnie z prawem amerykańskim, tj. federalną ustawą o arbitrażu ([2]). Wszelkie tego typu sprawy muszą być wnoszone przed federalny sąd pierwszej instancji, którego właściwość miejscowa obejmuje główne miejsce prowadzenia działalności podmiotu uczestniczącego.

Tego rodzaju arbitraż służy rozwiązywaniu sporów indywidualnych, przy czym orzeczenia arbitrażowe nie mają przymiotu niepodważalnego ani wiążącego precedensu w sprawach z udziałem stron przeciwnych, w tym w przyszłych postępowaniach arbitrażowych, postępowaniach przed sądami unijnymi lub amerykańskimi bądź w postępowaniach FTC.

F. **Panel arbitrażowy**

Strony wybiorą arbitrów panelu ds. ram ochrony danych UE–USA z wykazu arbitrów omówionego poniżej.

Zgodnie z obowiązującym prawem departament i Komisja opracują wykaz co najmniej 10 arbitrów, wybranych ze względu na ich niezależność, uczciwość i wiedzę fachową. W odniesieniu do tego procesu zastosowanie mają poniższe zasady.

Arbitrzy:

1) będą figurowali w wykazie przez okres trzech lat, chyba że zaistnieją wyjątkowe okoliczności lub zostaną skreśleni z uzasadnionego powodu, z możliwością przedłużenia przez departament, po uprzednim powiadomieniu Komisji, na kolejny okres obejmujący trzy lata;

2) nie podlegają żadnym instrukcjom wydanym przez stronę, dowolny podmiot uczestniczący, USA, UE, państwa członkowskie UE, inny dowolny organ rządowy, organ publiczny lub organ egzekwowania prawa ani nie są z tymi podmiotami powiązani; oraz

3) muszą być uprawnieni do praktykowania prawa w Stanach Zjednoczonych oraz muszą być ekspertami w zakresie praw ochrony danych osobowych w Stanach Zjednoczonych oraz posiadać wiedzę ekspercką w zakresie unijnego prawa ochrony danych.

([2]) Rozdział 2 federalnej ustawy o arbitrażu stanowi, że „umowa o arbitraż lub orzeczenie arbitrażowe wynikające ze stosunku prawnego, umownego bądź nie, które uznaje się za handlowe, w tym transakcja, kontrakt lub umowa opisane w [sekcji 2 federalnej ustawy o arbitrażu], podlega postanowieniom Konwencji [o uznawaniu i wykonywaniu zagranicznych orzeczeń arbitrażowych z dnia 10 czerwca 1958 r., Zbiór traktatów i innych umów międzynarodowych, których USA są stroną (U.S.T.), tom 21, s. 2519, Zbiór tekstów umów międzynarodowych, których USA są stroną (T.I.A.S.) Nr 6997 („konwencja nowojorska")]". Tytuł 9 § 202 U.S.C. Federalna ustawa o arbitrażu stanowi również, że „uznaje się, iż umowa lub orzeczenie wynikające ze stosunku istniejącego w całości między obywatelami Stanów Zjednoczonych nie podlega postanowieniom konwencji [nowojorskiej], chyba że stosunek taki dotyczy majątku znajdującego się za granicą, przewiduje podjęcie działać lub wykonanie za granicą lub jest w inny zasadny sposób powiązany z jednym państwem obcym lub większą ich liczbą". Tamże. Zgodnie z rozdziałem 2 „każda ze stron arbitrażu może wystąpić do dowolnego sądu posiadającego właściwość na mocy tego rozdziału o zatwierdzenie orzeczenia na niekorzyść dowolnej strony przeciwnej postępowania arbitrażowego. Sąd zatwierdzi orzeczenie, chyba że znajdzie jakąkolwiek podstawę do odmowy lub odroczenia uznania lub wykonania orzeczenia określonego we wspomnianej konwencji [nowojorskiej]". Tamże, § 207. Rozdział 2 stanowi również, że „sądy pierwszej instancji Stanów Zjednoczonych [. . .] są właściwe do orzekania [. . .] w sprawie powództwa lub postępowania [podlegającego konwencji nowojorskiej], niezależnie od wartości przedmiotu sporu". Tamże, § 203.
Rozdział 2 stanowi również, że „rozdział 1 ma zastosowanie do powództw i postępowań wszczętych na podstawie tego rozdziału, w zakresie, w jakim rozdział ten nie jest sprzeczny z niniejszym rozdziałem lub konwencją [nowojorską] ratyfikowaną przez Stany Zjednoczone". Tamże, § 208. Rozdział 1 stanowi z kolei, że „pisemne postanowienie [...] . umowy potwierdzającej zawarcie transakcji handlowej dotyczące poddania pod arbitraż sporu wynikającego z takiej umowy lub transakcji lub odmowy wykonania całości lub części umowy bądź pisemna umowa dotycząca poddania pod arbitraż istniejącego sporu wynikającego z takiej umowy, transakcji lub odmowy są ważne, nieodwołalne i wykonalne, z zastrzeżeniem wszelkich podstaw przewidzianych w prawie lub w zasadach słuszności w odniesieniu do rozwiązania jakiejkolwiek umowy". Tamże, § 2. Rozdział 1 stanowi ponadto, że „każda strona postępowania arbitrażowego może wnieść do wskazanego sądu o zatwierdzenie orzeczenia, przy czym sąd ma obowiązek wydać takie postanowienie, chyba że orzeczenie zostanie uchylone, zmienione lub sprostowane, jak określono w sekcjach 10 i 11 [federalnej ustawy o arbitrażu]". Tamże, § 9.

G. **Procedury arbitrażowe**

Zgodnie z obowiązującym prawem departament i Komisja uzgodniły przyjęcie zasad arbitrażu regulujących postępowania przed panelem ds. ram ochrony danych UE–USA ([3]). W przypadku konieczności zmiany zasad regulujących postępowania departament i Komisja uzgodnią zmianę tych zasad lub przyjęcie innego zestawu obowiązujących, ugruntowanych amerykańskich procedur arbitrażowych, w zależności od przypadku, z zastrzeżeniem każdego z następujących warunków:

1. Osoba fizyczna może wszcząć postępowanie arbitrażowe, z zastrzeżeniem powyższego przepisu dotyczącego wymogów przedarbitrażowych, poprzez doręczenia podmiotowi „zawiadomienia". Zawiadomienie zawiera podsumowanie kroków podjętych na podstawie pkt C w celu zaspokojenia roszczenia, opis domniemanego naruszenia oraz, według uznania osoby fizycznej, wszelkie dokumenty uzupełniające i materiały lub omówienie przepisów dotyczących zgłaszanego roszczenia.

2. Opracowane zostaną procedury w celu zapewnienia, aby w związku z tym samym naruszeniem zgłoszonym przez osobę fizyczną nie przyznano powielających się środków ochrony prawnej ani nie prowadzono powielających się procedur.

3. Postępowanie prowadzone przez FTC może przebiegać równolegle z postępowaniem arbitrażowym.

4. Żaden przedstawiciel USA, UE ani żadne państwo członkowskie UE ani jakikolwiek organ rządowy, organ publiczny lub organ egzekwowania prawa nie może uczestniczyć w takich postępowaniach arbitrażowych, chyba że na wniosek osoby fizycznej z UE organy ochrony danych mogą zapewnić pomoc jedynie w przygotowaniu zawiadomienia, ale nie mogą uzyskać dostępu do wyników postępowania dowodowego ani żadnych innych materiałów związanych z tymi postępowaniami arbitrażowymi.

5. Miejscem prowadzenia postępowania arbitrażowego będą Stany Zjednoczone, a osoba fizyczna może zdecydować się na udział w nim za pośrednictwem konferencji wideo lub konferencji telefonicznej, która zostanie zorganizowana nieodpłatnie. Osobiste stawiennictwo nie będzie wymagane.

6. Językiem arbitrażu będzie język angielski, chyba że strony uzgodnią inaczej. Na uzasadniony wniosek, a także uwzględniając fakt, czy osoba jest reprezentowana przez pełnomocnika, tłumaczenie ustne podczas postępowania arbitrażowego oraz tłumaczenie pisemne materiałów arbitrażowych zostanie zapewnione nieodpłatnie, chyba że panel ds. ram ochrony danych UE–USA uzna, iż w związku z okolicznościami danego postępowania arbitrażowego prowadziłoby to do nieuzasadnionych lub nieproporcjonalnych kosztów.

7. Materiały przekazane arbitrom będą traktowane jako poufne i będą wykorzystywane wyłącznie w związku z arbitrażem.

8. W razie potrzeby dozwolone może być przeprowadzenie szczegółowego postępowania dowodowego (ang. *discovery*) i wyniki takiego postępowania będą przez strony traktowane jako poufne i będą wykorzystywane wyłącznie w związku z arbitrażem.

9. Postępowanie arbitrażowe należy zakończyć w ciągu 90 dni od dnia doręczenia zawiadomienia temu podmiotowi, chyba że strony uzgodnią inaczej.

([3]) Międzynarodowe Centrum Rozstrzygania Sporów („ICDR"), czyli dział ds. międzynarodowych Amerykańskiego Stowarzyszenia Arbitrażowego („AAA") (określane zbiorczo „ICDR-AAA"), zostało wybrane przez departament do administrowania postępowaniami arbitrażowymi na podstawie i zarządzania funduszem arbitrażowym określonym w załączniku I do zasad. 15 września 2017 r. departament i Komisja uzgodniły przyjęcie zestawu zasad arbitrażowych regulujących wiążące postępowania arbitrażowe opisane w załączniku I do zasad, a także kodeksu postępowania dla arbitrów, który jest zgodny z ogólnie przyjętymi standardami etycznymi dla arbitrów handlowych i załącznikiem I do zasad. Departament i Komisja uzgodniły, że zasady arbitrażu i kodeks postępowania będą aktualizowane w celu odzwierciedlenia aktualizacji DPF UE–USA, a departament będzie współpracował z ICDR-AAA w celu wprowadzenia tych aktualizacji.

H. **Koszty**

Arbitrzy powinni podjąć zasadne kroki celem zminimalizowania kosztów lub opłat związanych z arbitrażem.

Zgodnie z mającym zastosowanie prawem departament ułatwi utrzymanie funduszu, na który podmioty uczestniczące będą zobowiązane wpłacać składkę proporcjonalną do ich wielkości, która to składka pokryje koszty arbitrażu, w tym honorarium arbitra, do maksymalnej kwoty („górna granica"). Funduszem będzie zarządzać strona trzecia, która będzie regularnie przedstawiać departamentowi sprawozdania z działalności funduszu. Departament będzie współpracował ze stroną trzecią w celu dokonania okresowego przeglądu funkcjonowania funduszu, w tym konieczności dostosowania kwoty składek lub górnej granicy kosztów arbitrażu, oraz przeanalizuje między innymi liczbę postępowań arbitrażowych oraz ich koszty i czas trwania, przy założeniu, że nie zostaną nałożone żadne nadmierne obciążenia finansowe na podmioty uczestniczące. Departament powiadomi Komisję o wynikach takich przeglądów dokonanych we współpracy ze stroną trzecią i z wyprzedzeniem powiadomi Komisję o wszelkich korektach kwoty składek. Honoraria pełnomocnika nie są objęte niniejszym przepisem ani żadnym funduszem ustanowionym na jego mocy.

ZAŁĄCZNIK II

DEPARTAMENT HANDLU STANÓW ZJEDNOCZONYCH
Sekretarz Handlu
Waszyngton 20230

Dnia 6 lipca 2023 r.

Szanowny Pan Didier Reynders
Komisarz do spraw wymiaru sprawiedliwości
European Commission
Rue de la Loi/ Wetstraat 200
1049 Brussels
Belgia

Szanowny Panie Komisarzu!

W imieniu Stanów Zjednoczonych Ameryki mam przyjemność niniejszym przekazać pakiet materiałów dotyczących ram ochrony danych UE–USA, które w połączeniu z rozporządzeniem wykonawczym 14086 w sprawie poprawy zabezpieczeń dotyczących działań Stanów Zjednoczonych w zakresie rozpoznania radioelektronicznego oraz tytułem 28 część 201 kodeksu przepisów federalnych zmieniającym przepisy Departamentu Sprawiedliwości w celu ustanowienia „Sądu Odwoławczego ds. Ochrony Danych", stanowią odzwierciedlenie ważnych i szczegółowych negocjacji mających na celu wzmocnienie ochrony prywatności i wolności obywatelskich. Wskutek przedmiotowych negocjacji opracowano nowe zabezpieczenia mające zapewnić, aby działania USA w zakresie rozpoznania radioelektronicznego były niezbędne i proporcjonalne do osiągnięcia określonych celów bezpieczeństwa narodowego, oraz nowy mechanizm dochodzenia roszczeń dla osób fizycznych z Unii Europejskiej („UE"), w przypadku gdy osoby te uważają, że są celem bezprawnych działań w zakresie rozpoznania radioelektronicznego, które razem zapewnią ochronę unijnych danych osobowych. Ramy ochrony danych UE–USA będą stanowić podstawę konkurencyjnej gospodarki cyfrowej sprzyjającej włączeniu społecznemu. Powinniśmy być dumni z udoskonaleń odzwierciedlonych w tych ramach, które zwiększą ochronę prywatności na całym świecie. Pakiet ten, wraz z rozporządzeniem wykonawczym, przepisami wykonawczymi i innymi dostępnymi materiałami ze źródeł publicznych, daje bardzo solidną podstawę przyjęcia przez Komisję Europejską nowego ustalenia dotyczącego adekwatności ([1]).

Załączono następujące materiały:

— zasady ramowe ochrony danych UE–USA, w tym zasady uzupełniające (zwane łącznie „zasadami") oraz załącznik I do zasad (tj. załącznik, w którym przedstawiono warunki rozpatrywania roszczeń dotyczących danych osobowych objętych zasadami w ramach postępowania arbitrażowego przez podmioty uczestniczące w ramach ochrony danych);

— pismo Urzędu ds. Handlu Międzynarodowego departamentu, który zarządza programem ram ochrony danych, w którym opisano zobowiązania, jakie nasz departament podjął, aby zapewnić skuteczne funkcjonowanie ram ochrony danych UE–USA;

— pismo Federalnej Komisji Handlu, w którym Komisja opisuje sposób, w jaki egzekwuje zasady;

— pismo Departamentu Transportu, w którym departament opisuje sposób, w jaki egzekwuje zasady;

— pismo sporządzone przez Urząd Dyrektora Krajowych Służb Wywiadowczych dotyczące gwarancji i ograniczeń mających zastosowanie do amerykańskich organów bezpieczeństwa narodowego; oraz

— pismo sporządzone przez Departament Sprawiedliwości dotyczące gwarancji i ograniczeń w dostępie rządu Stanów Zjednoczonych do danych na potrzeby egzekwowania prawa i interesu publicznego.

([1]) Pod warunkiem że decyzja Komisji w sprawie adekwatności ochrony przewidzianej w ramach ochrony danych UE–USA ma zastosowanie do Islandii, Liechtensteinu i Norwegii, pakiet ram ochrony danych UE–USA obejmuje zarówno Unię Europejską, jak i te trzy kraje.

Pełny pakiet ram ochrony danych UE–USA zostanie opublikowany na stronie internetowej departamentu dotyczącej ram ochrony danych, a zasady i załącznik I do zasad zaczną obowiązywać w dniu wejścia w życie decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony.

Zapewniam, że Stany Zjednoczone traktują te zobowiązania poważnie. Cieszymy się na współpracę z Państwem przy wdrażaniu ram ochrony danych UE–USA oraz przy wchodzeniu razem w nową fazę tego procesu.

Z poważaniem

Gina M. RAIMONDO

ZAŁĄCZNIK III

UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

Dnia 12 grudnia 2022 r.

Szanowny Pan Didier Reynders
Komisarz do spraw wymiaru sprawiedliwości
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Belgia

Szanowny Panie Komisarzu!

W imieniu Urzędu ds. Handlu Międzynarodowego („ITA") mam przyjemność przedstawić opis zobowiązań, jakie podjął Departament Handlu („departament"), aby zapewnić ochronę danych osobowych poprzez zarządzanie programem ram ochrony danych i nadzór nad nim. Sfinalizowanie ram ochrony danych UE–USA („DPF UE–USA") jest niezwykle znaczącym osiągnięciem zarówno w kontekście prywatności, jak i dla przedsiębiorstw po obu stronach Atlantyku, ponieważ buduje ono wśród osób fizycznych w UE poczucie bezpieczeństwa, że ich dane będą chronione i że przysługują im środki ochrony prawnej, z których mogą skorzystać, jeżeli mają jakiekolwiek obawy związane z ich danymi, a także umożliwi tysiącom przedsiębiorstw dalsze inwestowanie i prowadzenie handlu po obu stronach Atlantyku z korzyścią dla naszych gospodarek i obywateli. DPF UE–USA odzwierciedlają lata ciężkiej pracy oraz współpracy z Państwem oraz Państwa kolegami i koleżankami w Komisji Europejskiej („Komisja"). Liczymy na dalszą współpracę z Komisją w celu zapewnienia skutecznego funkcjonowania wspólnie wypracowanych ram.

DPF UE–USA przyniosą istotne korzyści zarówno osobom fizycznym, jak i przedsiębiorstwom. Po pierwsze, wprowadzono w nich ważny zestaw gwarancji ochrony prywatności w odniesieniu do danych osób fizycznych z UE przekazywanych do USA. Wymagają od uczestniczących amerykańskich podmiotów, aby opracowały odpowiednią politykę ochrony prywatności; publicznie zobowiązały się do przestrzegania „zasad ramowych ochrony danych UE–USA", w tym zasad uzupełniających (zwanych łącznie „zasadami") oraz załącznika I do zasad (tj. załącznik, w którym przedstawiono warunki rozpatrywania roszczeń dotyczących danych osobowych objętych zasadami w ramach postępowania arbitrażowego przez podmioty uczestniczące w DPF UE–USA), umożliwiając tym samym egzekwowanie zobowiązań na podstawie prawa amerykańskiego ([1]); co roku poświadczały w drodze ponownej certyfikacji w departamencie swoje zobowiązanie do przestrzegania zasad; wprowadziły dobrowolny niezależny mechanizm rozstrzygania sporów dla osób fizycznych z UE; oraz podlegały uprawnieniom dochodzeniowym i wykonawczym amerykańskiego organu ustawowego wymienionego w zasadach (np. Federalnej Komisji Handlu („FTC"), Departamentu Transportu („DoT")) lub innego amerykańskiego organu ustawowego wymienionego w przyszłym załączniku do zasad. Chociaż decyzja podmiotu o samocertyfikacji jest dobrowolna, to w momencie, gdy publicznie zobowiąże się on do przestrzegania DPF UE–USA, zobowiązanie takie może zostać wyegzekwowane na mocy prawa amerykańskiego przez FTC, DoT lub inny amerykański organ ustawowy, w zależności od tego, który organ jest właściwy do rozstrzygania spraw danego podmiotu uczestniczącego. Po drugie, DPF UE–USA pozwoli

([1]) Podmioty, które w drodze samocertyfikacji potwierdziły swoje zobowiązanie do przestrzegania zasad ramowych Tarczy Prywatności UE–USA i chcą czerpać korzyści z uczestnictwa w DPF UE–USA, muszą przestrzegać „zasad ramowych ochrony danych UE–USA". Zobowiązanie do przestrzegania „zasad ramowych ochrony danych UE–USA" zostanie odzwierciedlone w polityce prywatności tych podmiotów uczestniczących tak szybko, jak to możliwe, a w każdym razie nie później niż trzy miesiące od daty wejścia w życie „zasad ramowych ochrony danych UE–USA". (*Zob*. sekcja e) zasady uzupełniającej dotyczącej samocertyfikacji).

przedsiębiorstwom w Stanach Zjednoczonych, w tym spółkom zależnym przedsiębiorstw europejskich mających siedzibę w Stanach Zjednoczonych, na uzyskiwanie danych osobowych z Unii Europejskiej, aby ułatwić przepływy danych, które przyczyniają się do rozwoju handlu transatlantyckiego. Przepływy danych między Stanami Zjednoczonymi a Unią Europejską są największe na świecie i stanowią podstawę stosunków gospodarczych między USA a UE o wartości 7,1 bln USD, które zapewniają miliony miejsc pracy po obu stronach Atlantyku. Przedsiębiorstwa, które wykorzystują transatlantyckie przepływy danych, działają we wszystkich sektorach przemysłu i zaliczają się do nich zarówno największe spółki znajdujące się na liście Fortune 500, jak i liczne małe i średnie przedsiębiorstwa. Transatlantyckie przepływy danych umożliwiają amerykańskim podmiotom przetwarzanie danych potrzebnych do stworzenia oferty towarów i usług dla osób fizycznych z UE oraz możliwości zatrudnienia tych osób.

Departament zaangażuje się w ścisłą i produktywną współpracę z naszymi partnerami w UE w celu skutecznego zarządzania programem ram ochrony danych i nadzoru nad nim. Zaangażowanie to znajduje odzwierciedlenie w opracowywaniu i stałym udoskonalaniu przez departament różnych zasobów wspierających podmioty w procesie samocertyfikacji, utworzeniu strony internetowej zapewniającej ukierunkowane informacje zainteresowanym stronom, współpracy z Komisją i europejskimi organami ochrony danych w celu opracowania wytycznych wyjaśniających ważne elementy DPF UE–USA, działaniach informacyjnych służących ułatwieniu lepszego zrozumienia obowiązków podmiotów w zakresie ochrony danych, a także w nadzorze nad przestrzeganiem przez podmioty wymogów programu i jego monitorowaniu.

Nasza stała współpraca z cenionymi partnerami z UE umożliwi departamentowi zapewnienie skutecznego funkcjonowania DPF UE–USA. Rząd Stanów Zjednoczonych ma długą historię współpracy z Komisją służącej propagowaniu wspólnych zasad ochrony danych, niwelowaniu różnic w naszych podejściach prawnych przy jednoczesnym wspieraniu handlu i wzrostu gospodarczego w Unii Europejskiej i Stanach Zjednoczonych. Uważamy, że DPF UE–USA, które stanowią przykład takiej współpracy, pozwolą Komisji na wydanie nowej decyzji stwierdzającej odpowiedni stopień ochrony, która umożliwi podmiotom wykorzystywanie DPF UE–USA przy przekazywaniu danych osobowych z Unii Europejskiej do Stanów Zjednoczonych zgodnie z prawem UE.

Zarządzanie programem ram ochrony danych i nadzór nad nim przez Departament Handlu

Departament jest w pełni zaangażowany w skuteczne zarządzanie programem ram ochrony danych i nadzór nad nim oraz podejmie odpowiednie działania i przeznaczy odpowiednie zasoby, aby zapewnić osiągnięcie tego celu. Departament będzie prowadził i publicznie udostępniał oficjalny wykaz amerykańskich podmiotów, które dokonały samocertyfikacji w departamencie i zadeklarowały swoje zobowiązanie do przestrzegania zasad („wykaz DPF"), który będzie aktualizować na podstawie corocznych zgłoszeń dotyczących ponownej certyfikacji dokonywanych przez podmioty uczestniczące oraz poprzez usuwanie z niego podmiotów, jeżeli wycofają się one dobrowolnie, nie spełnią wymogu corocznej ponownej certyfikacji zgodnie z procedurami departamentu lub zostaną uznane za uporczywie nieprzestrzegające zasad. Departament będzie również prowadził i publicznie udostępniał oficjalny rejestr amerykańskich podmiotów, które usunięto z wykazu DPF, i określi powód, dla którego usunięto poszczególne podmioty. Wyżej wymieniony oficjalny wykaz i rejestr pozostaną publicznie dostępne na stronie internetowej departamentu dotyczącej ram ochrony danych. Strona internetowa dotycząca ram ochrony danych będzie zawierać umieszczone w widocznym miejscu wyjaśnienie, że każdy podmiot usunięty z wykazu DPF musi zaprzestać twierdzenia, że uczestniczy w DPF UE–USA lub ich przestrzega i że może otrzymywać dane osobowe zgodnie z DPF UE–USA. Podmiot taki musi jednak nadal stosować zasady do danych osobowych, które otrzymał w czasie, gdy uczestniczył w DPF UE–USA dopóty, dopóki przechowuje takie dane. Departament, w ramach nadrzędnego, stałego zaangażowania w skuteczne zarządzanie programem ram ochrony danych i nadzór nad nim, konkretnie podejmuje działania opisane poniżej.

Weryfikacja wymogów samocertyfikacji

— Departament, przed sfinalizowaniem samocertyfikacji podmiotu lub corocznej ponownej certyfikacji (zwanych łącznie „samocertyfikacją") i umieszczeniem go w wykazie DPF, zweryfikuje, czy podmiot co najmniej spełnił odpowiednie wymagania określone w zasadzie uzupełniającej dotyczącej samocertyfikacji w kwestii tego, jakie informacje podmiot musi podać w swoim zgłoszeniu samocertyfikacji złożonym w departamencie, i dostarczył w odpowiednim czasie odpowiednią politykę prywatności, w której informuje się osoby fizyczne o wszystkich 13 wymienionych elementach określonych w zasadzie powiadomienia. Departament zweryfikuje, czy podmiot:

— zidentyfikował podmiot zgłaszający samocertyfikację, a także wszelkie amerykańskie jednostki lub amerykańskie spółki zależne podmiotu dokonującego samocertyfikacji, które również przestrzegają zasad a które podmiot chce objąć swoją samocertyfikacją;

— przekazał wymagane informacje kontaktowe (np. informacje kontaktowe konkretnych osób fizycznych lub biur w ramach podmiotu dokonującego samocertyfikacji odpowiedzialnych za rozpatrywanie skarg, wniosków o udostępnienie danych oraz wszelkich innych kwestii wynikających z DPF UE–USA);

— opisała cele, dla których podmiot będzie gromadzić i wykorzystywać dane osobowe otrzymane z Unii Europejskiej;

— wskazał, jakie dane osobowe byłyby otrzymywane z Unii Europejskiej w oparciu o DPF UE–USA, a zatem byłyby objęte jego samocertyfikacją;

— w przypadku gdy podmiot prowadzi ogólnodostępną stronę internetową, dostarczył adres strony internetowej, na której dostępna jest odpowiednia polityka ochrony prywatności, lub w przypadku gdy podmiot nie prowadzi ogólnodostępnej strony internetowej, przedłożył w departamencie kopię swojej polityki ochrony prywatności i udzielił informacji, gdzie polityka ta jest dostępna do wglądu dla objętych nią osób fizycznych (tj. objętych nią pracowników, jeżeli odpowiednia polityka ochrony prywatności jest polityką ochrony prywatności w zakresie zasobów ludzkich, lub ogółu społeczeństwa, jeśli dana polityka ochrony prywatności nie jest polityką ochrony prywatności w zakresie zasobów ludzkich);

— zawarł w swojej odpowiedniej polityce ochrony prywatności we właściwym czasie (tj. początkowo wyłącznie w projekcie polityki ochrony prywatności dostarczonym wraz ze zgłoszeniem, jeśli to zgłoszenie stanowi wstępną samocertyfikację; w przeciwnym razie w ostatecznej i – w stosownych przypadkach – opublikowanej polityce ochrony prywatności) oświadczenie, że przestrzega zasad, oraz link lub adres strony internetowej departamentu dotyczącej ram ochrony danych (np. strony głównej lub strony internetowej zawierającej wykaz DPF);

— zawarł w swojej odpowiedniej polityce ochrony prywatności we właściwym czasie wszystkie 12 pozostałych wymienionych elementów określonych w zasadzie powiadomienia (np. możliwość – po spełnieniu określonych warunków – wystąpienia o arbitraż przez objętą nią osobę fizyczną z UE; wymóg ujawnienia danych osobowych na zgodny z prawem wniosek organów publicznych, w tym w celu spełnienia wymogów bezpieczeństwa narodowego lub na potrzeby egzekwowania prawa; swoją odpowiedzialność w razie dalszego przekazywania danych stronom trzecim);

— wskazał konkretny organ ustawowy właściwy do rozpatrywania wszelkich skarg na podmiot dotyczących możliwych nieuczciwych lub wprowadzających w błąd praktyk oraz naruszenia przepisów ustawowych lub wykonawczych regulujących ochronę prywatności (wymieniony w zasadach lub w przyszłym załączniku do zasad);

— wskazał wszelkie programy ochrony prywatności, których jest członkiem;

— wskazał, czy odpowiednia metoda (tj. procedury kontrolne, które musi zapewnić) weryfikacji zgodności z zasadami stanowi „samoocenę" (tj. weryfikację wewnętrzna) czy „zewnętrzny przegląd zgodności" (tj. weryfikację przez stronę trzecią), a jeśli określiła odpowiednią metodę jako zewnętrzny przegląd zgodności, wskazała również stronę trzecią, która przeprowadziła tę kontrolę;

— wskazał niezależny mechanizm ochrony prawnej dostępny do rozpatrywania skarg wniesionych na podstawie zasad oraz zagwarantował odpowiednie możliwości ochrony prawnej, z których zainteresowane osoby fizyczne mogą korzystać nieodpłatnie.

— Jeżeli podmiot wybrał niezależny mechanizm ochrony prawnej oferowany przez organ ds. rozstrzygania sporów z sektora prywatnego, zawarł w swojej odpowiedniej polityce ochrony prywatności link do odpowiedniej strony internetowej lub formularza skargi lub ich adres, które są dostępne w ramach mechanizmu w celu rozpatrzenia nierozstrzygniętych skarg wniesionych na podstawie zasad.

— Jeśli podmiot jest zobowiązany (tj. w odniesieniu do danych o zasobach ludzkich przekazywanych z Unii Europejskiej w kontekście stosunku pracy) albo zdecydował się współpracować z odpowiednimi organami ochrony danych przy badaniu i rozstrzyganiu skarg wniesionych na podstawie zasad, zadeklarował swoje zobowiązanie do współpracy z organami ochrony danych i przestrzegania ich zaleceń dotyczących podjęcia konkretnych działań w celu przestrzegania zasad.

— Departament zweryfikuje również, czy zgłoszenie przez podmiot samocertyfikacji jest zgodne z jej odpowiednią polityką prywatności. W przypadku gdy podmiot dokonujący samocertyfikacji chce objąć którąkolwiek ze swoich amerykańskich jednostek lub spółek zależnych, które mają odrębne odpowiednie polityki prywatności, departament dokona również przeglądu odpowiednich polityk prywatności takich objętych jednostek lub spółek zależnych, aby upewnić się, że zawierają one wszystkie wymagane elementy określone w zasadzie powiadomienia.

— Departament będzie współpracował z organami ustawowymi (np. FTC i DoT) w celu zweryfikowania, czy podmioty podlegają jurysdykcji odpowiedniego organu ustawowego wskazanego w ich zgłoszeniach samocertyfikacji, w przypadku gdy departament ma powody, by wątpić, że podlegają one tej jurysdykcji.

— Departament będzie współpracować z organami ds. rozstrzygania sporów z sektora prywatnego w celu sprawdzenia, czy podmioty są czynnie zarejestrowane w niezależnym mechanizmie ochrony prawnej wskazanym w ich zgłoszeniu samocertyfikacji; oraz współpracować z tymi organami w celu zweryfikowania, czy podmioty są czynnie zarejestrowane do zewnętrznego przeglądu zgodności wskazanego w ich zgłoszeniu samocertyfikacji, w przypadku gdy organy te mogą oferować oba rodzaje usług.

— Departament będzie współpracować z wybraną przez siebie stroną trzecią, która będzie depozytariuszem środków zebranych w ramach poboru opłaty na rzecz panelu organów ochrony danych (tj. rocznej opłaty przeznaczonej na pokrycie kosztów operacyjnych panelu organów ochrony danych) w celu sprawdzenia, czy podmioty wybierające organ ochrony danych jako niezależny mechanizm ochrony prawnej uiściły opłatę za dany rok.

— Departament będzie współpracować z wybraną przez siebie stroną trzecią do administrowania postępowaniami arbitrażowymi zgodnie z załącznikiem I do zasad oraz zarządzania funduszem arbitrażowym określonym w tym załączniku, aby zweryfikować, czy podmioty wniosły wkład do tego funduszu arbitrażowego.

— W przypadku gdy departament zidentyfikuje jakiekolwiek problemy podczas przeglądu dokonanych przez podmioty zgłoszeń samocertyfikacji, poinformuje je o konieczności rozwiązania wszystkich takich problemów w odpowiednich ramach czasowych wyznaczonych przez departament ([2]). Departament poinformuje je również, że brak odpowiedzi w wyznaczonych przez niego ramach czasowych lub inne niespełnienie wymogu samocertyfikacji zgodnie z procedurami departamentu doprowadzi do uznania tych zgłoszeń samocertyfikacji za zaniechane oraz że wszelkie fałszywe informacje na temat uczestnictwa podmiotu w DPF UE–USA lub zgodności z nimi mogą podlegać czynnościom egzekucyjnym ze strony FTC, DoT lub innego odpowiedniego organu rządowego. Departament poinformuje podmioty w sposób wskazany mu przez te podmioty.

Ułatwianie współpracy z organami ds. rozstrzygania sporów świadczącymi usługi związane z zasadami

— Departament będzie współpracował z organami ds. rozstrzygania sporów z sektora prywatnego zapewniającymi niezależne mechanizmy ochrony prawnej umożliwiające zbadanie nierozstrzygniętych skarg wniesionych zgodnie z zasadami, w celu sprawdzenia, czy spełniają one co najmniej wymagania określone w zasadzie uzupełniającej dotyczącej rozstrzygania sporów i egzekwowania prawa. Departament sprawdzi, czy:

  — zamieszczają one na swoich ogólnodostępnych stronach internetowych informacje na temat zasad oraz usług świadczonych przez siebie w zakresie DPF UE–USA, które muszą obejmować: 1) informacje na temat wymogów dotyczących niezależnych mechanizmów ochrony prawnej ustanowionych w zasadach lub link do takich informacji; 2) link do strony internetowej departamentu dotyczącej ram ochrony danych; 3) wyjaśnienie, że usługi rozwiązywania sporów w DPF UE–USA są świadczone na rzecz osób fizycznych nieodpłatnie; 4) opis procedury składania skargi dotyczącej kwestii związanych z zasadami; 5) wyznaczenie terminu na rozpoznanie skarg dotyczących zasad; oraz 6) opis zakresu potencjalnych środków ochrony prawnej. Departament terminowo powiadamia te organy o istotnych zmianach w nadzorze departamentu i zarządzaniu programem ram ochrony danych w przypadku, gdy takie zmiany są nieuchronne lub gdy zostały już wprowadzone oraz gdy są one istotne dla roli, jaką organy odgrywają w DPF UE–USA;

([2]) Przykładowo w przypadku ponownej certyfikacji oczekuje się, że podmioty rozwiążą wszelkie takie problemy w terminie 45 dni; z zastrzeżeniem wyznaczenia przez departament innych, odpowiednich ram czasowych.

— publikuje sprawozdanie roczne zawierające zagregowane dane statystyczne dotyczące świadczonych przez siebie usług w zakresie rozstrzygania sporów, które musi obejmować: 1) łączną liczbę skarg związanych z zasadami otrzymanych w roku sprawozdawczym; 2) rodzaje otrzymanych skarg; 3) wskaźniki pomiaru jakości rozstrzygania sporów, np. czas niezbędny do rozpatrzenia skarg; oraz 4) wyniki rozpatrywania otrzymanych skarg, w szczególności liczbę i rodzaj zastosowanych środków ochrony prawnej lub nałożonych sankcji. Departament przekaże organom szczegółowe, uzupełniające wytyczne dotyczące informacji, które powinny one przedstawić w sprawozdaniach rocznych, zawierające objaśnienia tych wymogów (np. wykaz konkretnych kryteriów, które musi spełniać skarga, aby została uznana za skargę związaną z zasadami dla celów sprawozdania rocznego), a także określające inne rodzaje informacji, które powinny przedstawić (np. jeśli organ świadczy również usługę weryfikacji związanej z zasadami, opis sposobu, w jaki organ unika wszelkich faktycznych lub potencjalnych konfliktów interesów w sytuacjach, gdy świadczy na rzecz podmiotu zarówno usługi w zakresie weryfikacji, jak i rozstrzygania sporów). W dodatkowych wytycznych departament określi również datę, do której organy powinny opublikować sprawozdania roczne za odpowiedni okres sprawozdawczy.

Działania następcze w odniesieniu do podmiotów, które pragną zostać usunięte lub które usunięto z wykazu podmiotów objętych DPF.

— Jeżeli podmiot pragnie wycofać się z DPF UE–USA, departament będzie wymagał od niego usunięcia z każdej odpowiedniej polityki ochrony prywatności wszelkich odniesień do DPF UE–USA, które sugerują, że podmiot wciąż uczestniczy w DPF UE–USA i że może otrzymywać dane osobowe zgodnie z DPF UE–USA (*zob*. opis zobowiązania departamentu do wyszukiwania fałszywych oświadczeń o uczestnictwie). Departament będzie również wymagał od podmiotów uczestniczących w wypełnienia i złożenia w departamencie szczegółowego kwestionariusza w celu weryfikacji:

  — jego wniosku o wycofanie się;

  — wyboru poniższych czynności, które wykona w odniesieniu do danych osobowych otrzymanych w oparciu o DPF UE–USA, gdy uczestniczył w DPF UE–USA: a) zatrzymanie takich danych, dalsze stosowanie zasad w odniesieniu do takich danych i coroczne potwierdzanie wobec departamentu swojego zobowiązania do stosowania zasad w odniesieniu do takich danych; b) zatrzymanie takich danych i zapewnienie ich „odpowiedniej" ochrony za pomocą innych dozwolonych środków; c) zwrot lub usunięcie wszystkich takich danych w określonym terminie; oraz

  — osoby w ramach podmiotu, która będzie pełniła funkcję osoby odpowiedzialnej za bieżące kontakty w przypadku zapytań związanych z zasadami.

— Jeśli podmiot wybrał opcję opisaną bezpośrednio powyżej w lit. a), departament będzie również wymagał od niego, aby corocznie po wycofaniu się (tj. przed upłynięciem roku od dnia wycofania się, a następnie przed każdą kolejną rocznicą, chyba że podmiot zapewni „odpowiednią" ochronę takich danych za pomocą innych dozwolonych środków albo zwróci lub usunie wszystkie takie dane i powiadomi departament o tym działaniu) wypełniał odpowiedni kwestionariusz i składał go w departamencie w celu sprawdzenia, co zrobił z tymi danymi osobowymi, co zrobi z częścią tych danych osobowych, które nadal przechowuje, oraz kto w ramach podmiotu będzie pełnił funkcję osoby odpowiedzialnej za bieżące kontakty w przypadku zapytań związanych z zasadami.

— Jeśli podmiot dopuścił do wygaśnięcia samocertyfikacji (tj. nie spełnił wymogu corocznej ponownej certyfikacji przestrzegania zasad ani nie został usunięty z wykazu DPF z innego powodu, takiego jak wycofanie), departament zarządzi, aby wypełnił odpowiedni kwestionariusz w celu sprawdzenia, czy chce się wycofać czy dokonać ponownej certyfikacji, oraz złożył go w departamencie:

  — oraz jeśli pragnie się wycofać – dodatkowo zweryfikował, co zrobi z danymi osobowymi, które otrzymał w oparciu o DPF UE–USA, gdy uczestniczył w DPF UE–USA (*zob*. wcześniejszy opis kwestii, które podmiot musi zweryfikować, jeśli chce się wycofać);

  — a jeśli zamierza dokonać ponownej certyfikacji – dodatkowo zweryfikował, czy w okresie wygaśnięcia statusu certyfikacji stosował zasady w odniesieniu do danych osobowych otrzymanych w oparciu o DPF UE–USA i wyjaśnił, jakie kroki podejmie w celu rozwiązania nierozstrzygniętych kwestii, które opóźniły jego ponowną certyfikację.

— Jeśli podmiot zostanie usunięty z wykazu DPF z któregokolwiek z poniższych powodów: a) wycofania się z uczestnictwa w DPF UE–USA, b) niespełnienia wymogu corocznej ponownej certyfikacji (tj. albo rozpoczął, ale nie ukończył corocznego procesu ponownej certyfikacji w odpowiednim czasie, albo nawet nie rozpoczął corocznego procesu ponownej certyfikacji) lub c) „uporczywego nieprzestrzegania zasad", departament wyśle zawiadomienie do osób odpowiedzialnych za kontakty wskazanych w zgłoszeniu samocertyfikacji podmiotu, określając przyczynę usunięcia i wyjaśniając, że musi zaprzestać wszelkich wyraźnych lub dorozumianych oświadczeń, że uczestniczy w DPF UE–USA lub ich przestrzega oraz że może otrzymywać dane osobowe zgodnie z DPF UE–USA. W zawiadomieniu, które może również zawierać inne treści dostosowane do przyczyny usunięcia, będzie wskazane, że wobec podmiotów podających fałszywe informacje na temat swojego uczestnictwa w DPF UE–USA lub zgodności z DPF UE–USA, również w przypadku gdy oświadczają, iż uczestniczą w DPF UE–USA, po usunięciu z wykazu DPF, FTC, DoT lub inne odpowiednie organy rządowe mogą wszcząć odpowiednie czynności egzekucyjne.

Wyszukiwanie fałszywych oświadczeń dotyczących uczestnictwa w programie i przeciwdziałanie im

— Na bieżąco, w przypadku gdy podmiot: a) wycofał się z uczestnictwa w DPF UE–USA, b) nie spełnił wymogu corocznej ponownej certyfikacji (tj. albo rozpoczął, ale nie ukończył corocznego procesu ponownej certyfikacji w odpowiednim czasie, albo nawet nie rozpoczął corocznego procesu ponownej certyfikacji), c) został usunięty z wykazu podmiotów uczestniczących w DPF UE–USA, w szczególności z powodu „uporczywego nieprzestrzegania zasad", lub d) nie spełnił wymogu wstępnej samocertyfikacji potwierdzającej zobowiązanie do przestrzegania zasad (tj. rozpoczął, ale nie ukończył procesu wstępnej certyfikacji w odpowiednim czasie), departament będzie podejmować z urzędu działania mające na celu sprawdzenie, czy jakakolwiek opublikowana polityka prywatności podmiotu nie zawiera odniesień do DPF UE–USA, które sugerowałyby, że podmiot uczestniczy w DPF UE–USA i że może otrzymywać dane osobowe zgodnie z DPF UE–USA.. Jeżeli departament ustali, że istnieją takie odniesienia, poinformuje podmiot, że – w stosownych przypadkach – skieruje sprawę do odpowiedniego organu, zwracając się o ewentualne wszczęcie odpowiedniego postępowania, jeżeli podmiot ten nadal będzie podawał fałszywe informacje na temat uczestnictwa w DPF UE–USA. Departament poinformuje podmiot w sposób wskazany przez ten podmiot lub, w stosownych przypadkach, w inny odpowiedni sposób. Jeżeli podmiot nie usunie odniesień ani nie dokona samocertyfikacji zobowiązującej go do przestrzegania zasad DPF UE–USA zgodnie z procedurami departamentu, departament z urzędu skieruje sprawę do FTC, DoT lub innego odpowiedniego organu egzekwowania prawa lub też podejmie stosowne działanie służące wyegzekwowaniu znaku certyfikacyjnego DPF UE–USA;

— Departament będzie podejmował inne działania służące zidentyfikowaniu fałszywych oświadczeń dotyczących uczestnictwa w DPF UE–USA i przypadków niewłaściwego wykorzystywania znaku certyfikacyjnego DPF UE–USA, w tym przez podmioty, które w przeciwieństwie do podmiotów opisanych bezpośrednio powyżej nigdy nawet nie rozpoczęły procesu samocertyfikacji (np. przeprowadzając odpowiednie wyszukiwania w internecie w celu zidentyfikowania odniesień do DPF UE–USA w politykach ochrony prywatności podmiotu). Jeżeli w wyniku takich działań departament zidentyfikuje fałszywe oświadczenia o uczestnictwie w DPF UE–USA i niewłaściwym użyciu znaku certyfikacyjnego DPF UE–USA, poinformuje podmiot, że – w stosownych przypadkach – skieruje sprawę do odpowiedniego organu, zwracając się o ewentualne wszczęcie odpowiedniego postępowania, jeżeli podmiot ten nadal będzie podawał fałszywe informacje na temat uczestnictwa w DPF UE–USA. Departament poinformuje podmiot w sposób, który ewentualnie został wskazany przez ten podmiot, lub, w stosownych przypadkach, w inny odpowiedni sposób. Jeżeli podmiot nie usunie odniesień ani nie dokona samocertyfikacji zobowiązującej go do przestrzegania zasad DPF UE–USA zgodnie z procedurami departamentu, departament z urzędu skieruje sprawę do FTC, DoT lub innego odpowiedniego organu egzekwowania prawa lub też podejmie stosowne działanie służące wyegzekwowaniu znaku certyfikacyjnego DPF UE–USA;

— Departament niezwłocznie przeanalizuje konkretne, poważne skargi dotyczące fałszywych oświadczeń o uczestnictwie w DPF UE–USA, które otrzyma (np. otrzymane skargi ze strony organów ochrony danych, niezależnych mechanizmów ochrony prawnej zapewnianych przez organy ds. pozasądowego rozstrzygania sporów z sektora prywatnego, osób, których dane dotyczą, przedsiębiorstw z UE i USA oraz innych rodzajów stron trzecich), i odpowie na nie; oraz

— Departament może podjąć inne odpowiednie działania naprawcze. Podanie fałszywych informacji departamentowi może stanowić podstawę wszczęcia postępowania na podstawie ustawy o fałszywych oświadczeniach (tytuł 18 § 1001 U.S.C.).

Dokonywanie z urzędu przeglądów i oceny przestrzegania zasad programu ram ochrony danych

— Departament będzie na bieżąco podejmował działania w zakresie monitorowania przestrzegania zasad przez podmioty uczestniczące w DPF UE–USA, aby wskazać problemy, które mogą wymagać podjęcia działań następczych. W szczególności departament będzie przeprowadzać z urzędu kontrole wyrywkowe losowo wybranych podmiotów uczestniczących w DPF UE–USA, a także kontrole wyrywkowe *ad hoc* określonych podmiotów uczestniczących w DPF UE–USA w przypadku, gdy wykryte zostaną potencjalne problemy dotyczące zgodności (np. potencjalne problemy w zakresie zgodności zgłoszone Departamentowi przez strony trzecie) w celu sprawdzenia, czy: a) osoby odpowiedzialne za kontakty w kwestii rozpatrywania skarg, wniosków o udostępnienie danych oraz innych kwestii wynikających z DPF UE–USA są dostępne; b) w stosownych przypadkach, polityka prywatności podmiotu jest łatwo dostępna dla ogółu społeczeństwa, zarówno na stronie internetowej podmiotu, jak i za pośrednictwem linku w wykazie DPF; c) polityka prywatności podmiotu jest niezmiennie zgodna z wymogami samocertyfikacji opisanymi w zasadach; oraz d) niezależny mechanizm ochrony prawnej wskazany przez podmiot jest dostępny do rozpatrywania skarg wniesionych na podstawie DPF UE–USA. Departament będzie również aktywnie monitorować wiadomości w poszukiwaniu doniesień dostarczających wiarygodnych dowodów niezgodności podmiotów uczestniczących w DPF UE–USA.

— W ramach przeglądu zgodności departament będzie wymagał od podmiotów uczestniczących w DPF UE–USA wypełnienia szczegółowego kwestionariusza i złożenia go w departamencie, gdy: a) departament otrzymał jakiekolwiek konkretne poważne skargi dotyczące nieprzestrzegania zasad przez podmiot, b) podmiot nie reaguje w zadowalający sposób na zapytania z departamentu dotyczące informacji związanych z DPF UE–USA lub c) istnieją przekonujące dowody na to, że podmiot nie dochowuje swoich zobowiązań w zakresie DPF UE–USA. W przypadku gdy departament wysłał taki szczegółowy kwestionariusz do podmiotu, a podmiot ten nie udzieli satysfakcjonującej odpowiedzi na kwestionariusz, departament poinformuje podmiot, że – w stosownych przypadkach – przekaże sprawę do odpowiedniego organu w celu podjęcia ewentualnych czynności egzekucyjnych, jeśli nie otrzyma terminowej i satysfakcjonującej odpowiedzi od tego podmiotu. Departament poinformuje podmiot w sposób wskazany przez ten podmiot lub, w stosownych przypadkach, w inny odpowiedni sposób. Jeżeli podmiot nie odpowie w sposób terminowy i zadowalający, departament z urzędu przekaże sprawę do FTC, DoT lub innego odpowiedniego organu egzekwowania prawa lub podejmie inne stosowne działanie służące zapewnieniu zgodności. departament konsultuje się – w stosownych przypadkach – z właściwymi organami ochrony danych w związku z takimi przeglądami przestrzegania zasad; oraz

— departament będzie przeprowadzał okresową ocenę zarządzania programem ram ochrony danych i nadzoru nad nim w celu zapewnienia, aby działania podejmowane w związku z monitorowaniem, w tym działania podejmowane z wykorzystaniem narzędzi do wyszukiwania (np. w celu sprawdzenia martwych linków do polityk ochrony prywatności podmiotów uczestniczących w DPF UE–USA) były adekwatne pod kątem rozwiązania nowych problemów, gdy te się pojawią.

Dostosowanie strony internetowej dotyczącej ram ochrony danych do indywidualnych potrzeb docelowych odbiorców

Departament dostosuje stronę internetową dotyczącą ram ochrony danych, aby uwzględnić następujące grupy docelowe: osoby fizyczne z UE, przedsiębiorstwa z UE i przedsiębiorstwa z USA i organy ochrony danych. Udostępnienie na stronie materiałów skierowanych bezpośrednio do osób fizycznych z UE i przedsiębiorstw z UE zwiększy przejrzystość na wiele sposobów. W odniesieniu do osób fizycznych z UE strona internetowa będzie zawierać dokładne wyjaśnienie: 1) praw, jakie przysługują osobom fizycznym z UE w DPF UE–USA; 2) mechanizmów ochrony prawnej dostępnych dla osób fizycznych z UE, jeżeli uważają one, że podmiot nie dochował swojego zobowiązania do przestrzegania zasad; oraz 3) jak znaleźć informacje dotyczące samocertyfikacji podmiotu w DPF UE–USA. W odniesieniu do przedsiębiorstw z UE ułatwi ona sprawdzenie: 1) czy podmiot uczestniczy w DPF UE–USA; 2) rodzaju informacji objętych samocertyfikacją podmiotu w DPF UE–USA; 3) polityki ochrony prywatności mającej zastosowanie do danych objętych samocertyfikacją; oraz 4) metody, jaką wykorzystuje podmiot do kontroli przestrzegania przez nią zasad. W odniesieniu do przedsiębiorstw z USA będzie ona zawierać dokładne wyjaśnienie: 1) przywilejów wynikających z uczestnictwa w DPF UE–USA; 2) sposobu przystąpienia do DPF UE–USA, a także sposób ponownego dokonania certyfikacji i wycofania się z DPF UE–USA; oraz 3) sposobu zarządzania przez Stany Zjednoczone DPF UE–USA i ich egzekwowania. Uwzględnienie materiałów skierowanych bezpośrednio do organów ochrony danych (np. informacji o osobie odpowiedzialnej za kontakty w departamencie ds. kontaktów z organami ochrony danych oraz linku do treści związanych z zasadami na stronie internetowej FTC) zarówno ułatwi współpracę, jak i poprawi przejrzystość. Departament będzie również współpracował na zasadzie *ad hoc* z Komisją i Europejską Radą Ochrony Danych („EROD") w celu opracowania dodatkowych, aktualnych materiałów (np. odpowiedzi na często zadawane pytania) do wykorzystania na stronie internetowej dotyczącej ram ochrony danych, w przypadkach gdy takie informacje ułatwiłyby skuteczne zarządzanie programem ram ochrony danych i nadzór nad nim.

Usprawnianie współpracy z organami ochrony danych

Aby zwiększyć możliwości współpracy z organami ochrony danych, departament wyznaczy specjalną osobę odpowiedzialną za kontakty w departamencie, która będzie pełniła funkcję łącznika z organami ochrony danych. W przypadkach, w których organ ochrony danych uzna, że podmiot uczestniczący w DPF UE–USA nie przestrzega zasad, w tym w następstwie skargi złożonej przez osobę fizyczną z UE, organ ochrony danych będzie mógł skontaktować się ze specjalną osobą odpowiedzialną za kontakty w departamencie w celu skierowania sprawy tego podmiotu do dalszego rozpoznania. Departament dołoży wszelkich starań, aby ułatwić rozstrzygnięcie skargi na podmiot uczestniczący w DPF UE–USA. W terminie 90 dni od otrzymania skargi departament przekaże organowi ochrony danych aktualne informacje. Osoba odpowiedzialna za kontakty będzie również otrzymywała zgłoszenia dotyczące podmiotów, które nieprawdziwie twierdzą, że uczestniczą w DPF UE–USA. Osoba odpowiedzialna za kontakty będzie monitorowała wszystkie zgłoszenia, jakie departament otrzymuje od organów ochrony danych; ponadto departament przedstawi sprawozdanie – we wspólnym przeglądzie opisanym poniżej – zawierające łączną analizę otrzymanych w danym roku skarg. Osoba odpowiedzialna za kontakty będzie wspierała organy ochrony danych w poszukiwaniu informacji dotyczących konkretnej samocertyfikacji podmiotu lub jego wcześniejszego uczestnictwa w DPF UE–USA i będzie odpowiadała na zapytania organu ochrony danych dotyczące realizacji określonych wymogów DPF UE–USA. Departament będzie również współpracować z Komisją i EROD w zakresie w zakresie proceduralnych i administracyjnych aspektów panelu organów ochrony danych, w tym ustanowienia odpowiednich procedur dystrybucji środków zebranych w ramach poboru opłaty na rzecz panelu organów ochrony danych. Rozumiemy, że Komisja będzie współpracować z departamentem w celu usprawnienia rozwiązania wszelkich problemów, które mogą pojawić się w związku z tymi procedurami. Ponadto departament przekaże organom ochrony danych materiały dotyczące DPF UE–USA, aby organy mogły opublikować te materiały na swoich stronach internetowych w celu zagwarantowania większej przejrzystości względem osób fizycznych i przedsiębiorstw z UE. Wyższy stopień świadomości na temat DPF UE–USA oraz praw i obowiązków, jakie z niej płyną, powinien przyczynić się do identyfikacji problemów, gdy te się pojawią, tak aby można je było rozwiązać w odpowiedni sposób.

Wypełnienie zobowiązań wynikających z załącznika I do zasad

Departament będzie wypełniał zobowiązania wynikające z załącznika I do zasad, w tym prowadził wykaz arbitrów wybranych wspólnie z Komisją ze względu na ich niezależność, uczciwość i wiedzę fachową; oraz, w stosownych przypadkach, wspierał stronę trzecią wybraną przez departament do administrowania postępowaniami arbitrażowymi na podstawie załącznika I do zasad i zarządzania funduszem arbitrażowym określonym w tym załączniku ([3]). Departament będzie współpracować ze stroną trzecią m.in. w celu sprawdzenia, czy strona trzecia prowadzi stronę internetową zawierającą wytyczne dotyczące procesu arbitrażu, w tym: 1) sposobu wszczynania postępowań i składania dokumentów; 2) wykazu arbitrów prowadzonego przez departament oraz sposobu wyboru arbitrów z tego wykazu; 3) obowiązujących procedur arbitrażowych i kodeksu postępowania arbitra przyjętych przez departament i Komisję ([4]); oraz 4) pobierania i uiszczania opłat arbitrażowych. Ponadto departament będzie współpracował ze stroną trzecią w celu dokonania okresowego przeglądu funkcjonowania funduszu arbitrażowego, w tym konieczności dostosowania kwoty składek lub górnej granicy (*tj.* maksymalnych kwot) kosztów arbitrażu, oraz przeanalizuje między innymi liczbę postępowań arbitrażowych oraz ich koszty i czas trwania, przy założeniu, że nie zostaną nałożone żadne nadmierne obciążenia finansowe na podmioty uczestniczące w DPF UE–USA. Departament powiadomi Komisję o wynikach takich przeglądów dokonanych we współpracy ze stroną trzecią i z wyprzedzeniem powiadomi Komisję o wszelkich korektach kwoty składek.

Przeprowadzanie wspólnego przeglądu funkcjonowania DPF UE–USA

Departament i inne organy – w stosownych przypadkach – będą organizowały okresowe spotkania z Komisją, zainteresowanymi organami ochrony danych i odpowiednimi przedstawicielami EROD, podczas których departament przekaże aktualne informacje na temat DPF UE–USA. Spotkania będą obejmowały omówienie bieżących problemów dotyczących funkcjonowania, wdrażania i egzekwowania programu ram ochrony danych oraz nadzoru nad nim. Spotkania mogą, w stosownych przypadkach, obejmować dyskusję na powiązane tematy, takie jak inne mechanizmy przekazywania danych, które korzystają z zabezpieczeń w zakresie DPF UE–USA.

([3]) Międzynarodowe Centrum Rozstrzygania Sporów („ICDR"), czyli dział ds. międzynarodowych Amerykańskiego Stowarzyszenia Arbitrażowego („AAA") (określane zbiorczo „ICDR-AAA"), zostało wybrane przez departament do administrowania postępowaniami arbitrażowymi na podstawie i zarządzania funduszem arbitrażowym określonym w załączniku I do zasad.

([4]) 15 września 2017 r. departament i Komisja uzgodniły przyjęcie zestawu zasad arbitrażowych regulujących wiążące postępowania arbitrażowe opisane w załączniku I do zasad, a także kodeksu postępowania dla arbitrów, który jest zgodny z ogólnie przyjętymi standardami etycznymi dla arbitrów handlowych i załącznikiem I do zasad. Departament i Komisja uzgodniły, że zasady arbitrażu i kodeks postępowania będą aktualizowane w celu odzwierciedlenia aktualizacji DPF UE–USA, a departament będzie współpracował z ICDR-AAA w celu wprowadzenia tych aktualizacji.

Zmiany ustaw

Departament dołoży zasadnych starań, aby poinformować Komisję o istotnych zmianach w amerykańskim prawie, o ile zmiany odnoszą się do DPF UE–USA w dziedzinie ochrony danych oraz ograniczeń i gwarancji mających zastosowanie do dostępu do danych osobowych przez amerykańskie organy i późniejszego wykorzystania danych.

Dostęp rządu USA do danych osobowych

Stany Zjednoczone wydały rozporządzenie wykonawcze 14086 w sprawie poprawy zabezpieczeń dotyczących działań Stanów Zjednoczonych w zakresie rozpoznania radioelektronicznego oraz tytuł 28 część 201 kodeksu przepisów federalnych zmieniający przepisy Departamentu Sprawiedliwości w celu ustanowienia Sądu Odwoławczego ds. Ochrony Danych („DPRC"), które zapewniają silną ochronę danych osobowych w związku z dostępem rządowym do danych osobowych do celów bezpieczeństwa narodowego. Zapewniana ochrona obejmuje: ugruntowanie zabezpieczeń w zakresie ochrony prywatności i wolności obywatelskich w celu zapewnienia, aby działania USA w zakresie rozpoznania radioelektronicznego były niezbędne i proporcjonalne do osiągnięcia określonych celów bezpieczeństwa narodowego; ustanowienie nowego mechanizmu dochodzenia roszczeń z niezależnymi i wiążącymi uprawnieniami; oraz poprawę istniejącego rygorystycznego i wielowarstwowego nadzoru nad działaniami USA w zakresie rozpoznania radioelektronicznego. Dzięki tej ochronie osoby fizyczne z UE mogą dochodzić roszczeń w ramach nowego wielopoziomowego mechanizmu dochodzenia roszczeń, który obejmuje niezależny Sąd Odwoławczy ds. Ochrony Danych, składający się z osób wybranych spoza rządu USA, które miałyby pełne uprawnienia do rozpatrywania skarg i w razie potrzeby wskazywania środków zaradczych. Departament będzie prowadził rejestr osób fizycznych z UE, które złożyły kwalifikującą się skargę zgodnie z rozporządzeniem wykonawczym 14086 i tytułem 28 część 201 kodeksu przepisów federalnych. Po upływie pięciu lat od dnia sporządzenia niniejszego pisma, a następnie co pięć lat, departament będzie kontaktował się z odpowiednimi organami w sprawie tego, czy informacje dotyczące przeglądu kwalifikujących się skarg lub przeglądu wszelkich wniosków o przegląd złożonych do Sądu Odwoławczego ds. Ochrony Danych zostały odtajnione. Jeśli takie informacje zostały odtajnione, departament będzie współpracował z odpowiednim organem ochrony danych w celu poinformowania danej osoby fizycznej z UE. Te udoskonalenia stanowią potwierdzenie, że dane osobowe z UE przekazywane do Stanów Zjednoczonych będą traktowane w sposób zgodny z wymogami prawnymi UE dotyczącymi dostępu rządu do danych.

Mając na uwadze zasady, rozporządzenie wykonawcze 14086, tytuł 28 część 201 kodeksu przepisów federalnych oraz towarzyszące im pisma i materiały, w tym zobowiązania departamentu dotyczące zarządzania ramami ochrony danych i nadzoru nad nimi, oczekujemy, że Komisja uzna, iż DPF UE–USA zapewniają odpowiednią ochronę do celów prawa Unii i że dane z Unii Europejskiej nadal będą przekazywane podmiotom uczestniczącym w DPF UE–USA. Oczekujemy również, że przekazywanie danych do podmiotów amerykańskich w oparciu o standardowe klauzule umowne UE lub wiążące reguły korporacyjne UE będzie jeszcze łatwiejsze dzięki warunkom tych ustaleń.

Z poważaniem

Marisa LAGO

ZAŁĄCZNIK IV

STANY ZJEDNOCZONE AMERYKI
Federalna Komisja Handlu
Waszyngton 20580

Urząd Przewodniczącego

Dnia 9 czerwca 2023 r.

Didier Reynders
Komisarz do spraw wymiaru sprawiedliwości
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Belgia

Szanowny Panie Komisarzu!

Federalna Komisja Handlu Stanów Zjednoczonych („FTC") docenia możliwość omówienia swojej roli w zakresie egzekwowania zasad ram ochrony danych UE–USA („DPF UE–USA"). FTC od dawna angażuje się w ochronę konsumentów i prywatności ponad granicami, w związku z czym zobowiązujemy się do egzekwowania aspektów tych ram związanych z sektorem handlowym. FTC pełni tę funkcję od 2000 r. w związku z ramami programu „bezpieczna przystań" UE–USA i ostatnio od 2016 r. w związku z ramami Tarczy Prywatności UE–USA ([1]). 16 lipca 2020 r. Trybunał Sprawiedliwości Unii Europejskiej („TSUE") unieważnił decyzję Komisji Europejskiej stwierdzającą odpowiedni stopień ochrony stanowiącej podstawę Tarczy Prywatności UE–USA ze względu na kwestie inne niż zasady handlowe egzekwowane przez FTC. Stany Zjednoczone i Komisja Europejska od tego czasu negocjowały ramy ochrony danych UE–USA w celu uwzględnienia tego orzeczenia TSUE.

Pragnę potwierdzić zobowiązanie FTC do stanowczego egzekwowania zasad DPF UE–USA. Warto zauważyć, że potwierdzamy nasze zobowiązanie w trzech kluczowych obszarach: 1) określania pierwszeństwa zgłoszeń i ich badania; 2) ubieganie się o wydanie decyzji i ich monitorowanie; oraz 3) współpraca z unijnymi organami ochrony danych w zakresie egzekwowania prawa.

I. **Wprowadzenie**

a. **Działania FTC w zakresie polityki dotyczącej prywatności i jej egzekwowania**

FTC przysługują szerokie uprawnienia w dziedzinie egzekwowania prawa z zakresu administracji cywilnej na potrzeby rozpowszechniania ochrony konsumentów i konkurencji w sektorze związanym z działalnością handlową. W zakresie swoich kompetencji obejmujących ochronę konsumentów FTC wprowadza w życie bardzo zróżnicowane przepisy w celu ochrony

([1]) Pismo przewodniczącej Edith Ramirez do Věry Jourovej, komisarz do spraw sprawiedliwości, konsumentów i równouprawnienia płci Komisji Europejskiej, opisujące egzekwowanie nowych ram Tarczy Prywatności UE–USA przez Federalną Komisję Handlu (29 lutego 2016 r.), *dostępne pod adresem:* https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. FTC wcześniej zobowiązała się również do egzekwowania programu „bezpieczna przystań" UE–USA. Pismo Roberta Pitofskiego, przewodniczącego FTC, do Johna Mogga, dyrektora DG ds. Rynku Wewnętrznego, Komisja Europejska (14 lipca 2000 r.), *dostępne pod adresem:* https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. Pismo to zastępuje wspomniane wcześniejsze zobowiązania.

prywatności i bezpieczeństwa konsumentów i ich danych. W prawie pierwotnym stosowanym przez FTC, czyli w ustawie o Federalnej Komisji Handlu, zakazuje się „nieuczciwych" lub „wprowadzających w błąd" czynów lub praktyk handlowych lub wpływających na handel ([2]). FTC wykonuje również ustawy szczególne chroniące informacje na temat zdrowia, kredytów i innych kwestii finansowych i informacje internetowe na temat dzieci, oraz wydaje regulacje wdrażające te ustawy ([3]).

Ostatnio FTC podjęła również wiele inicjatyw mających na celu poprawę naszych działań na rzecz ochrony prywatności. W sierpniu 2022 r. FTC ogłosiła, że rozważa wprowadzenie zasad służących ograniczeniu szkodliwego nadzoru handlowego i niewystarczającego bezpieczeństwa danych ([4]). Celem tego projektu jest stworzenie solidnego rejestru publicznego, który pozwoli stwierdzić, czy FTC powinna wprowadzić zasady służące ograniczeniu praktyk w zakresie nadzoru handlowego i bezpieczeństwa danych oraz jak takie zasady powinny ewentualnie wyglądać. Z zadowoleniem przyjęliśmy uwagi zainteresowanych stron z UE na temat tej inicjatywy i innych inicjatyw.

W naszych konferencjach „PrivacyCon" nadal biorą udział czołowi naukowcy, którzy omawiają najnowsze badania naukowe i trendy związane z prywatnością konsumentów i bezpieczeństwem danych. Zwiększyliśmy również możliwości naszej agencji, aby dotrzymać kroku rozwojowi technologicznemu, który odgrywa tak ważną rolę w naszych działaniach na rzecz ochrony prywatności, przez stworzenie zespołu technologów i interdyscyplinarnych naukowców, który cały czas się powiększa. Jak Państwo wiedzą, ogłosiliśmy również wspólny dialog z Państwem oraz z Państwa kolegami i koleżankami z Komisji Europejskiej, który obejmuje zajęcie się takimi zagadnieniami związanymi z prywatnością, jak zwodnicze interfejsy i modele biznesowe charakteryzujące się wszechobecnym gromadzeniem danych ([5]). Niedawno przedstawiliśmy również Kongresowi sprawozdanie zawierające ostrzeżenie przed problemami związanymi z korzystaniem ze sztucznej inteligencji („AI") w celu wyeliminowania problemów internetowych zidentyfikowanych przez Kongres. W sprawozdaniu tym podnieśliśmy kwestie dotyczące nieprawidłowości, stronniczości, dyskryminacji i stosowania nadzoru handlowego, który z czasem staje się niewspółmiernie duży (ang. *commercial surveillance creep*) ([6]).

b. **Ochrona prawna zapewniana konsumentom unijnym przez Stany Zjednoczone**

DPF UE–USA działają w kontekście większego amerykańskiego systemu zapewniającego ochronę prywatności, który również chroni na wiele sposobów konsumentów UE. Zakaz ustanowiony w ustawie o FTC dotyczący nieuczciwych lub wprowadzających w błąd czynów lub praktyk nie ogranicza się do ochrony konsumentów amerykańskich przed amerykańskimi spółkami, ponieważ obejmuje te praktyki, które 1) powodują lub mogą spowodować możliwe do przewidzenia szkody w Stanach Zjednoczonych lub 2) obejmują prowadzenie istotnych operacji w Stanach Zjednoczonych. Ponadto FTC może korzystać ze wszystkich środków ochrony prawnej, które są dostępne w celu ochrony konsumentów krajowych podczas ochrony konsumentów zagranicznych ([7]).

FTC zapewnia również wykonanie innych przepisów szczególnych, których gwarancje rozciągają się na konsumentów niebędących obywatelami ani rezydentami USA – przykładem jest ustawa o ochronie prywatności dzieci w internecie. W ustawie o ochronie prywatności dzieci w internecie od operatorów stron i usług internetowych skierowanych do dzieci lub stron internetowych skierowanych do ogółu społeczeństwa, na których świadomie gromadzone są dane osobowe dzieci w wieku poniżej 13 lat, wymaga się między innymi, aby wprowadzili ostrzeżenie dla rodziców i uzyskali możliwą do zweryfikowania zgodę rodziców. Strony internetowe i usługi na serwerach amerykańskich, które podlegają przepisom ustawy

([2]) Tytuł 15 § 45 lit. a) U.S.C. FTC nie przysługują uprawnienia na gruncie prawa karnego lub w dziedzinie bezpieczeństwa narodowego. FTC nie może także realizować większości innych działań rządowych. Ponadto wprowadzono wyjątki dotyczące właściwości FTC w obszarze związanym z handlem m.in. w odniesieniu do banków, przewoźników lotniczych i zakładów ubezpieczeń oraz wspólnej działalności transportowej dostawców usług telekomunikacyjnych. FTC nie jest również właściwa do rozstrzygania spraw dotyczących większości organizacji non-profit, ale przysługuje jej właściwość w odniesieniu do fałszywych organizacji charytatywnych lub innych organizacji non-profit, które w istocie nastawione są na osiągnięcie zysku. FTC przysługuje również właściwość w odniesieniu do organizacji non-profit, które działają na rzecz swoich członków nastawionych na osiągnięcie zysku m.in. poprzez zapewnienie tym członkom znacznych korzyści gospodarczych. W niektórych przypadkach właściwość FTC jest zbieżna z właściwością innych agencji egzekwowania prawa. Wypracowaliśmy bliskie relacje z organami federalnymi i stanowymi oraz ściśle z nimi współpracujemy w celu koordynowania dochodzeń lub, w stosownych przypadkach, dokonania zgłoszeń.

([3]) *Zob*. FTC, prywatność i bezpieczeństwo, https://www.ftc.gov/business-guidance/privacy-security.

([4]) *Zob*. komunikat prasowy, FTC, FTC bada zasady służące ograniczeniu praktyk w zakresie nadzoru handlowego i zapewniania niewystarczającego bezpieczeństwa danych (11 sierpnia 2022 r.) dostępny pod adresem: https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices

([5]) *Zob*. Wspólne oświadczenie prasowe Didiera Reyndersa, komisarza ds. wymiaru sprawiedliwości Komisji Europejskiej, i Liny Khan, przewodniczącej Federalnej Komisji Handlu Stanów Zjednoczonych (30 marca 2022 r.), dostępne pod adresem: https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

([6]) *Zob*. komunikat prasowy FTC, FTC ostrzega przed wykorzystywaniem sztucznej inteligencji do zwalczania problemów internetowych (16 czerwca 2022 r.), dostępny pod adresem: https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) Tytuł 15 § 45 lit. a) ppkt 4 część B U.S.C. Ponadto „nieuczciwe lub wprowadzające w błąd czyny lub praktyki" obejmują takie czyny lub praktyki obejmujące handel zagraniczny, które (i) powodują lub mogą spowodować możliwe do przewidzenia szkody w Stanach Zjednoczonych lub (ii) obejmują prowadzenie istotnych operacji w Stanach Zjednoczonych. Tytuł 15 § 45 lit. a) ppkt 4 część A U.S.C.

o ochronie prywatności dzieci w internecie i na których gromadzone są dane osobowe małoletnich cudzoziemców, muszą spełniać wymogi ustawy o ochronie prywatności dzieci w internecie. Strony i usługi internetowe na serwerach zagranicznych muszą również spełniać wymogi ustawy o ochronie prywatności dzieci w internecie, jeżeli są skierowane do dzieci w Stanach Zjednoczonych lub jeżeli na stronach tych świadomie gromadzone są dane osobowe dzieci w Stanach Zjednoczonych. Ponadto poza przepisami amerykańskiego prawa federalnego, których wykonanie FTC egzekwuje, dodatkowe korzyści dla konsumentów z UE zapewniają inne federalne i stanowe przepisy dotyczące ochrony konsumentów, naruszeń ochrony danych i ochrony prywatności.

c. **Działania FTC w zakresie egzekwowania prawa**

FTC wniosła sprawy zarówno na podstawie ram programu „bezpieczna przystań" UE–USA, jak i ram Tarczy Prywatności UE–USA, i kontynuowała egzekwowanie Tarczy Prywatności UE–USA nawet po tym, jak TSUE unieważnił decyzję stwierdzającą odpowiedni stopień ochrony stanowiącej podstawę Tarczy Prywatności UE–USA ([8]). W kilku ostatnich skargach złożonych do FTC przedstawiono zarzuty dotyczące naruszenia Tarczy Prywatności UE–USA przez przedsiębiorstwa, w tym w postępowaniach przeciwko spółkom Twitter ([9]), CafePress ([10]) i Flo ([11]). W ramach czynności egzekucyjnej wobec spółki Twitter FTC zażądała od spółki Twitter 150 mln USD za naruszenie wcześniejszego nakazu FTC, które dotyczyło praktyk wywierających wpływ na ponad 140 mln klientów, w tym naruszenia zasady Tarczy Prywatności UE–USA numer 5 (Integralność danych i ograniczenie celu). Ponadto zgodnie z nakazem agencji spółka Twitter musi umożliwić użytkownikom stosowanie bezpiecznych metod uwierzytelniania wieloskładnikowego, które nie wymagają od użytkowników podania ich numerów telefonu.

W sprawie *CafePress* FTC twierdziła, że przedsiębiorstwo to nie zabezpieczyło informacji szczególnie chronionych należących do konsumentów, ukryło ważne naruszenie ochrony danych oraz naruszyło zasady Tarczy Prywatności UE–USA numer 2 (Wybór), numer 4 (Bezpieczeństwo) i numer 6 (Dostęp). Zgodnie z nakazem FTC przedsiębiorstwo to musi zastąpić nieodpowiednie środki uwierzytelniające uwierzytelnieniem wieloskładnikowym, istotnie ograniczyć ilość gromadzonych i przechowywanych danych, zaszyfrować numery ubezpieczenia społecznego, zlecić stronie trzeciej ocenę swoich programów zabezpieczenia informacji oraz przekazać FTC kopię, którą można upublicznić.

W sprawie *Flo* FTC twierdziła, że aplikacja służąca do śledzenia płodności ujawniała dane dotyczące zdrowia użytkowników dostawcom usług analizy danych będącym osobami trzecimi pomimo zobowiązań do zachowania prywatności takich danych. W skardze złożonej do FTC odnotowano w szczególności interakcje tego przedsiębiorstwa z konsumentami unijnymi oraz to, że spółka Flo naruszyła zasady Tarczy Prywatności UE–USA nr 1 (Zawiadomienie), 2 (Wybór), 3 (Odpowiedzialność za dalsze przekazywanie) i 5 (Integralność danych i ograniczenie celu). Zgodnie z nakazem FTC spółka Flo musi powiadomić użytkowników, których dane zostały ujawnione, o ujawnieniu ich danych osobowych, i nakazać wszystkich stronom trzecim, które otrzymały dane dotyczące zdrowia użytkowników, zniszczenie tych danych. Co istotne, decyzje FTC chronią wszystkich konsumentów, którzy mają do czynienia z amerykańskim przedsiębiorstwem, na całym świecie, a nie tylko tych konsumentów, którzy złożyli skargę.

Wiele byłych spraw związanych ze stosowaniem programu „bezpieczna przystań" UE–USA i Tarczy Prywatności UE–USA dotyczyło podmiotów, które dokonały wstępnej samocertyfikacji za pośrednictwem Departamentu Handlu, ale nie dokonały swojej corocznej certyfikacji, a nadal przedstawiały się jako aktywni uczestnicy. Inne sprawy dotyczyły fałszywych oświadczeń o uczestnictwie w programie ze strony podmiotów, które nigdy nie dokonały wstępnej samocertyfikacji za pośrednictwem Departamentu Handlu. W przyszłości zamierzamy koncentrować nasze działania w zakresie aktywnego egzekwowania prawa na rodzajach istotnych naruszeń zasad DPF UE–USA zarzucanych w sprawach wniesionych przeciwko takim spółkom, jak Twitter, CafePress i Flo. Jednocześnie Departament Handlu będzie zarządzał procesem samocertyfikacji i go nadzorował, jak również będzie prowadził oficjalny wykaz uczestników DPF UE–USA i zajmie się innymi kwestiami dotyczącymi oświadczeń w sprawie uczestnictwa w tym programie ([12]). Co istotne, podmioty, które oświadczają, że uczestniczą w DPF UE–USA, mogą podlegać stanowczemu egzekwowaniu zasad DPF UE–USA, nawet jeżeli nie dokonały ani nie odnawiają swojej samocertyfikacji za pośrednictwem Departamentu Handlu.

([8]) *Zob*. dodatek A w celu zapoznania się z wykazem kwestii podejmowanych przez FTC w związku z programem „bezpieczna przystań" i Tarczą Prywatności.

([9]) *Zob*. komunikat prasowy FTC, FTC nakłada na spółkę Twitter karę za oszukańcze wykorzystywanie danych zapewniających bezpieczeństwo kont do sprzedaży targetowanych reklam (25 maja 2022 r.), dostępny pod adresem: https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) *Zob*. komunikat prasowy FTC, FTC podejmuje działania przeciwko CafePress za ukrycie naruszenia ochrony danych (15 marca 2022 r.), dostępny pod adresem: https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) *Zob*. komunikat prasowy FTC, FTC finalizuje porozumienie z firmą Flo Health oferującą aplikację do śledzenia płodności, która udostępniała wrażliwe dane dotyczące zdrowia serwisom Facebook, Google i innym (22 czerwca 2021 r.), dostępny pod adresem: https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Pismo Marisy Lago, podsekretarz handlu międzynarodowego, do Pana Didiera Reyndersa, komisarza ds. wymiaru sprawiedliwości Komisji Europejskiej (12 grudnia 2022 r.).

II. **Określanie pierwszeństwa zgłoszeń i ich badanie**

Podobnie jak w przypadku ram programu „bezpieczna przystań" UE–USA oraz ram Tarczy Prywatności UE–USA, tak i w tym programie FTC zobowiązuje się do przyznania pierwszeństwa zgłoszeniom dotyczącym zasad DPF UE–USA z Departamentu Handlu i państw członkowskich UE. Pierwszeństwo damy również zgłoszeniom dotyczącym nieprzestrzegania zasad DPF UE–USA otrzymanych od organów samoregulacyjnych ds. prywatności i innych niezależnych organów ds. rozstrzygania sporów.

Aby ułatwić dokonywanie zgłoszeń z państw członkowskich UE zgodnie z DPF UE–USA, FTC opracowała ujednoliconą procedurę dokonywania zgłoszeń i przekazała wytyczne państwom członkowskim UE na temat rodzaju informacji, które najbardziej ułatwią FTC rozpatrywanie zgłoszeń. W ramach tych starań FTC wyznaczyła osobę odpowiedzialną za kontakty ze strony agencji w odniesieniu do zgłoszeń państw członkowskich UE. Największym ułatwieniem jest, gdy organ dokonujący zgłoszenia wstępnie bada domniemane naruszenie i gdy może podjąć współpracę z FTC w toku rozpoznawania sprawy.

Po przyjęciu takiego zgłoszenia od Departamentu Handlu, z państwa członkowskiego UE lub od organów samoregulacyjnych ds. prywatności lub innych niezależnych organów ds. rozstrzygania sporów FTC może podjąć szereg działań, aby zaradzić powstałym problemom. Przykładowo możemy dokonać przeglądu polityk ochrony prywatności podmiotu, uzyskać dalsze informacje bezpośrednio od podmiotu lub od stron trzecich, podjąć działania następcze wraz z jednostką dokonującą zgłoszenia, ocenić, czy naruszenia odbywają się według określonego schematu lub czy mają wpływ na znaczną liczbę konsumentów, określić, czy zgłoszenie obejmuje kwestie podlegające kompetencji Departamentu Handlu, ocenić, czy pomocne byłoby podjęcie dodatkowych starań w celu zawiadomienia uczestników rynku, i w stosownych przypadkach, wszcząć odpowiednie postępowanie.

Poza określaniem pierwszeństwa zgłoszeń dotyczących zasad DPF UE–USA od Departamentu Handlu, z państw członkowskich UE i od organów samoregulacyjnych ds. prywatności lub innych niezależnych organów ds. rozstrzygania sporów ([13]) FTC, w stosownych przypadkach, będzie kontynuować badanie z urzędu istotnych naruszeń zasad DPF UE–USA przy zastosowaniu właściwych narzędzi. W ramach realizowanego przez FTC programu dochodzenia problemów związanych z ochroną prywatności i bezpieczeństwem, który angażuje podmioty komercyjne, agencja rutynowa badała, czy dana jednostka podawała informacje na temat uczestnictwa w Tarczy Prywatności UE–USA. Jeżeli jednostka podawała takie informacje, a w postępowaniu wykryto oczywiste naruszenia zasad Tarczy Prywatności UE–USA, FTC uwzględniała zarzuty naruszenia tych zasad w swoich czynnościach egzekucyjnych. Będziemy nadal prezentować tę aktywną postawę w odniesieniu do zasad DPF UE–USA.

III. **Ubieganie się o wydanie decyzji i ich monitorowanie**

FTC potwierdza również swoje zobowiązanie do ubiegania się o wydanie decyzji służących wykonaniu przepisów na potrzeby zapewnienia zgodności z zasadami DPF UE–USA oraz do ich monitorowania. Wymóg przestrzegania zasad DPF UE–USA będziemy realizować za pomocą różnych odpowiednich nakazów w przyszłych decyzjach FTC dotyczących zasad DPF UE–USA. Naruszenia decyzji administracyjnych FTC mogą skutkować nałożeniem kar na gruncie prawa cywilnego w wysokości do 50 120 USD za każde naruszenie lub 50 120 USD za każdy dzień trwania naruszenia ([14]), w przypadku praktyk mających wpływ na wielu konsumentów kary mogą wynieść nawet miliony dolarów. Każda decyzja wydana w następstwie porozumienia zawiera również postanowienia dotyczące sprawozdawczości i przestrzegania zasad. Podmioty, do których skierowana jest decyzja, mają obowiązek przechowywać dokumenty, w których wykazuje się, że przestrzegają zasad przez określony okres. Decyzje należy również udostępnić pracownikom odpowiedzialnym za zapewnienie przestrzegania ich postanowień.

FTC systematycznie monitoruje również przestrzeganie decyzji dotyczących zasad Tarczy Prywatności UE–USA, co czyni w przypadku wszystkich wydawanych przez siebie decyzji, i podejmuje w stosownych przypadkach działania służące ich wykonaniu ([15]). Co istotne, decyzje FTC będą nadal chronić wszystkich konsumentów, którzy mają do czynienia z tym przedsiębiorstwem, na całym świecie, a nie tylko tych konsumentów, którzy złożyli skargę. Ponadto FTC będzie prowadzić internetowy wykaz przedsiębiorstw podlegających decyzjom dotyczącym stosowania zasad DPF UE–USA ([16]).

([13]) Chociaż FTC nie rozstrzyga indywidualnych skarg konsumenckich ani nie pośredniczy w ich rozstrzyganiu, FTC potwierdza, że będzie przyznawać pierwszeństwo zgłoszeniom dotyczącym zasad DPF UE–USA wniesionym przez unijne organy ochrony danych. Co więcej, FTC wykorzystuje skargi znajdujące się w bazie danych „straż konsumencka" (ang. Consumer Sentinel), do której dostęp ma wiele innych agencji egzekwowania prawa, aby określać tendencje, wskazywać priorytety egzekwowania prawa i identyfikować potencjalne cele dochodzenia. Osoby fizyczne z Unii Europejskiej mogą korzystać z tego samego systemu składania skarg, który jest dostępny dla amerykańskich konsumentów, aby złożyć skargę do FTC; jest on dostępny pod adresem: https://reportfraud.ftc.gov/. W przypadku indywidualnych skarg dotyczących zasad DPF UE–USA najbardziej użyteczną drogą dla osób fizycznych z Unii Europejskiej może być jednak wnoszenie skarg do organu ochrony danych lub niezależnego organu ds. rozstrzygania sporów w ich państwie członkowskim.

([14]) Tytuł 15 § 45 lit. m) U.S.C.; tytuł 16 § 1.98 kodeksu przepisów federalnych (ang. Code of Federal Regulations, „C.F.R."). Kwota ta jest okresowo korygowana o inflację.

([15]) W ubiegłym roku FTC głosowała za usprawnieniem procesu prowadzenia dochodzeń przeciwko wielokrotnym sprawcom. *Zob.* komunikat prasowy FTC, FTC zezwala na prowadzenie dochodzeń w sprawie kluczowych priorytetów w zakresie egzekwowania prawa (1 lipca 2021 r.), dostępny pod adresem: https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) *Por.* FTC, Tarcza Prywatności, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **Współpraca z unijnymi organami ochrony danych w zakresie egzekwowania prawa**

FTC uznaje ważną rolę, jaką odgrywają unijne organy ochrony danych w odniesieniu do zapewnienia przestrzegania zasad DPF UE–USA, i zachęca do pogłębionych konsultacji i zacieśniania współpracy w zakresie egzekwowania prawa. Skoordynowane podejście do wyzwań, jakie stwarza obecna sytuacja na rynku cyfrowym, oraz modele biznesowe, które przewidują przetwarzanie dużych ilości danych, faktycznie staje się coraz bardziej znaczące. FTC będzie udostępniać informacje na temat zgłoszeń organom egzekwowania prawa dokonującym zgłoszenia, w tym na temat statusu zgłoszenia, z zastrzeżeniem zachowania przepisów i ograniczeń dotyczących poufności. W największym stopniu, na jaki pozwala liczba i rodzaj otrzymanych zgłoszeń, przedstawione informacje będą zawierać ocenę zgłoszonych kwestii, w tym opis istotnych problemów, które w nich podniesiono, i wszelkich działań podjętych w celu zaradzenia naruszeniom prawa w ramach właściwości FTC. FTC przedstawi również organowi dokonującemu zgłoszenia informacje zwrotne dotyczące rodzajów otrzymanych zgłoszeń, aby podnieść efektywność starań, jakie podejmuje w celu przeciwdziałania niezgodnemu z prawem postępowaniu. Jeżeli organ egzekwowania prawa dokonujący zgłoszenia występuje o uzyskanie informacji na temat statusu konkretnego zgłoszenia do celów prowadzenia własnego postępowania służącego egzekwowaniu prawa, wówczas FTC udziela mu odpowiedzi, biorąc pod uwagę liczbę rozpatrywanych zgłoszeń i z zastrzeżeniem wymogów poufności i innych wymogów prawnych.

FTC podejmie również bliską współpracę z unijnymi organami ochrony danych, aby udzielić wsparcia na potrzeby egzekwowania prawa. W stosownych przypadkach może ona obejmować udostępnianie informacji i udzielanie wsparcia w badaniu spraw na podstawie amerykańskiej ustawy o bezpieczeństwie w sieci (ang. SAFE WEB Act), która zezwala na udzielanie wsparcia przez FTC zagranicznym organom egzekwowania prawa, jeżeli dany organ jest właściwy do stosowania przepisów zakazujących praktyk w znacznym stopniu podobnych do praktyk zakazanych przepisami, które egzekwuje FTC ([17]). W ramach tego wsparcia FTC może udostępniać informacje uzyskane w związku z prowadzonym przez siebie dochodzeniem, zarządzić obowiązkowe postępowanie w imieniu unijnego organu ochrony danych prowadzącego własne dochodzenie i pozyskiwać ustne zeznania świadków lub strony oskarżonej o naruszenie w związku z postępowaniem organu ochrony danych służącym egzekwowaniu prawa, z zastrzeżeniem wymogów amerykańskiej ustawy o bezpieczeństwie w sieci. FTC regularnie korzysta ze swoich uprawnień do wspierania innych organów na całym świecie w sprawach dotyczących ochrony prywatności i ochrony konsumentów.

Oprócz prowadzenia wszelkich konsultacji z unijnymi organami ochrony danych w sprawie kwestii dotyczących konkretnych przypadków FTC będzie brać udział w okresowych spotkaniach z wyznaczonymi przedstawicielami Europejskiej Rady Ochrony Danych („EROD") w celu omówienia zagadnień ogólnych związanych z ulepszaniem współpracy w zakresie egzekwowania prawa. Ponadto FTC będzie uczestniczyć, wraz z Departamentem Handlu, Komisją Europejską i przedstawicielami EROD, w okresowym przeglądzie DPF UE–USA w celu omówienia ich wdrożenia. FTC wspiera również opracowywanie narzędzi, które będą służyć pogłębianiu współpracy z unijnymi organami ochrony danych, a także z innymi organami egzekwowania prawa w zakresie ochrony prywatności na całym świecie. FTC z zadowoleniem potwierdza swoje zobowiązanie do egzekwowania aspektów DPF UE–USA związanych z sektorem handlowym. Uważamy, że nasze partnerstwo z kolegami i koleżankami z UE wnosi zasadniczy wkład w zapewnienie ochrony prywatności zarówno naszych obywateli, jak i Państwa obywateli.

Z poważaniem

Lina M. KHAN
Przewodnicząca Federalnej Komisji Handlu

([17]) Określając, czy powinna skorzystać ze swojego uprawnienia na podstawie amerykańskiej ustawy o bezpieczeństwie w sieci, FTC uwzględnia między innymi: „A) czy agencja, która wystąpiła o wsparcie, zgodziła się zapewnić lub zapewni wzajemne wsparcie Komisji; B) czy zrealizowanie wniosku odbyłoby się ze szkodą dla amerykańskiego interesu publicznego oraz C) czy dochodzenie lub postępowanie służące egzekwowaniu prawa prowadzone przez agencję, która wystąpiła o wsparcie, dotyczy działań lub praktyk, które powodują lub które mogą spowodować szkodę dla znacznej liczby osób". Tytuł 15 § 46 lit. j) ppkt 3 U.S.C. To uprawnienie nie ma zastosowania do egzekwowania przepisów prawa konkurencji.

Dodatek A

Tarcza Prywatności i wdrażanie programu „bezpieczna przystań”

	Docket/FTC File No.	Case	Link
1	Sygnatura akt FTC: 2023062 Sprawa nr 3:22-cv-03070 (N.D. Cal.)	Stany Zjednoczone/**Twitter, Inc.**	Twitter
2	Sygnatura akt FTC: 192 3209	Sprawa Residual Pumpkin Entity, LLC, spółki działającej wcześniej pod nazwą **CafePress**, i PlanetArt, LLC, spółki działającej wcześniej pod nazwą **CafePress**	CafePress
3	Sygnatura akt FTC: 192 3133 Nr rejestracyjny: C-4747	Sprawa **Flo Health, Inc.**	Flo Health
4	Sygnatura akt FTC: 192 3050 Nr rejestracyjny C-4723	Sprawa **Ortho-Clinical Diagnostics, Inc.**	Ortho-Clinical
5	Sygnatura akt FTC: 192 3092 Nr rejestracyjny C-4709	Sprawa **T&M Protection, LLC**	T&M Protection
6	Sygnatura akt FTC: 192 3084 Nr rejestracyjny C-4704	Sprawa **TDARX, Inc.**	TDARX
7	Sygnatura akt FTC: 192 3093 Nr rejestracyjny C-4706	Sprawa **Global Data Vault, LLC**	Global Data
8	Sygnatura akt FTC: 192 3078 Nr rejestracyjny C-4703	Sprawa **Incentive Services, Inc.**	Incentive Services
9	Sygnatura akt FTC: 192 3090 Nr rejestracyjny C-4705	Sprawa **Click Labs, Inc.**	Click Labs
10	Sygnatura akt FTC: 182 3192 Nr rejestracyjny C-4697	Sprawa **Medable, Inc.**	Medable
11	Sygnatura akt FTC: 182 3189 Nr rejestracyjny: 9386	Sprawa NTT Global Data Centers Americas, Inc., jako zainteresowanego następcy **RagingWire Data Centers, Inc.**	RagingWire
12	Sygnatura akt FTC: 182 3196 Nr rejestracyjny C-4702	Sprawa **Thru, Inc.**	Thru
13	Sygnatura akt FTC: 182 3188 Nr rejestracyjny C-4698	Sprawa **DCR Workforce, Inc.**	DCR Workforce
14	Sygnatura akt FTC: 182 3194 Nr rejestracyjny C-4700	Sprawa **LotaData, Inc.**	LotaData
15	Sygnatura akt FTC: 182 3195 Nr rejestracyjny C-4701	Sprawa **EmpiriStat, Inc.**	EmpiriStat

16	Sygnatura akt FTC: 182 3193 Nr rejestracyjny C-4699	Sprawa 214 Technologies, Inc., spółki działającej wcześniej pod nazwą **Trueface.ai**	Trueface.ai
17	Sygnatura akt FTC: 182 3107 Nr rejestracyjny: 9383	Sprawa **Cambridge Analytica, LLC**	Cambridge Analytica
18	Sygnatura akt FTC: 182 3152 Nr rejestracyjny C-4685	Sprawa **SecureTest, Inc.**	SecurTest
19	Sygnatura akt FTC: 182 3144 Nr rejestracyjny C-4664	Sprawa **VenPath, Inc.**	VenPath
20	Sygnatura akt FTC: 182 3154 Nr rejestracyjny C-4666	Sprawa **SmartStart Employment Screening, Inc.**	SmartStart
21	Sygnatura akt FTC: 182 3143 Nr rejestracyjny C-4663	Sprawa **mResourceLLC,** spółki działającej wcześniej pod nazwą Loop Works LLC	mResource
22	Sygnatura akt FTC: 182 3150 Nr rejestracyjny C-4665	Sprawa **Idmission LLC**	IDmission
23	Sygnatura akt FTC: 182 3100 Nr rejestracyjny C-4659	Sprawa **ReadyTech Corporation**	ReadyTech
24	Sygnatura akt FTC: 172 3173 Nr rejestracyjny C-4630	Sprawa **Decusoft, LLC**	Decusoft
25	Sygnatura akt FTC: 172 3171 Nr rejestracyjny C-4628	Sprawa **Tru Communication, Inc.**	Tru
26	Sygnatura akt FTC: 172 3172 Nr rejestracyjny C-4629	Sprawa **Md7, LLC**	Md7
30	Sygnatura akt FTC: 152 3198 Nr rejestracyjny C-4543	Spółki **Jhayrmaine Daniels (spółki działającej wcześniej pod nazwą California Skate-Line)**	Jhayrmaine Daniels
31	Sygnatura akt FTC: 152 3190 Nr rejestracyjny C-4545	Sprawa **Dale Jarrett Racing Adventure, Inc.**	Dale Jarrett
32	Sygnatura akt FTC: 152 3141 Nr rejestracyjny C-4540	Sprawa **Golf Connect, LLC**	Golf Connect
33	Sygnatura akt FTC: 152 3202 Nr rejestracyjny: C-4546	Sprawa **Inbox Group, LLC**	Inbox Group
34	Sygnatura akt: 152 3187 Nr rejestracyjny C-4542	Sprawa **IOActive, Inc.**	IOActive
35	Sygnatura akt FTC: 152 3140 Nr rejestracyjny C-4549	Sprawa **Jubilant Clinsys, Inc.**	Jubilant
36	Sygnatura akt FTC: 152 3199 Nr rejestracyjny C-4547	Sprawa **Just Bagels Manufacturing, Inc.**	Just Bagels

37	Sygnatura akt FTC: 152 3138 Nr rejestracyjny C-4548	Sprawa **NAICS Association, LLC**	NAICS
38	Sygnatura akt FTC: 152 3201 Nr rejestracyjny C-4544	Sprawa **One Industries Corp.**	One Industries
39	Sygnatura akt FTC: 152 3137 Nr rejestracyjny C-4550	Sprawa **Pinger, Inc.**	Pinger
40	Sygnatura akt FTC: 152 3193 Nr rejestracyjny C-4552	Sprawa **SteriMed Medical Waste Solutions**	SteriMed
41	Sygnatura akt FTC: 152 3184 Nr rejestracyjny C-4541	Sprawa **Contract Logix, LLC**	Contract Logix
42	Sygnatura akt FTC: 152 3185 Nr rejestracyjny C-4551	Sprawa **Forensics Consulting Solutions, LLC**	Forensics Consulting
43	Sygnatura akt FTC: 152 3051 Nr rejestracyjny C-4526	Sprawa **American Int'l Mailing, Inc.**	AIM
44	Sygnatura akt FTC: 152 3015 Nr rejestracyjny C-4525	Sprawa **TES Franchising, LLC**	TES
45	Sygnatura akt FTC: 142 3036 Nr rejestracyjny C-4459	Sprawa **American Apparel, Inc.**	American Apparel
46	Sygnatura akt FTC: 142 3026 Nr rejestracyjny C-4469	Sprawa **Fantage.com, Inc.**	Fantage
47	Sygnatura akt FTC: 142 3017 Nr rejestracyjny C-4461	Sprawa **Apperian, Inc.**	Apperian
48	Sygnatura akt FTC: 142 3018 Nr rejestracyjny C-4462	Sprawa **Atlanta Falcons Football Club, LLC**	Atlanta Falcons
49	Sygnatura akt FTC: 142 3019 Nr rejestracyjny C-4463	Sprawa **Baker Tilly Virchow Krause, LLP**	Baker Tilly
50	Sygnatura akt FTC: 142 3020 Nr rejestracyjny C-4464	Sprawa **BitTorrent, Inc.**	BitTorrent
51	Sygnatura akt FTC: 142 3022 Nr rejestracyjny C-4465	Sprawa **Charles River Laboratories, Int'l**	Charles River
52	Sygnatura akt FTC: 142 3023 Nr rejestracyjny C-4466	Sprawa **DataMotion, Inc.**	DataMotion
53	Sygnatura akt FTC: 142 3024 Nr rejestracyjny C-4467	Sprawa **DDC Laboratories, Inc.**, spółki działającej pod nazwą DNA Diagnostics Center	DDC
54	Sygnatura akt FTC: 142 3028 Nr rejestracyjny C-4470	Sprawa **Level 3 Communications, LLC**	Level 3

55	Sygnatura akt FTC: 142 3025 Nr rejestracyjny C-4468	Sprawa **PDB Sports, Ltd.**, spółki działającej pod nazwą Denver Broncos Football Club, LLP	Broncos
56	Sygnatura akt FTC: 142 3030 Nr rejestracyjny C-4471	Sprawa **Reynolds Consumer Products, Inc.**	Reynolds
57	Sygnatura akt FTC: 142 3031 Nr rejestracyjny C-4472	Sprawa **Receivable Management Services Corporation**	Receivable Mgmt
58	Sygnatura akt FTC: 142 3032 Nr rejestracyjny C-4473	Sprawa **Tennessee Football, Inc.**	Tennessee Football
59	Sygnatura akt FTC: 102 3058 Nr rejestracyjny C-4369	Sprawa **Myspace LLC**	Myspace
60	Sygnatura akt FTC: 092 3184 Nr rejestracyjny C-4365	Sprawa **Facebook, Inc.**	Facebook
61	Sygnatura akt FTC: 092 3081 Powództwo cywilne nr 09-CV-5276 (Dystrykt Centralny, Kalifornia)	FTC przeciwko Javian Karnani oraz **Balls of Kryptonite, LLC**, spółka działająca pod nazwą Bite Size Deals, LLC oraz Best Priced Brands, LLC	Balls of Kryptonite
62	Sygnatura akt FTC: 102 3136 Nr rejestracyjny C-4336	Sprawa **Google, Inc.**	Google
63	Sygnatura akt FTC: 092 3137 Nr rejestracyjny C-4282	Sprawa **World Innovators, Inc.**	World Innovators
64	Sygnatura akt FTC: 092 3141 Nr rejestracyjny C-4271	Sprawa **Progressive Gaitways LLC**	Progressive Gaitways
65	Sygnatura akt FTC: 092 3139 Nr rejestracyjny C-4270	Sprawa **Onyx Graphics, Inc.**	Onyx Graphics
66	Sygnatura akt FTC: 092 3138 Nr rejestracyjny C-4269	Sprawa **ExpatEdge Partners, LLC**	ExpatEdge
67	Sygnatura akt FTC: 092 3140 Nr rejestracyjny C-4281	Sprawa **Directors Desk LLC**	Directors Desk
68	Sygnatura akt FTC: 092 3142 Nr rejestracyjny C-4272	Sprawa **Collectify LLC**	Collectify

ZAŁĄCZNIK V

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

Dnia 6 lipca 2023 r.

Komisarz Didier Reynders
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Belgia

Szanowny Panie Komisarzu!

Departament Transportu Stanów Zjednoczonych („departament" lub „DoT") docenia możliwość przedstawienia swojej roli we wspieraniu zasad ram ochrony danych UE–USA („DPF UE–USA"). DPF UE–USA odegra kluczową rolę w ochronie danych osobowych przekazywanych podczas transakcji handlowych w świecie, który jest coraz bardziej pełny wzajemnych powiązań. Ramy te umożliwią przedsiębiorstwom dokonywanie ważnych operacji w gospodarce światowej, przy jednoczesnym zagwarantowaniu, że konsumenci unijni zachowają istotne gwarancje ochrony prywatności.

DoT po raz pierwszy publicznie wyraził swoje zobowiązanie do egzekwowania zasad programu „bezpieczna przystań" UE–USA w piśmie wysłanym do Komisji Europejskiej ponad 22 lata temu, a zobowiązania te zostały powtórzone i rozszerzone w piśmie z 2016 r. dotyczącym ram Tarczy Prywatności UE–USA. W pismach tych DoT zobowiązał się do zdecydowanego egzekwowania zasad dotyczących prywatności określonych w programie „bezpieczna przystań" UE–USA, a następnie zasad Tarczy Prywatności UE–USA. DoT rozszerza to zobowiązanie na zasady DPF UE–USA, a niniejsze pismo potwierdza to zobowiązanie.

W szczególności DoT potwierdza swoje zobowiązanie w następujących obszarach kluczowych. Są to: 1) przyznawanie pierwszeństwa dochodzeniu domniemanych naruszeń zasad DPF UE–USA; 2) podejmowanie odpowiednich czynności egzekucyjnych wobec jednostek, które składają fałszywe lub wprowadzające w błąd oświadczenia dotyczące udziału w programie DPF UE–USA; oraz 3) monitorowanie i publikowanie decyzji służących egzekwowaniu przepisów w sprawach naruszeń zasad DPF UE–USA. Przekazujemy informacje na temat przestrzegania każdego z tych zobowiązań i w razie konieczności informacje związane z rolą DoT w obszarze ochrony prywatności konsumentów i stosowania zasad DPF UE–USA.

1. **Przebieg procedury**

A. Uprawnienia DoT w zakresie ochrony prywatności

Departament jest bardzo zaangażowany w zapewnianie ochrony informacji dostarczonych przez

konsumentów przewoźnikom lotniczym i pośrednikom sprzedaży biletów. Uprawnienie DoT do podjęcia działania w tym obszarze uregulowano w tytule 49 U.S.C. § 41712, w którym zakazuje się przewoźnikowi lub pośrednikowi sprzedaży biletów stosowania „nieuczciwych lub wprowadzających w błąd praktyk" w usługach transportu lotniczego lub w sprzedaży usług transportu lotniczego. Sekcję 41712

wzorowano na sekcji 5 ustawy o Federalnej Komisji Handlu (FTC) (tytuł 15 § 45 U.S.C.). Niedawno DoT wydał regulacje określające nieuczciwe i wprowadzające w błąd praktyki, zgodne z precedensem dotyczącym zarówno DoT, jak i FTC (tytuł 14 § 399.79). W szczególności dana praktyka jest nieuczciwa, jeżeli powoduje lub może spowodować znaczną szkodę, której w sposób rozsądny nie da się uniknąć, a której jednocześnie nie równoważą korzyści osiągane przez konsumentów lub konkurencję.

Praktyka ma charakter „wprowadzający w błąd" wobec konsumentów, jeżeli – w odniesieniu do istotnej kwestii – wprowadza w błąd konsumenta działającego rozsądnie w danych okolicznościach. Kwestia jest istotna, jeśli może mieć wpływ na postępowanie lub decyzję konsumenta w odniesieniu do produktu lub usługi. Poza tymi ogólnymi zasadami zgodnie ze stosowaną przez DoT wykładnią § 41712 przewoźnicy i pośrednicy sprzedaży biletów nie mogą: 1) naruszać polityki prywatności DoT; 2) naruszać żadnych przepisów wydanych przez departament, w których konkretne praktyki ochrony prywatności uznano za nieuczciwe lub wprowadzające w błąd; 3) naruszać przepisów ustawy o ochronie prywatności dzieci w internecie ani przepisów wykonawczych do tej ustawy wydanych przez FTC; ani 4) jako uczestnik DPF UE–USA unikać przestrzegania zasad DPF UE–USA ([1]).

Jak zauważono powyżej, na mocy prawa federalnego DoT dysponuje wyłącznym uprawnieniem do regulowania praktyk ochrony prywatności przewoźników lotniczych i uprawnieniem dzielonym z FTC w odniesieniu do praktyk ochrony prywatności stosowanych przez pośredników sprzedaży biletów w sprzedaży usług transportu lotniczego.

W związku z tym, jeżeli przewoźnik lub pośrednik sprzedaży usług transportu lotniczego publicznie zobowiąże się do przestrzegania zasad DPF UE–USA, departament może skorzystać ze swoich uprawnień ustawowych na podstawie § 41712, aby zapewnić przestrzeganie tych zasad. Jeżeli zatem pasażer przekazuje dane przewoźnikowi lub pośrednikowi sprzedaży biletów, który zobowiązał się do przestrzegania zasad DPF UE–USA, jakiekolwiek nieprzestrzeganie tych zasad przez przewoźnika lub pośrednika sprzedaży biletów stanowi naruszenie § 41712.

B. Praktyki w zakresie egzekwowania prawa

Urząd ds. Ochrony Konsumentów w Lotnictwie („OACP") ([2]) departamentu prowadzi dochodzenia i rozstrzyga sprawy na podstawie tytułu 49 § 41712 U.S.C. Egzekwuje zakaz ustawowy w § 41712 dotyczący nieuczciwych i wprowadzających w błąd praktyk przede wszystkim w drodze negocjacji, sporządzając orzeczenia zawierające nakaz zaprzestania stosowania kwestionowanych praktyk i orzeczenia, którymi nakłada kary na gruncie prawa cywilnego. Urząd dowiaduje się o potencjalnych naruszeniach głównie ze skarg, jakie otrzymuje od osób fizycznych, biur podróży, przewoźników lotniczych oraz agencji rządowych Stanów Zjednoczonych i zagranicznych instytucji rządowych. Konsumenci mogą wnosić skargi dotyczące ochrony prywatności na przewoźników lotniczych i pośredników sprzedaży biletów za pośrednictwem strony internetowej DoT ([3]).

Jeżeli nie osiągnięto zasadnego i odpowiedniego porozumienia w sprawie, OACP ma prawo wszcząć odpowiednie postępowanie, które obejmuje postępowanie dowodowe przed sędzią administracyjnym w DoT. Sędzia ten ma prawo wydać orzeczenie zawierające nakaz zaprzestania stosowania zaskarżonych praktyk i nałożyć kary cywilne. Naruszenia § 41712 mogą skutkować wydaniem orzeczenia zawierającego nakaz zaprzestania stosowania kwestionowanych praktyk i nałożeniem kar na gruncie prawa cywilnego w wysokości do 37 377 USD za każde naruszenie § 41712.

Departament nie jest uprawniony do zasądzania odszkodowania ani zadośćuczynienia pieniężnego w przypadku skarg wnoszonych przez osoby fizyczne. Departament dysponuje jednak uprawnieniem do zatwierdzania ustaleń będących wynikiem dochodzenia przeprowadzonego przez OACP, które dają bezpośrednie korzyści konsumentom (np. w postaci środków pieniężnych, bonów) w celu zrównoważenia kar pieniężnych należnych w innym razie rządowi Stanów Zjednoczonych. Z tego rozwiązania korzystano w przeszłości i można z niego skorzystać również w kontekście zasad DPF UE–USA, jeżeli zajdą określone okoliczności. Powtarzające się przypadki naruszania § 41712 przez przewoźnika lotniczego postawiłyby również pod znakiem zapytania zdolność przewoźnika lotniczego do przestrzegania przepisów, co w drastycznych przypadkach mogłoby doprowadzić do uznania, że utracił on zdolność do prowadzenia działalności, i w związku z tym do utraty licencji na prowadzenie działalności.

Do dziś DoT otrzymał stosunkowo niewielką liczbę skarg dotyczących domniemanych naruszeń zasad ochrony prywatności przez pośredników sprzedaży biletów lub przewoźników lotniczych. Otrzymane skargi są badane zgodnie z zasadami przedstawionymi powyżej.

C. Ochrona prawna zapewniana konsumentom unijnym przez DoT

Zgodnie z § 41712 zakaz nieuczciwych lub wprowadzających w błąd praktyk w transporcie lotniczym lub sprzedaży usług transportu lotniczego ma zastosowanie do amerykańskich i zagranicznych przewoźników lotniczych i pośredników sprzedaży biletów. DoT często podejmuje działania wobec amerykańskich i zagranicznych przewoźników lotniczych w związku z praktykami, które mają wpływ zarówno na zagranicznych, jak i amerykańskich konsumentów; podstawą tych działań jest fakt, że praktyki przewoźnika lotniczego miały miejsce w toku świadczenia usług transportu lotniczego do lub z Stanów Zjednoczonych. DoT wykorzystuje i nadal będzie wykorzystywał wszystkie środki ochrony prawnej, które służą ochronie zarówno konsumentów zagranicznych, jak i będących obywatelami lub rezydentami USA przed nieuczciwymi lub wprowadzającymi w błąd praktykami stosowanymi w transporcie lotniczym przez jednostki regulowane.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.
([2]) Dawniej znany pod nazwą Urzędu ds. Egzekwowania Prawa i Prowadzenia Postępowań w Lotnictwie.
([3]) http://www.transportation.gov/airconsumer/privacy-complaints.

DoT zapewnia również, w odniesieniu do przewoźników lotniczych, egzekwowanie innych przepisów szczególnych, które rozszerzając zakres ochrony na konsumentów niebędących obywatelami ani rezydentami USA – przykładem jest ustawa o ochronie prywatności dzieci w internecie. W ustawie o ochronie prywatności dzieci w internecie przed operatorami stron i usług internetowych skierowanych do dzieci lub stron internetowych skierowanych do ogółu społeczeństwa, na których świadomie gromadzone są dane osobowe dzieci w wieku poniżej 13 lat, wymaga się między innymi, aby wprowadzili ostrzeżenie dla rodziców i uzyskali możliwą do zweryfikowania zgodę rodziców. Strony internetowe i usługi na serwerach amerykańskich, które podlegają przepisom ustawy o ochronie prywatności dzieci w internecie i na których gromadzone są dane osobowe małoletnich cudzoziemców, muszą spełniać wymogi ustawy o ochronie prywatności dzieci w internecie. Strony i usługi internetowe na serwerach zagranicznych muszą również spełniać wymogi ustawy o ochronie prywatności dzieci w internecie, jeżeli są skierowane do dzieci w Stanach Zjednoczonych lub jeżeli na stronach tych świadomie gromadzone są dane osobowe dzieci w Stanach Zjednoczonych. DoT jest uprawniony do podjęcia czynności egzekucyjnych w stopniu, w jakim amerykańscy lub zagraniczni przewoźnicy lotniczy prowadzący działalność w Stanach Zjednoczonych naruszają ustawę o ochronie prywatności dzieci w internecie.

II. **Egzekwowanie zasad DPF UE–USA**

Jeżeli przewoźnik lotniczy lub pośrednik sprzedaży biletów postanawia zostać uczestnikiem programu DPF UE–USA, a departament otrzymuje skargę, że taki przewoźnik lotniczy lub pośrednik sprzedaży biletów dokonał domniemanego naruszenia zasad tego programu, departament podejmie następujące kroki w celu zdecydowanego egzekwowania zasad DPF UE–USA.

A. Przyznawanie pierwszeństwa dochodzeniu domniemanych naruszeń

OACP wchodzący w skład departamentu zbada każdą skargę, w której zarzuca się domniemane naruszenie zasad DPF UE–USA, w tym skargi otrzymane od unijnych organów ochrony danych, i podejmie czynności egzekucyjne, jeżeli pojawią się dowody wskazujące na naruszenie.

Ponadto OACP będzie współpracował z FTC i Departamentem Handlu oraz przyzna pierwszeństwo sprawom dotyczącym zarzutów nieprzestrzegania zobowiązań z zakresu ochrony prywatności zgodnie z DPF UE–USA.

Po otrzymaniu skargi na domniemane naruszenie zasad DPF UE–USA OACP może podjąć w toku swojego dochodzenia szereg czynności. Przykładowo departament może dokonać przeglądu polityk ochrony prywatności pośrednika sprzedaży biletów lub przewoźnika lotniczego, uzyskać dalsze informacje od pośrednika sprzedaży biletów lub przewoźnika lotniczego bądź od stron trzecich, podjąć działania następcze wraz z jednostką dokonującą zgłoszenia oraz ocenić, czy naruszenia odbywają się według określonego schematu lub czy mają wpływ na znaczną liczbę konsumentów. Ponadto określi, czy zgłoszenie obejmuje kwestie podlegające kompetencji Departamentu Handlu lub FTC, oceni, czy pomocne byłoby zwiększenie wiedzy konsumentów lub przedsiębiorstw, i, w stosownych przypadkach, rozpocznie postępowanie służące egzekwowaniu prawa.

Jeżeli departament dowie się o potencjalnych naruszeniach zasad DPF UE–USA przez pośredników sprzedaży biletów, podejmie w tej sprawie współpracę z FTC. Będziemy również informować FTC i Departament Handlu na temat wyników wszelkich działań służących egzekwowaniu tych zasad.

B. Przeciwdziałanie fałszywym lub wprowadzającym w błąd oświadczeniom dotyczącym uczestnictwa

Departament podtrzymuje zobowiązanie do badania naruszeń zasad DPF UE–USA, w tym fałszywych lub wprowadzających w błąd oświadczeń dotyczących uczestnictwa w programie DPF UE–USA. Rozpatrując wnioski, przyznamy pierwszeństwo zgłoszeniom z Departamentu Handlu dotyczącym podmiotów, w przypadku których stwierdzimy, że niezasadnie podają się za członków programu DPF UE–USA lub korzystają z jakiegokolwiek znaku certyfikacyjnego DPF UE–USA bez pozwolenia.

Ponadto chcielibyśmy zauważyć, że jeżeli w polityce ochrony prywatności podmiotu zobowiązano się do przestrzegania zasad DPF UE–USA, sam fakt, iż podmiot nie dokona lub nie odnowi samocertyfikacji w Departamencie Handlu, może skutkować podjęciem przez DoT działań w celu wyegzekwowania tych zobowiązań.

C. Monitorowanie i publikowanie decyzji służących egzekwowaniu przepisów w sprawach naruszeń DPF UE–USA

OACP wchodzący w skład departamentu podtrzymuje również swoje zobowiązanie do monitorowania decyzji służących egzekwowaniu przepisów w sprawach naruszeń zasad DPF UE–USA. W szczególności, jeżeli urząd wyda decyzję, w której nakaże przewoźnikowi lotniczemu lub pośrednikowi sprzedaży biletów powstrzymanie się od przyszłych naruszeń zasad DPF UE–USA i przepisów § 41712, będzie następnie monitorował, czy jednostka przestrzega postanowienia o powstrzymaniu się od tych określonych naruszeń. Ponadto urząd zapewni, aby decyzje wydane w sprawach dotyczących zasad DPF UE–USA były dostępne na jego stronie internetowej.

Liczymy na dalszą współpracę w sprawach związanych z DPF UE–USA z naszymi partnerami na poziomie federalnym i zainteresowanymi stronami z Unii Europejskiej.

Mam nadzieję, że te informacje będą dla Państwa pomocne. W razie jakichkolwiek pytań lub potrzeby dalszych informacji jestem do Państwa dyspozycji.

Z poważaniem

Pete BUTTIGIEG

ZAŁĄCZNIK VI

Departament Sprawiedliwości USA

Wydział Karny

Biuro Asystenta Prokuratora Generalnego Waszyngton 20530

Dnia 23 czerwca 2023 r.

Ana Gallego Torres
Dyrektor Generalna ds. Sprawiedliwości i Konsumentów
European Commission
Rue Montoyer/Montoyerstraat 59
1049 Brussels
Belgia

Szanowna Pani!

W niniejszym piśmie przedstawiono krótki opis głównych narzędzi dochodzeniowych wykorzystywanych w celu pozyskania danych handlowych i innych informacji przechowywanych w rejestrach prowadzonych przez korporacje w Stanach Zjednoczonych w celach związanych z egzekwowaniem prawa w sprawach karnych lub w celach leżących w interesie publicznym (na potrzeby organów administracji cywilnej lub regulacyjnych), uwzględniając ograniczenia dostępu przyjęte w aktach stanowiących podstawę prawną ([1]). Wszystkie pisma sądowe omawiane w niniejszym piśmie nie mają dyskryminacyjnego charakteru, ponieważ służą do pozyskiwania informacji od korporacji w Stanach Zjednoczonych, w tym od spółek, które dokonały samocertyfikacji w ramach ochrony danych UE–USA, niezależnie od narodowości lub miejsca zamieszkania osoby, której dane dotyczą. Ponadto korporacje, które otrzymują pismo sądowe w Stanach Zjednoczonych, mogą je zaskarżyć w sądzie w opisany poniżej sposób ([2]).

Szczególne znaczenie w kontekście zatrzymywania danych przez organy publiczne ma czwarta poprawka do konstytucji Stanów Zjednoczonych, która stanowi, że „[p]rawa ludu do nietykalności osobistej, mieszkania, dokumentów i mienia nie wolno naruszać przez bezzasadne przeszukania i zatrzymanie; nakaz w tym przedmiocie można wystawić tylko wówczas, gdy zachodzi wiarygodna przyczyna potwierdzona przysięgą lub zastępującym ją oświadczeniem. Miejsce podlegające przeszukaniu oraz osoby i rzeczy podlegające zatrzymaniu powinny być w nakazie szczegółowo określone". Czwarta poprawka do konstytucji Stanów Zjednoczonych. Zgodnie z treścią wyroku wydanego przez Sąd Najwyższy Stanów Zjednoczonych w sprawie Berger przeciwko Stanowi Nowy Jork „[p]odstawowym celem przedmiotowej poprawki, który został potwierdzony w niezliczonych orzeczeniach tego Sądu, jest zapewnienie osobom fizycznym prywatności oraz ochrony przed bezpodstawnymi próbami jej naruszenia przez urzędników państwowych". 388 U.S. 41, 53 (1967) (przytoczono treść wyroku w sprawie Camara przeciwko sądowi miejskiemu w San Francisco, 387 U.S. 523, 528 (1967)). Zgodnie z treścią czwartej poprawki funkcjonariusze w dochodzeniach krajowych są zasadniczo zobowiązani do uzyskania nakazu wydanego przez sąd przed przeprowadzeniem przeszukania. Zob. wyrok w sprawie Katz przeciwko Stanom Zjednoczo-

([1]) W niniejszym przeglądzie nie opisano narzędzi dochodzeniowych w obszarze bezpieczeństwa narodowego wykorzystywanych przez organy egzekwowania prawa w dochodzeniach dotyczących terroryzmu i dochodzeniach dotyczących innych kwestii związanych z bezpieczeństwem narodowym, w tym wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego dotyczącego określonych informacji pochodzących ze sprawozdań kredytowych, dokumentacji finansowej, dokumentacji abonenta elektronicznego i dokumentacji dotyczącej transakcji (tytuł 12 § 3414 U.S.C.; tytuł 15 § 1681u U.S.C., tytuł 15 § 1681v U.S.C.; tytuł 18 § 2709 U.S.C.;, tytuł 50 § 3162 U.S.C.), a także informacji zgromadzonych w ramach obserwacji elektronicznej, nakazów przeszukania, dokumentacji dotyczącej prowadzonej działalności oraz innego rodzaju informacji zgromadzonych zgodnie z przepisami ustawy o kontroli wywiadu (tytuł 50 § 1801 i nast.).

([2]) W niniejszym piśmie omówiono federalne organy egzekwowania prawa i organy regulacyjne; w przypadkach naruszenia prawa stanowego dochodzenie prowadzą organy egzekwowania prawa na szczeblu stanowym, a postępowanie sądowe toczy się w sądach stanowych. Organy egzekwowania prawa na szczeblu stanowym korzystają z nakazów i wezwań wystawianych zgodnie z prawem stanowym, stosując zasadniczo takie same procedury jak te opisane w niniejszym piśmie, przy czym stanowe pisma sądowe mogą być objęte gwarancjami przewidzianymi w konstytucjach stanowych, których zakres wykracza poza zakres gwarancji przewidzianych w konstytucji Stanów Zjednoczonych. Gwarancje przewidziane w prawie stanowym muszą być co najmniej równoważne środkom przewidzianym w konstytucji Stanów Zjednoczonych, poprzez uwzględnienie co najmniej postanowień czwartej poprawki.

nym, 389 U.S. 347, 357 (1967). Normy dotyczące wydawania nakazu, takie jak wymogi dotyczące zachodzenia prawdopodobnej przyczyny i szczegółowości, mają zastosowanie do nakazów przeszukania i zatrzymania, a także do nakazów dotyczących treści komunikatów przekazywanych za pomocą łączności elektronicznej wydanych na podstawie ustawy o przechowywanych danych przekazywanych za pomocą łączności elektronicznej, jak omówiono poniżej. Jeżeli obowiązek uzyskania nakazu nie ma zastosowania w danym przypadku, niezależnie od tego działanie organów rządowych poddaje się testowi „zasadności" na podstawie czwartej poprawki. W związku z tym gwarancja, że rząd Stanów Zjednoczonych nie będzie posiadał nieograniczonych lub arbitralnych uprawnień w zakresie zatrzymywania prywatnych informacji, została ustanowiona w samej konstytucji ([3]).

Uprawnienia organów egzekwowania prawa w sprawach karnych:

Prokuratorzy federalni, którzy są urzędnikami Departamentu Sprawiedliwości (DoJ), oraz federalni agenci śledczy, w tym przedstawiciele Federalnego Biura Śledczego (FBI), agencji egzekwowania prawa w ramach Departamentu Sprawiedliwości, mają prawo nakazać osobom prawnym w Stanach Zjednoczonych przedstawienie dokumentów i innych informacji przechowywanych w rejestrach do celów dochodzeniowych w postępowaniu karnym za pośrednictwem różnego rodzaju obowiązkowych pism sądowych, takich jak wezwania do stawienia się przed wielką ławą przysięgłych, wezwania administracyjne oraz nakazy przeszukania, i mogą pozyskiwać innego rodzaju informacje na podstawie aktów stanowiących podstawę prawną na szczeblu federalnym do kontroli rozmów telefonicznych oraz instalowania urządzeń rejestrujących wybierane numery na gruncie prawa karnego.

Wezwania do stawienia się przed wielką ławą przysięgłych lub na rozprawie: wezwania do stawienia się przed ławą przysięgłych w sprawie karnej są wykorzystywane do wspierania ukierunkowanych dochodzeń prowadzonych przez organy egzekwowania prawa. Wezwanie do stawienia się przed wielką ławą przysięgłych to pismo urzędowe wydawane przez wielką ławę przysięgłych (zazwyczaj na wniosek prokuratora federalnego), którego celem jest zapewnienie wsparcia w ramach prowadzonego przez wielką ławę przysięgłych dochodzenia w sprawie określonego przypadku domniemanego naruszenia przepisów prawa karnego. Wielkie ławy przysięgłych to organ dochodzeniowy sądu, którego skład określa sędzia lub sędzia pokoju. W wezwaniu można zwrócić się do danej osoby o złożenie zeznań w postępowaniu, przedstawienie lub udostępnienie rejestrów związanych z prowadzoną działalnością, przekazanie informacji przechowywanych w formie elektronicznej lub dostarczenie innych przedmiotów materialnych. Informacje muszą mieć istotne znaczenie dla prowadzonego dochodzenia, a wezwanie nie może być nieuzasadnione z uwagi na jego zbyt szeroki zakres lub z uwagi na jego uciążliwy lub obciążający charakter. Odbiorca może sprzeciwić się wezwaniu, powołując się na przywołane powyżej przesłanki. Zob. zasada 17 federalnego kodeksu postępowania karnego. W ściśle określonych okolicznościach wezwania dotyczące przedstawienia dokumentów mogą zostać wystosowane po rozpoznaniu danej sprawy przez wielką ławę przysięgłych.

Akty stanowiące podstawę prawną wezwań administracyjnych: przepisy aktów stanowiących podstawę prawną wezwań administracyjnych mogą być stosowane w postępowaniach karnych lub cywilnych. Jeżeli chodzi o sprawy karne, w szeregu ustaw federalnych dopuszcza się możliwość stosowania wezwań administracyjnych w celu pozyskania rejestrów dotyczących prowadzonej działalności, informacji przechowywanych w formie elektronicznej lub innych przedmiotów materialnych lub uzyskania dostępu do takich rejestrów, informacji lub przedmiotów w ramach postępowań w przedmiocie nadużyć w obszarze opieki zdrowotnej, znęcania się nad dziećmi, ochrony tajnych służb, spraw dotyczących substancji kontrolowanych i prowadzonych przez Inspektora Generalnego dochodzeń przeciwko agencjom rządowym. Jeżeli rząd postanowi wystąpić do sądu o zobowiązanie danego podmiotu do zastosowania się do treści wezwania administracyjnego, odbiorca wezwania – podobnie jak odbiorca wezwania do stawienia się przed wielką ławą przysięgłych – może stwierdzić, że wezwanie jest nieuzasadnione, ponieważ jego zakres jest zbyt szeroki lub ponieważ ma ono uciążliwy lub obciążający charakter.

Nakazy sądowe upoważniające do instalowania urządzeń rejestrujących wybierane numery oraz urządzeń śledzących: zgodnie z przepisami dotyczącymi instalowania urządzeń rejestrujących wybierane numery oraz urządzeń śledzących w sprawach karnych organy egzekwowania prawa mogą uzyskać nakaz sądowy przyznający im uprawnienia do rejestrowania w czasie rzeczywistym informacji billingowych, informacji o trasowaniu, informacji adresowych i informacji przekazywanych w ramach sygnalizacji telekomunikacyjnej dotyczących danego numeru telefonu lub adresu e-mail po upewnieniu się, że przekazywane informacje mają istotne znaczenie dla toczącego się dochodzenia. Zob. tytuł 18 § 3121–3127 U.S.C. Korzystanie z takich urządzeń lub ich instalowanie w sytuacji, w której nie jest to dopuszczalne zgodnie z obowiązującymi przepisami, stanowi przestępstwo federalne.

Ustawa o ochronie danych w łączności elektronicznej: w tytule II ustawy o ochronie danych w łączności elektronicznej przewidziano dodatkowe przepisy regulujące kwestie związane z dostępem rządu do informacji na temat abonentów, danych o ruchu oraz treści komunikatów przechowywanych przez dostawców usług internetowych, przedsiębiorstwa telekomunikacyjne oraz innych dostawców usług internetowych będących osobami trzecimi, które określa się również mianem ustawy o przechowywanych danych przekazywanych za pomocą łączności elektronicznej (tytuł 18 § 2701–2712 U.S.C.). W ustawie o przechowywanych danych przekazywanych za pomocą łączności elektronicznej ustanowiono system ustawowych praw do prywatności, który ogranicza dostęp organów egzekwowania prawa do danych dotyczących klientów i abonentów dostawców usług interne-

([3]) Omówione powyżej zasady wynikające z czwartej poprawki, dotyczące ochrony prywatności i interesów bezpieczeństwa, są regularnie stosowane przez sądy amerykańskie w odniesieniu do nowych rodzajów narzędzi egzekwowania prawa, których zastosowanie jest możliwe dzięki rozwojowi technologii. Na przykład w 2018 r. Sąd Najwyższy orzekł, że pozyskiwanie przez rząd w ramach egzekwowania prawa historycznych informacji o lokalizacji telefonu komórkowego od operatora telefonii komórkowej przez dłuższy wyczerpuje definicję „przeszukania" podlegającego wymogowi posiadania nakazu takiego przeszukania wynikającemu z czwartej poprawki. Sprawa Carpenter przeciwko Stanom Zjednoczonym, zbiór orzeczeń Sądu Najwyższego (S. Ct.) t. 138 s. 2206, 2018.

towych innych niż dane określone w prawie konstytucyjnym. W ustawie tej przewidziano możliwość zwiększenia poziomu ochrony prywatności w zależności od inwazyjności metody gromadzenia danych. Aby uzyskać dostęp do danych zgromadzonych przy rejestracji abonentów, ich adresów IP, powiązanych z tymi adresami znaczników czasu oraz informacji billingowych, organy egzekwowania prawa w sprawach karnych muszą uzyskać stosowny nakaz. Aby uzyskać dostęp do większości innych przechowywanych informacji niedotyczących treści, takich jak nagłówki wiadomości e-mail bez tematu, organ egzekwowania prawa musi przedstawić sędziemu konkretne przesłanki faktyczne świadczące o tym, że żądane informacje mają istotne i zasadnicze znaczenie dla toczącego się dochodzenia. Aby uzyskać dostęp do treści komunikatów przekazywanych za pomocą łączności elektronicznej, organy egzekwowania prawa w sprawach karnych muszą zasadniczo uzyskać nakaz wydany przez sędziego na podstawie uzasadnionego podejrzenia, że dane konto użytkownika zawiera dowody popełnienia przestępstwa. W ustawie o przechowywanych danych przekazywanych za pomocą łączności elektronicznej przewidziano również możliwość pociągnięcia odpowiednich osób do odpowiedzialności cywilnej i karnej ([4]).

Sądowe nakazy objęcia danej osoby obserwacją wydawane zgodnie z przepisami federalnej ustawy o podsłuchach: ponadto organy egzekwowania prawa mogą przechwytywać w czasie rzeczywistym komunikaty przekazywane za pomocą łączności kablowej, ustnie lub za pomocą łączności elektronicznej do celów związanych z prowadzeniem dochodzeń w sprawach karnych zgodnie z przepisami federalnej ustawy o podsłuchach. Zob. tytuł 18 § 2510–2523 U.S.C. Z takiego aktu stanowiącego podstawę prawną można skorzystać wyłącznie po uzyskaniu nakazu sądowego, w którym sędzia stwierdzi m.in., że istnieje uzasadnione podejrzenie, iż informacje uzyskane dzięki zainstalowaniu podsłuchu lub zastosowaniu środków przechwytywania komunikatów przekazywanych drogą elektroniczną pozwoli uzyskać dowody popełnienia przestępstwa federalnego lub ustalić miejsce pobytu osoby ukrywającej się przed wymiarem sprawiedliwości. W ustawie przewidziano możliwość pociągnięcia odpowiednich osób do odpowiedzialności cywilnej i karnej z tytułu naruszenia przepisów dotyczących podsłuchów.

Nakaz przeszukania – zasada 41 federalnego kodeksu postępowania karnego: organy egzekwowania prawa mogą przeprowadzić fizyczne przeszukanie pomieszczeń na terytorium Stanów Zjednoczonych, jeżeli zostaną do tego upoważnione przez sędziego. Organy egzekwowania prawa muszą wykazać sędziemu, że istnieje uzasadnione podejrzenie, iż doszło do popełnienia przestępstwa lub że ma dojść do popełnienia przestępstwa, oraz że przedmioty związane z przestępstwem prawdopodobnie znajdują się w miejscu wskazanym w nakazie. Tego rodzaju akt stanowiący podstawę przeszukania często wykorzystuje się w przypadku, gdy fizyczne przeszukanie pomieszczeń przez policję jest konieczne z uwagi na ryzyko zniszczenia dowodów, jeżeli osobie prawnej zostanie dostarczone wezwanie do stawienia się lub inny nakaz przedstawienia danych. Osoba, u której dokonano przeszukania lub której nieruchomość została przeszukana, może wnieść o wyłączenie dowodów uzyskanych lub pochodzących z bezprawnego przeszukania, jeśli dowody te zostaną przedstawione przeciwko tej osobie podczas procesu karnego. Zob. wyrok w sprawie Mapp przeciwko Ohio, 367 U.S. 643 (1961). W przypadku gdy posiadacz danych jest zobowiązany do ujawnienia danych na podstawie nakazu, strona zobowiązana może zakwestionować wymóg ujawnienia danych jako nadmiernie obciążający. Zob. wniosek Stanów Zjednoczonych w przedmiotowej sprawie, 610 F.2d 1148, 1157 (Sąd Apelacyjny dla Trzeciego Okręgu, 1979) (w którym uznano, że „należyty proces wymaga przesłuchania w kwestii potencjalnego nadmiernego obciążenia przed zobowiązaniem firmy telefonicznej do udzielenia" pomocy w odniesieniu do nakazu przeszukania); Wniosek Stanów Zjednoczonych w przedmiotowej sprawie, 616 F.2d 1122 (Sąd Apelacyjny dla Dziewiątego Okręgu, 1980) (w którym uznano tak samo w oparciu o uprawnienia sądu jako organu nadzorczego).

Wytyczne i strategie Departamentu Sprawiedliwości: niezależnie od wspomnianych konstytucyjnych, ustawowych i wynikających z zasad ograniczeń dostępu organów rządowych do danych Prokurator Generalny wydał wytyczne nakładające dodatkowe ograniczenia w obszarze dostępu organów egzekwowania prawa do danych – w wytycznych tych przewidziano również środki ochrony prywatności i wolności obywatelskich. Na przykład w wytycznych Prokuratora Generalnego w sprawie krajowych operacji Federalnego Biura Śledczego (FBI) (wrzesień 2008) (zwanych dalej wytycznymi Prokuratora Generalnego w sprawie FBI) dostępnych pod adresem http://www.justice.gov/archive/opa/docs/guidelines.pdf, ustanowiono ograniczenia w zakresie korzystania ze środków dochodzeniowych w celu gromadzenia informacji na potrzeby dochodzeń dotyczących przestępstw federalnych. Zgodne z treścią tych wytycznych FBI jest zobowiązane do stosowania możliwie jak najmniej inwazyjnych metod śledczych, biorąc pod uwagę ich wpływ na prywatność i wolności obywatelskie oraz potencjalne szkody wizerunkowe, jakie mogą wiązać się z ich stosowaniem. Ponadto w wytycznych podkreślono, że „oczywistym jest, że FBI musi prowadzić swoje dochodzenia i podejmować inne działania w zgodny z prawem i rozsądny sposób, tak aby zapewnić poszanowanie wolności obywatelskich i prywatności praworządnych jednostek i unikać zbędnych ingerencji w ich życie". Wytyczne Prokuratora Generalnego w sprawie FBI, s. 5. FBI wdrożyło te wytyczne w ramach poradnika dotyczącego prowadzenia dochodzeń i operacji na szczeblu krajowym (DIOG), dostępnego pod adresem https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29; dokument ten stanowi kompleksowy podręcznik zawierający szczegółowe informacje o ograniczeniach w zakresie korzystania z narzędzi dochodzeniowych oraz wskazówki służące zapewnieniu ochrony wolności obywatelskich i prywatności w każdym dochodzeniu. Dodatkowe zasady i strategie ograniczające działalność śledczą prokuratorów federalnych zostały ustanowione w podręczniku wymiaru sprawiedliwości, który jest również dostępny pod adresem https://www.justice.gov/jm/justicemanual.

Organy administracji cywilnej lub regulacyjne (interes publiczny):

([4]) Ponadto w sekcji 2705 lit. b) ustawy o przechowywanych danych przekazywanych za pomocą łączności elektronicznej upoważniono rząd do uzyskania nakazu sądowego w oparciu o wykazaną potrzebę ochrony przed ujawnieniem, jednocześnie zakazując dostawcy usług telekomunikacyjnych dobrowolnego powiadamiania swoich użytkowników o otrzymaniu pisma sądowego w związku z przepisami tej ustawy. W październiku 2017 r. Zastępca Prokuratora Generalnego Rod Rosenstein wydał memorandum skierowane do prawników i przedstawicieli DoJ, w którym określił wytyczne mające na celu zapewnienie, aby wnioski o takie nakazy zabezpieczające były dostosowane do konkretnych faktów i obaw związanych z dochodzeniem, oraz ustanowił ogólny roczny limit czasu, przez jaki możliwe jest dążenie do opóźnienia powiadomienia na podstawie wniosku. W maju 2022 r. zastępca prokuratora generalnego Lisa Monaco wydała dodatkowe wytyczne na ten temat, na mocy których m.in. ustanowiono wewnętrzne wymagania DoJ dotyczące zatwierdzania wniosków o przedłużenie nakazu zabezpieczającego poza początkowo ustalony okres jednego roku i wprowadzono wymóg zaprzestania wykonywania nakazów zabezpieczających po zakończeniu dochodzenia.

Ustanowiono również istotne ograniczenia w zakresie dostępu do danych posiadanych przez korporacje w Stanach Zjednoczonych przez organy administracji cywilnej lub regulacyjne (tj. ze względu na „interes publiczny"). Agencje o kompetencjach cywilnych i regulacyjnych mogą wezwać korporacje do przekazania dokumentacji dotyczącej prowadzonej działalności, informacji przechowywanych w formie elektronicznej lub innych przedmiotów materialnych. Możliwość korzystania przez tego rodzaju agencje z aktów stanowiących podstawę prawną dla wezwań administracyjnych lub wezwań do udziału w postępowaniu cywilnym jest ograniczona nie tylko postanowieniami ich statutów założycielskich, ale również faktem, że przed ewentualnym wyegzekwowaniem wezwania musi zostać ono poddane niezależnej kontroli sądowej. Zob. np. zasada 45 federalnego kodeksu postępowania karnego. Agencje mogą zwrócić się o udzielenie im dostępu wyłącznie do tych danych, które są istotne dla kwestii wchodzących w zakres przysługujących im uprawnień. Ponadto odbiorca wezwania administracyjnego może sprzeciwić się wezwaniu do sądu, przedstawiając dowody świadczące o tym, że agencja nie działała zgodnie z podstawowymi normami racjonalności, jak omówiono powyżej.

Przedsiębiorstwa mogą również podważyć zasadność składanych przez agencje administracyjne wniosków o udostępnienie danych w oparciu o inne podstawy prawne, w zależności od sektora, w którym prowadzą działalność, oraz od rodzaju danych znajdujących się w ich posiadaniu. Na przykład instytucje finansowe mogą zakwestionować zasadność wezwań administracyjnych do udostępnienia określonych rodzajów informacji, argumentując, że takie wezwania naruszają przepisy ustawy o tajemnicy bankowej i przepisów wykonawczych do tej ustawy. Zob. tytuł 31 § 5318 U.S.C., tytuł 31 część X C.F.R. Inne przedsiębiorstwa mogą powołać się na przepisy ustawy o rzetelnej sprawozdawczości kredytowej, zob. tytuł 15 § 1681b U.S.C., lub na szereg innych przepisów sektorowych. Nadużywanie przez agencję aktów stanowiących podstawę prawną do wydawania wezwań może skutkować pociągnięciem agencji do odpowiedzialności lub pociągnięciem urzędników agencji do odpowiedzialności osobistej. Zob. np. ustawa o prawie do prywatności w kwestiach finansowych, tytuł 12 § 3401–3423 U.S.C. Dlatego też sądy w Stanach Zjednoczonych zapewniają stosownym podmiotom ochronę przed nieprawidłowymi żądaniami organów regulacyjnych i sprawują niezależny nadzór nad działalnością agencji federalnych.

Ponadto wszelkie przysługujące organom administracji uprawnienia ustawowe do fizycznego zajęcia rejestrów prowadzonych przez przedsiębiorstwo w Stanach Zjednoczonych w drodze przeszukania administracyjnego muszą być zgodne z wymogami czwartej poprawki. Zob. wyrok w sprawie See przeciwko miastu Seattle, 387 U.S. 541 (1967).

Wniosek:

Wszystkie działania w obszarze egzekwowania prawa i wszystkie działania regulacyjne w Stanach Zjednoczonych muszą być prowadzone zgodnie z obowiązującym prawem, przy jednoczesnym uwzględnieniu postanowień konstytucji Stanów Zjednoczonych, ustaw, przepisów i regulacji. Takie działania muszą być również zgodnie z obowiązującymi strategiami oraz wytycznymi Prokuratora Generalnego dotyczącymi działań organów egzekwowania prawa na szczeblu federalnym. Opisane powyżej ramy prawne ograniczają zdolność amerykańskich organów egzekwowania prawa i agencji regulacyjnych do pozyskiwania informacji od korporacji w Stanach Zjednoczonych – niezależnie od tego, czy stosowne informacje dotyczą obywateli i rezydentów Stanów Zjednoczonych czy obywateli państw trzecich – oraz zapewniają możliwość poddawania kontroli sądowej wszelkich żądań udostępnienia danych wystosowywanych na podstawie aktów stanowiących podstawę prawną.

Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

ZAŁĄCZNIK VII

URZĄD DYREKTORA KRAJOWYCH SŁUŻB WYWIADOWCZYCH GŁÓWNEGO DORADCY

WASZYNGTON, DC 20511

Dnia 9 grudnia 2022 r.

Leslie B. Kiernan
Główny Doradca
Departamentu Handlu Stanów
Zjednoczonych 1401 Constitution
Ave., NW Washington, DC 20230

Szanowna Pani!

7 października 2022 r. prezydent Biden podpisał rozporządzenie wykonawcze nr 14086 dotyczące zwiększenia gwarancji dla działań w zakresie rozpoznania radioelektronicznego Stanów Zjednoczonych (*Enhancing Safeguards for United States Signals Intelligence Activities*), wzmacniające ściśle określony wachlarz gwarancji na rzecz ochrony prywatności i wolności obywatelskich mających zastosowanie do działalności w zakresie rozpoznania radioelektronicznego w Stanach Zjednoczonych. Gwarancje te obejmują: wymóg zakładający osiągnięcie zamkniętej listy uzasadnionych celów podczas realizacji działań w zakresie rozpoznania radioelektronicznego; wyraźne zakazanie takich działań w celu realizacji określonych zakazanych celów; wprowadzenie nowatorskich procedur w celu zapewnienia, aby działania w zakresie rozpoznania radioelektronicznego były zgodne z takimi uzasadnionymi celami i nie wspierają realizacji celów zakazanych; wymóg zakładający prowadzenie działań w zakresie rozpoznania radioelektronicznego wyłącznie po ustaleniu, w oparciu o racjonalną ocenę wszystkich istotnych czynników, że działania takie są niezbędne do realizacji zatwierdzonego priorytetu wywiadowczego w odniesieniu do rozpoznania radioelektronicznego i tylko w zakresie proporcjonalnym oraz w sposób proporcjonalny do zatwierdzonego priorytetu wywiadowczego, w odniesieniu do którego działania takie zostały dozwolone; oraz nakazanie jednostkom Wspólnoty Wywiadowczej przeprowadzenia aktualizacji ich polityk i procedur, tak aby odzwierciedlały wymagane na mocy rozporządzenia wykonawczego gwarancje dotyczące rozpoznana radioelektronicznego. Co najważniejsze, w rozporządzeniu wykonawczym wprowadzono również niezależny i wiążący mechanizm umożliwiający osobom z „kwalifikujących się stanów", wyznaczonych zgodnie z treścią przedmiotowego rozporządzenia, dochodzenie roszczeń, jeśli uważają, że zostały poddane bezprawnym działaniom w zakresie rozpoznania radioelektronicznego Stanów Zjednoczonych, w tym działaniom naruszającym gwarancje określone w rozporządzeniu wykonawczym.

Wydanie przez prezydenta Bidena rozporządzenia wykonawczego nr 14086 stanowi zwieńczenie trwających ponad rok szczegółowych negocjacji między przedstawicielami Komisji Europejskiej i Stanów Zjednoczonych, a w rozporządzeniu tym określono kroki, jakie Stany Zjednoczone podejmą w celu realizacji swoich zobowiązań wynikających z ram ochrony danych UE–USA. W duchu współpracy, dzięki któremu powstały przedmiotowe ramy, jak sądzę otrzymała Pani od Komisji Europejskiej dwa zestawy pytań dotyczących sposobu, w jaki Wspólnota Wywiadowcza wdroży zapisy rozporządzenia wykonawczego. Z przyjemnością odpowiem na te pytania w niniejszym piśmie.

Sekcja 702 ustawy o kontroli wywiadu z 1978 r.

Pierwszy zestaw pytań dotyczy sekcji 702 ustawy o kontroli wywiadu, której zapisy umożliwiają pozyskiwanie danych wywiadowczych poprzez ukierunkowanie działań na osoby niebędące obywatelami ani rezydentami Stanów Zjednoczonych, co do których istnieje uzasadnione podejrzenie, że znajdują się poza granicami Stanów Zjednoczonych, przy obowiązkowej pomocy ze strony amerykańskich dostawców usług łączności elektronicznej. W szczególności pytania te dotyczą relacji zachodzących między tym przepisem a rozporządzeniem wykonawczym nr 14086, a także pozostałymi gwarancjami, które mają zastosowanie do działań prowadzonych zgodnie z zapisami sekcji 702 ustawy o kontroli wywiadu.

Przede wszystkim możemy potwierdzić, że Wspólnota Wywiadowcza stosować będzie gwarancje określone w rozporządzeniu wykonawczym nr 14086 dotyczące działań prowadzonych zgodnie z sekcją 702 ustawy o kontroli wywiadu.

Ponadto wiele innych gwarancji odnosi się do korzystania przez rząd z zapisów sekcji 702 ustawy o kontroli wywiadu. Na przykład wszystkie certyfikacje wynikające z sekcji 702 ustawy o kontroli wywiadu muszą zostać podpisane zarówno przez Prokuratora Generalnego, jak i Dyrektora Krajowych Służb Wywiadowczych, a rząd zobowiązany jest przedłożyć wszystkie takie certyfikacje do zatwierdzenia przez Sąd ds. Kontroli Wywiadu, składający się z niezależnych sędziów wybieranych dożywotnio, na nieodnawialną siedmioletnią kadencję. W certyfikacjach określa się kategorie danych wywiadowczych, które muszą spełniać wymogi ustawowej definicji danych wywiadowczych i które mają być gromadzone za pomocą ukierunkowywania działań na osoby niebędące obywatelami ani rezydentami Stanów Zjednoczonych, w odniesieniu do których można racjonalnie założyć, że znajdują się poza terytorium Stanów Zjednoczonych. Certyfikacje obejmują informacje dotyczące międzynarodowego terroryzmu i inne tematy, takie jak pozyskiwanie informacji dotyczących broni masowego rażenia. Każda coroczna certyfikacja musi zostać przedłożona Sądowi ds. Kontroli Wywiadu do zatwierdzenia w formie pakietu wniosków o certyfikację, zawierającego certyfikację Prokuratora Generalnego i Dyrektora Krajowych Służb Wywiadowczych, oświadczenia z mocą przysięgi niektórych szefów agencji wywiadu oraz opis wiążących dla rządu procedur ukierunkowywania, minimalizacji i zapytań. W ramach procedur ukierunkowywania wymagane jest, między innymi, aby Wspólnota Wywiadowcza w sposób racjonalny oceniła, w oparciu o ogół okoliczności, że ukierunkowywanie działań prawdopodobnie doprowadzi do zgromadzenia danych wywiadowczych określonych w certyfikacji zgodnie z zapisami sekcji 702 ustawy o kontroli wywiadu.

Ponadto podczas gromadzenia danych zgodnie z sekcją 702 ustawy o kontroli wywiadu, Wspólnota Wywiadowcza zobowiązana jest: dostarczyć pisemne wyjaśnienie podstaw uznania, że w momencie ukierunkowywania działań na daną osobę prawdopodobnie posiada, prawdopodobnie otrzyma lub prawdopodobnie przekaże dane wywiadowcze określone w certyfikacji zgodnie z zapisami sekcji 702 ustawy o kontroli wywiadu; potwierdzić, że spełniane są wymogi normy dotyczącej ukierunkowywania działań określonej w procedurach ukierunkowywania zawartych w sekcji 702 ustawy o kontroli wywiadu; oraz zaprzestać gromadzenia danych, jeśli wymogi normy nie są już spełniane. *Zob*. dokument przedłożony Sądowi ds. Kontroli Wywiadu przez rząd Stanów Zjednoczonych, „2015 Summary of Notable Section 702 Requirements" („Podsumowanie najważniejszych wymogów określonych w sekcji 702, 2015 r."), 2–3 (15 lipca 2015 r.).

Wymaganie od Wspólnoty Wywiadowczej rejestrowania na piśmie i regularnego potwierdzania ważności dokonanej przez tę Wspólnotę oceny tego, czy w stosunku do określonych osób, których dotyczy sekcja 702 ustawy o kontroli wywiadu, spełnione są obowiązujące normy ukierunkowywania, ułatwia nadzór Sądu ds. Kontroli Wywiadu nad działaniami Wspólnoty Wywiadowczej w odniesieniu do ukierunkowywania. Każda zarejestrowana ocena dotycząca ukierunkowywania, wraz z uzasadnieniem, jest sprawdzana co dwa miesiące przez prawników zajmujących się nadzorem nad służbami wywiadowczymi w Departamencie Sprawiedliwości (DoJ), wykonującymi taką funkcję nadzorczą niezależnie od działań w obszarze wywiadu zagranicznego. Zgodnie z ugruntowaną zasadą przestrzeganą przez Sąd ds. Kontroli Wywiadu dział DoJ pełniący taką funkcję nadzorczą jest również odpowiedzialny za zgłaszanie temu sądowi wszelkich naruszeń obowiązujących procedur. Taka forma sprawozdawczości, w połączeniu z regularnymi spotkaniami Sądu ds. Kontroli Wywiadu z przedstawicielami tego działu DoJ dotyczącymi nadzoru nad ukierunkowywaniem działań prowadzonym zgodnie z sekcją 702 ustawy o kontroli wywiadu, umożliwia Sądowi egzekwowanie zgodności z zapisami dotyczącymi ukierunkowywania zawartymi w sekcji 702 tej ustawy i innymi procedurami oraz w inny sposób gwarantuje, że działania rządu są zgodne z prawem. Sąd ds. Kontroli Wywiadu może to zrobić na wiele sposobów, w tym za pomocą wydawania wiążących decyzji naprawczych w celu wycofania upoważnienia rządu do gromadzenia danych przeciwko danej osobie lub w celu zmodyfikowania lub opóźnienia gromadzenia danych zgodnie z zapisami sekcji 702 ustawy o kontroli wywiadu. Sąd ds. Kontroli Wywiadu może również zażądać od rządu dostarczenia kolejnych sprawozdań lub informacji na temat zgodności z procedurami ukierunkowywania i innymi procedurami lub zażądać wprowadzenia zmian do tych procedur.

„Hurtowe" gromadzenie informacji w ramach rozpoznania radioelektronicznego

Drugi zestaw pytań dotyczy „hurtowego" gromadzenia informacji w ramach rozpoznania radioelektronicznego, które w rozporządzeniu wykonawczym nr 14086 zdefiniowano jako „uprawnione gromadzenie dużych ilości danych w ramach rozpoznania radioelektronicznego, które ze względów technicznych lub operacyjnych jest dokonywane bez wykorzystania wyróżników (np. konkretnych identyfikatorów lub terminów umożliwiających selekcję)".

W odniesieniu do tych pytań należy przede wszystkim zauważyć, że ani ustawa o kontroli wywiadu, ani wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego nie zezwalają na hurtowe gromadzenie informacji. W odniesieniu do ustawy o kontroli wywiadu:

— Zgodnie z tytułami I i III ustawy o kontroli wywiadu, które zezwalają odpowiednio na obserwację elektroniczną oraz przeszukania, wymagany jest nakaz sądowy (z ograniczonymi wyjątkami, takimi jak nagłe przypadki); zawsze należy określić również prawdopodobną przyczynę podejrzeń, że dana osoba działa na korzyść innego kraju lub jest jego przedstawicielem. *Zob*. tytuł 50 § 1805 i 1824 U.S.C.

— Amerykańską ustawą o wolności z 2015 r. zmieniono tytuł IV ustawy o kontroli wywiadu zezwalający na korzystanie z urządzeń rejestrujących wybierane numery oraz urządzeń śledzących (z wyjątkiem nagłych przypadków), wprowadzając wobec rządu wymóg oparcia składanych wniosków na „konkretnych terminach umożliwiających selekcję". *Zob*. tytuł 50 § 1842 lit. c) pkt 3 U.S.C.

— W tytule V ustawy o kontroli wywiadu, zgodnie z którym zezwala się Federalnemu Biuru Śledczemu (FBI) na uzyskiwanie niektórych rodzajów rejestrów handlowych, zawarto wymóg wydania nakazu sądowego opartego na wniosku, w którym stwierdza się, że „istnieją konkretne i jasne fakty, zgodnie z którymi istnieją podstawy, by przypuszczać, że osoba, której rejestry dotyczą, działa na korzyść innego kraju lub jest jego przedstawicielem". *Zob*. tytuł 50 § 1862 lit. b) pkt 2 ppkt B U.S.C. ([1]).

— Ponadto zgodnie z przepisami sekcji 702 ustawy o kontroli wywiadu zezwala się na „ukierunkowywanie działań na osoby, co do których istnieje uzasadnione podejrzenie, że przebywają poza terytorium Stanów Zjednoczonych w celu pozyskiwania danych wywiadowczych". *Zob*. tytuł 50 § 188la lit. a) U.S.C. W związku z tym, zgodnie z opinią Rady Nadzoru nad Ochroną Danych i Wolnościami Obywatelskimi, gromadzenie danych przez rząd na podstawie sekcji 702 ustawy o kontroli wywiadu „polega wyłącznie na ukierunkowywaniu działań na poszczególne osoby i pozyskiwaniu wiadomości związanych z tymi osobami, co do których istnieją przesłanki aby przypuszczać, że uzyska się od nich określone rodzaje danych wywiadowczych", tak że „program ten nie polega na hurtowym gromadzeniu informacji". Przygotowane przez Radę Nadzoru nad Ochroną Danych i Wolnościami Obywatelskimi „Sprawozdanie z programu kontroli funkcjonującego zgodnie z art. 702 ustawy o kontroli wywiadu" („Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act"), s. 103 (2 lipca 2014 r.) ([2]).

W odniesieniu do wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego w amerykańskiej ustawie o wolności z 2015 r. nałożono wymóg dotyczący „konkretnych terminów umożliwiających selekcję" na korzystanie z takich wezwań. *Zob*. tytuł 12 § 3414 lit. a) pkt 2 U.S.C., tytuł 15 § 1681u U.S.C., tytuł 15 § 1681v lit. a) U.S.C., tytuł 18 § 2709 lit. b) U.S.C.

Ponadto rozporządzenie wykonawcze nr 14086 stanowi, że „[u]kierunkowane gromadzenie danych będzie traktowane priorytetowo" oraz że w przypadku, gdy Wspólnota Wywiadowcza prowadzi hurtowe gromadzenie danych, takie „gromadzone hurtowo dane pochodzące z rozpoznania radioelektronicznego muszą być zatwierdzane wyłącznie na podstawie wskazania (...), że informacje niezbędne do realizacji zatwierdzonego priorytetu wywiadowczego nie mogą być w sposób zasadny uzyskiwane w drodze ukierunkowanego gromadzenia danych". *Zob*. rozporządzenie wykonawcze nr 14086, § 2 lit. c) pkt (ii) ppkt A.

Co więcej, w rozporządzeniu wykonawczym nr 14086 zapewniono dodatkowe gwarancje w przypadku, gdy Wspólnota Wywiadowcza ustali, że hurtowe gromadzenie danych spełnia wspomniane wymagania. W szczególności zgodnie z tym rozporządzeniem wykonawczym wymagane jest, aby Wspólnota Wywiadowcza, prowadząc hurtowe gromadzenie danych, „stosowała zasadne metody i środki techniczne w celu ograniczenia gromadzenia danych tylko do tych danych, których posiadanie jest niezbędne do realizacji zatwierdzonego priorytetu wywiadowczego, przy jednoczesnym zminimalizowaniu gromadzenia nieistotnych informacji". *Zob*. *tamże*. Rozporządzenie stanowi również, że „działania w zakresie rozpoznania radioelektronicznego", obejmujące zapewnienie zgodności danych pochodzących z takiego rozpoznania uzyskanych w drodze hurtowego gromadzenia danych, „będą prowadzone wyłącznie po ustaleniu, w oparciu o racjonalną ocenę wszystkich istotnych czynników, że działania takie są niezbędne do realizacji zatwierdzonego priorytetu wywiadowczego". *Zob*. *tamże* § 2 lit. a) pkt (ii) ppkt A. W dalszej części rozporządzenia określono sposób wdrażania tej zasady, stwierdzając, że Wspólnota Wywiadowcza może jedynie kierować zapytania dotyczące niezminimalizowanych danych pochodzących z rozpoznania radioelektronicznego uzyskiwanych hurtowo w ramach realizacji sześciu dopuszczalnych celów oraz że takie zapytania muszą być formułowane zgodnie z polityką i procedurami, w których „odpowiednio uwzględniono wpływ [zapytań] na prywatność i wolności obywatelskie wszystkich osób, niezależnie od ich narodowości lub miejsca zamieszkania". *Zob*. *tamże* § 2 lit. c) pkt (iii) ppkt D. Ponadto w rozporządzeniu określono środki dotyczące przetwarzania i zapewnienia bezpieczeństwa gromadzonych danych oraz kontroli dostępu do tych danych. *Zob*. *tamże* § 2 lit. c) pkt (iii) ppkt A oraz § 2 lit. c) pkt (iii) ppkt B.

* * * * *

Mamy nadzieję, że powyższe wyjaśnienia okażą się pomocne. Prosimy o kontakt w przypadku dalszych pytań dotyczących sposobu, w jaki amerykańska Wspólnota Wywiadowcza planuje wdrożyć rozporządzenie wykonawcze nr 14086.

([1]) Od 2001 r. do 2020 r. na mocy tytułu V ustawy o kontroli wywiadu FBI było upoważnione do ubiegania się o zezwolenie od Sądu ds. Kontroli Wywiadu na uzyskanie „przedmiotów materialnych", które są istotne w niektórych zatwierdzonych dochodzeniach. *Zob*. amerykańska ustawa antyterrorystyczna („USA Patriot Act"), Pub. L. nr 107–56, 115 Stat. 272, § 215 (2001). Ta obecnie wygasła, a zatem niestanowiąca już części obowiązującego prawa ustawa nadawała rządowi upoważnienie, na podstawie którego w pewnym momencie hurtowo gromadził on metadane telefoniczne. Jednak jeszcze przed jej wygaśnięciem ustawa ta została zmieniona amerykańską ustawą o wolności w taki sposób, aby od rządu wymagane było oparcie wniosku kierowanego do Sądu ds. Kontroli Wywiadu na „konkretnych terminach umożliwiających selekcję". *Zob*. amerykańska ustawa o wolności („USA Freedom Act"), Pub. L. nr 114–23, 129 Stat. 268, § I 03 (2015).

([2]) W sekcjach 703 i 704, na mocy których Wspólnota Wywiadowcza upoważniona jest do namierzania obywateli i rezydentów Stanów Zjednoczonych przebywających za granicą, zawarto wymóg wydania nakazu sądowego (z wyjątkiem nagłych przypadków) oraz wymóg każdorazowego istnienia uzasadnionego podejrzenia pozwalającego przypuszczać, że dana osoba działa na korzyść innego kraju, jest jego przedstawicielem, funkcjonariuszem lub pracownikiem. *Zob*. *tytuł 50* § 1881b i 1881c U.S.C.

Sincerly,

Christopher C. FONZONE
Główny Doradca

ZAŁĄCZNIK VIII

Wykaz skrótów

W niniejszej decyzji występują następujące skróty:

AAA	Amerykańskie Stowarzyszenie Arbitrażowe
AGG-DOM	wytyczne prokuratora generalnego w sprawie krajowych operacji Federalnego Biura Śledczego (FBI)
APA	ustawa o postępowaniu administracyjnym
CIA	Centralna Agencja Wywiadowcza
CNSS	Komitet ds. Systemów Bezpieczeństwa Narodowego
decyzja	decyzja wykonawcza Komisji na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE–USA
DHS	Departament Bezpieczeństwa Wewnętrznego
DNI	Dyrektor Krajowych Służb Wywiadowczych
DoC	Departamentu Handlu USA
DoJ	Departament Sprawiedliwości USA
DoT	Departament Transportu USA
DPA	organ ochrony danych
DPF UE-USA lub DPF	ramy ochrony danych UE–USA
DPRC	Sąd ds. Kontroli Ochrony Danych
dyrektywa polityczna Prezydenta nr 28	dyrektywa polityczna Prezydenta nr 28
ECOA	ustawa o równych możliwościach kredytowych
ECPA	ustawa o ochronie danych w łączności elektronicznej
EOG	Europejski Obszar Gospodarczy
FBI	Federalne Biuro Śledcze
FCRA	ustawa o rzetelnej sprawozdawczości kredytowej
FISA	ustawa o kontroli wywiadu
FISC	Sąd ds. Kontroli Wywiadu
FISCR	Sąd Apelacyjny ds. Kontroli Wywiadu
FOIA	ustawa o wolności informacji
FRA	ustawa o rejestrach federalnych
FTC	Federalna Komisja Handlu USA
HIPAA	ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych
ICDR	Międzynarodowe Centrum Rozstrzygania Sporów
IOB	Rada Nadzoru nad Służbami Wywiadowczymi
NIST	Krajowy Instytut Standaryzacji i Technologii

NSA	Agencja Bezpieczeństwa Narodowego
NSL	wezwanie do przedstawienia informacji do celów bezpieczeństwa narodowego
ODNI	Urząd Dyrektora Krajowych Służb Wywiadowczych
ODNI CLPO, CLPO	urzędnik ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych, urzędnik ds. ochrony wolności obywatelskich
OMB	Urząd ds. Administracji i Budżetu
OPCL	Biuro Ochrony Prywatności i Wolności Obywatelskich Departamentu Sprawiedliwości
panel ds. DPF UE–USA	panel ds. ram ochrony danych UE–USA
PCLOB	Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi
PIAB	prezydencka Rada Konsultacyjna ds. Wywiadu
rozporządzenie (UE) 2016/679	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 danych oraz uchylenia dyrektywy 95/46/WE
rozporządzenie wykonawcze 12333	rozporządzenie wykonawcze 12333 „Działania wywiadowcze Stanów Zjednoczonych”
rozporządzenie wykonawcze 14086, rozporządzenie wykonawcze	rozporządzenie wykonawcze 14086 „Poprawa zabezpieczeń dotyczących działań Stanów Zjednoczonych w zakresie rozpoznania radioelektronicznego”
SAOP	urzędnik wyższego szczebla Agencji ds. Prywatności
Trybunał Sprawiedliwości	Trybunał Sprawiedliwości Unii Europejskiej
zarządzenie prokuratora generalnego	zarządzenie Sądu Odwoławczego ds. Ochrony Danych wydane przez prokuratora generalnego USA
Zasady	zasady ramowe ochrony danych UE–USA
Unia	Unia Europejska
USA	Stany Zjednoczone
wykaz DPF	wykaz podmiotów objętych ramami ochrony danych