II

(Akty o charakterze nieustawodawczym)

DECYZJE

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

(notyfikowana jako dokument nr C(2016) 4176)

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ([1]), w szczególności jej art. 25 ust. 6,

po zasięgnięciu opinii Europejskiego Inspektora Ochrony Danych ([2]),

1. WPROWADZENIE

(1) W dyrektywie 95/46/WE określa się zasady przekazywania danych osobowych z państw członkowskich do państw trzecich w zakresie, w jakim takie przekazywanie danych jest objęte zakresem stosowania dyrektywy.

(2) Artykuł 1 dyrektywy 95/46/WE oraz motywy 2 i 10 jej preambuły mają zapewnić nie tylko skuteczną i pełną ochronę podstawowych praw i wolności osób fizycznych, w szczególności ich prawa podstawowego do poszanowania życia prywatnego w odniesieniu do przetwarzania danych osobowych, ale także wysokiego stopnia ochrony tych podstawowych praw i wolności ([3]).

(3) Znaczenie zarówno prawa podstawowego do poszanowania życia prywatnego zagwarantowanego w art. 7, jak i prawa podstawowego do ochrony danych osobowych zagwarantowanego w art. 8 Karty praw podstawowych Unii Europejskiej zostało podkreślone w orzecznictwie Trybunału Sprawiedliwości ([4]).

(4) Zgodnie z art. 25 ust. 1 dyrektywy 95/46/WE państwa członkowskie są zobowiązane zapewnić, aby przekazywanie danych osobowych do państwa trzeciego mogło nastąpić tylko wówczas gdy, dane państwo trzecie zapewnia odpowiedni stopień ochrony, a prawa państw członkowskich wprowadzających w życie inne przepisy dyrektywy są przestrzegane przed przekazaniem danych. Komisja może uznać, że państwo trzecie zapewnia taki odpowiedni stopień ochrony z uwagi na jego prawo krajowe lub zobowiązania międzynarodowe, jakie państwo to podjęło w celu ochrony praw osób fizycznych. W takim przypadku – bez uszczerbku dla zgodności z przepisami krajowymi przyjętymi zgodnie z innymi przepisami dyrektywy – dane osobowe mogą być przekazywane z państw członkowskich bez konieczności ustanowienia dodatkowych gwarancji.

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Zob. opinia nr 4/2016 dotycząca projektu decyzji w sprawie odpowiedniej ochrony danych osobowych w ramach Tarczy Prywatności UE-USA, opublikowana w dniu 30 maja 2016 r.
([3]) Sprawa C-362/14, Maximillian Schrems przeciwko Data Protection Commissioner („wyrok w sprawie Schrems"), EU:C:2015:650, pkt 39.
([4]) Sprawa C-553/07, Rijkeboer, EU:C:2009:293, pkt 47; sprawy połączone C-293/12 i C-594/12, Digital Rights Ireland i in., EU:C:2014:238, pkt 53; sprawa C-131/12, Google Spain i Google, EU:C:2014:317, pkt 53, 66 i 74.

(5) Zgodnie z art. 25 ust. 2 dyrektywy 95/46/WE stopień ochrony danych zapewnianej przez państwo trzecie należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zbioru takich operacji, w tym przepisów prawa, zarówno ogólnych, jak i sektorowych, obowiązujących w danym państwie trzecim.

(6) W decyzji Komisji 2000/520/WE ([5]), przyjętej do celów art. 25 ust. 2 dyrektywy 95/46/WE, uznano, że zasady ochrony prywatności w ramach „bezpiecznej przystani" wdrożone zgodnie z wytycznymi zawartymi w „najczęściej zadawanych pytaniach" wydanych przez Departament Handlu Stanów Zjednoczonych, zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do podmiotów mających siedzibę w Stanach Zjednoczonych.

(7) Komisja w swoich komunikatach COM(2013) 846 final ([6]) i COM(2013) 847 final ([7]) z dnia 27 listopada 2013 r. uznała, że konieczne jest dokonanie przeglądu i wzmocnienie zasadniczej podstawy programu „bezpieczna przystań" w kontekście wielu czynników, w tym gwałtownego wzrostu przepływów danych i ich kluczowego znaczenia dla gospodarki transatlantyckiej, szybko rosnącej liczby przedsiębiorstw w Stanach Zjednoczonych przestrzegających programu „bezpieczna przystań" oraz nowych informacji dotyczących skali i zakresu niektórych amerykańskich programów nadzoru, które wzbudziły obawy dotyczące stopnia ochrony, jaki mogą zapewnić te programy. Ponadto Komisja zidentyfikowała szereg niedociągnięć i braków w programie „bezpieczna przystań".

(8) Na podstawie dowodów zebranych przez Komisję, w tym informacji wynikających z prac grupy kontaktowej UE-USA ds. ochrony prywatności ([8]) oraz informacji na temat amerykańskich programów wywiadowczych otrzymanych od grupy roboczej *ad hoc* UE-USA ([9]) Komisja sformułowała 13 zaleceń dotyczących przeglądu programu „bezpieczna przystań". Zalecenia te dotyczyły przede wszystkim: wzmocnienia konkretnych zasad dotyczących prywatności, zwiększenia przejrzystości polityki ochrony prywatności stosowanej przez samocertyfikowane przedsiębiorstwa amerykańskie, usprawnienia nadzoru nad przestrzeganiem tych zasad przez przedsiębiorstwa oraz monitorowania i egzekwowania przestrzegania tych zasad przez organy amerykańskie, zapewnienia dostępu do przystępnych cenowo mechanizmów rozstrzygania sporów oraz potrzeby zapewnienia ograniczenia korzystania z wyjątku dotyczącego bezpieczeństwa narodowego przewidzianego w decyzji 2000/520/WE do działań, których podjęcie jest ściśle konieczne i proporcjonalne.

(9) W swoim wyroku z dnia 6 października 2015 r. w sprawie C-362/14 Maximillian Schrems przeciwko Data Protection Commissioner ([10]) Trybunał Sprawiedliwości Unii Europejskiej orzekł nieważność decyzji 2000/520/WE. Bez badania treści zasad ochrony prywatności w ramach „bezpiecznej przystani" Trybunał uznał, że Komisja nie wykazała w swojej decyzji, iż Stany Zjednoczone rzeczywiście „zapewniają" odpowiedni stopień ochrony ze względu na swoje ustawodawstwo lub zobowiązania międzynarodowe ([11]).

(10) W tym kontekście Trybunał Sprawiedliwości wyjaśnił, że chociaż wyrażenie „odpowiedni stopień ochrony" zawarte w art. 25 ust. 6 dyrektywy 95/46/WE nie oznacza stopnia ochrony identycznego z tym, jaki jest gwarantowany w unijnym porządku prawnym, należy je rozumieć jako wymagające od tego państwa trzeciego zapewnienia stopnia ochrony podstawowych praw i wolności „merytorycznie równoważnego" stopniowi gwarantowanemu w Unii na mocy dyrektywy 95/46/WE w związku z Kartą praw podstawowych Unii Europejskiej. Jakkolwiek środki, z jakich to państwo trzecie korzysta w tym względzie, mogą różnić się od środków wprowadzonych w Unii, środki te muszą być jednak w praktyce skuteczne ([12]).

(11) Trybunał Sprawiedliwości skrytykował brak wystarczających ustaleń w decyzji 2000/520/WE, dotyczących istnienia w Stanach Zjednoczonych reguł o charakterze ogólnopaństwowym, służących do ograniczenia ewentualnych ingerencji w prawa podstawowe osób, których dane zostały przekazane z Unii do Stanów Zjednoczonych, ingerencji, których organy państwowe tego kraju mogłyby dokonywać przy okazji dążenia do realizacji uzasadnionego prawem celu, takiego jak bezpieczeństwo narodowe, oraz istnienia skutecznej ochrony prawnej przed ingerencją tego rodzaju ([13]).

([5]) Decyzja Komisji 2000/520/WE z dnia 26 lipca 2000 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (Dz.U. L 215 z 28.8.2000, s. 7).

([6]) Komunikat Komisji do Parlamentu Europejskiego i Rady – Odbudowa zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi, COM(2013) 846 final z dnia 27 listopada 2013 r.

([7]) Komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE, COM(2013) 847 final z dnia 27 listopada 2013 r.

([8]) Zob. np. Rada Unii Europejskiej, sprawozdanie końcowe grupy kontaktowej wysokiego szczebla UE-USA ds. wymiany informacji i ochrony danych osobowych i prywatności, nota 9831/08 z dnia 28 maja 2008 r., dostępna na stronie internetowej: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

([9]) Sprawozdanie z ustaleń współprzewodniczących z ramienia Unii w grupie roboczej ad hoc UE-USA ds. ochrony danych z dnia 27 listopada 2013 r., dostępne na stronie internetowej: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

([10]) Zob. przypis 3.

([11]) Wyrok w sprawie Schrems, pkt 97.

([12]) Wyrok w sprawie Schrems, pkt 73–74.

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

(12) W 2014 r. Komisja podjęła rozmowy z organami amerykańskimi celem omówienia wzmocnienia programu „bezpieczna przystań" zgodnie z 13 zaleceniami zawartymi w komunikacie COM(2013) 847 final. Po wydaniu przez Trybunał Sprawiedliwości Unii Europejskiej wyroku w sprawie Schrems rozmowy te zintensyfikowano w celu ewentualnego przyjęcia nowej decyzji w sprawie odpowiedniej ochrony danych osobowych, która spełniałaby wymogi określone w art. 25 dyrektywy 95/46/WE, zgodnie z wykładnią Trybunału Sprawiedliwości. Dokumenty, które załączono do tej decyzji i które również zostaną opublikowane w amerykańskim Rejestrze Federalnym, są wynikiem tych dyskusji. Zasady ochrony prywatności (załącznik II) oraz oficjalne oświadczenia i zobowiązania różnych organów amerykańskich zawarte w dokumentach załączonych jako załączniki I, III–VII składają się na „Tarczę Prywatności UE-USA".

(13) Komisja uważnie przeanalizowała prawo i praktykę Stanów Zjednoczonych, w tym wspomniane oficjalne oświadczenia i zobowiązania. W oparciu o ustalenia przedstawione w motywach 136–140 Komisja stwierdza, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych w ramach Tarczy Prywatności UE-USA z Unii do samocertyfikowanych podmiotów w Stanach Zjednoczonych.

2. **„TARCZA PRYWATNOŚCI UE-USA"**

(14) Tarcza Prywatności UE-USA opiera się na systemie samocertyfikacji, zgodnie z którym amerykańskie podmioty zobowiązują się przestrzegać zbioru zasad ochrony prywatności – zasad ramowych Tarczy Prywatności UE-USA, w tym zasad uzupełniających (zwanych dalej łącznie: „zasadami") – wydanych przez Departament Handlu USA i zawartych w załączniku II do niniejszej decyzji. Ma ona zastosowanie zarówno do administratorów danych, jak i podmiotów przetwarzających dane (przedstawicieli), z uwzględnieniem faktu, że podmioty przetwarzające muszą być zobowiązane umownie do działania wyłącznie na polecenie unijnego administratora danych i do wspomagania tego administratora w udzielaniu odpowiedzi osobom fizycznym, które korzystają ze swoich praw wynikających z zasad ([14]).

(15) Bez uszczerbku dla przestrzegania przepisów krajowych przyjętych na mocy dyrektywy 95/46/WE niniejsza decyzja skutkuje tym, że przekazywanie danych od administratora danych lub podmiotu przetwarzającego dane w Unii do podmiotów w USA, które przyjęły zasady w drodze samocertyfikacji w Departamencie Handlu i zobowiązały się do ich przestrzegania, jest dozwolone. Zasady mają zastosowanie wyłącznie do przetwarzania danych osobowych przez amerykańskie podmioty w zakresie, w jakim przetwarzanie przez takie podmioty nie wchodzi w zakres prawodawstwa unijnego ([15]). Tarcza Prywatności pozostaje bez wpływu na stosowanie unijnego prawodawstwa regulującego przetwarzanie danych osobowych w państwach członkowskich ([16]).

([14]) Zob. załącznik II sekcja III pkt 10 lit. a). Zgodnie z definicją zawartą w sekcji I pkt 8 lit. c) administrator danych określi cel i środki przetwarzania danych osobowych. Co więcej, w umowie z przedstawicielem należy wyraźnie zaznaczyć, czy wtórne przekazywanie jest dozwolone (zob. sekcja III pkt 10 lit. a) ppkt (ii) pkt 2).

([15]) Ma to również zastosowanie w przypadku danych o zasobach ludzkich przekazywanych z Unii w kontekście stosunku pracy. Chociaż w zasadach podkreślono „główną odpowiedzialność" unijnego pracodawcy (zob. załącznik II sekcja III pkt 9 lit. d) ppkt (i)), jednocześnie zaznaczono w nich wyraźnie, że postępowanie pracodawcy będzie podlegać przepisom mającym zastosowanie w Unii lub w odpowiednim państwie członkowskim, a nie zasadom. Zob. załącznik II sekcja III pkt 9 lit. a) ppkt (i), sekcja III pkt 9 lit. b) ppkt (ii), sekcja III pkt 9 lit. c) ppkt (i), sekcja III pkt 9 lit. d) ppkt (i).

([16]) Ma to również zastosowanie do przetwarzania, które odbywa się za pomocą urządzeń znajdujących się w Unii, ale wykorzystywanych przez podmiot z siedzibą poza Unią (zob. art. 4 ust. 1 lit. c) dyrektywy 95/46/WE). Od dnia 25 maja 2018 r. ogólne rozporządzenie o ochronie danych będzie miało zastosowanie do przetwarzania danych osobowych: (i) w kontekście działań przedsiębiorstwa administratora danych lub podmiotu przetwarzającego dane w Unii (nawet jeżeli przetwarzanie ma miejsce w Stanach Zjednoczonych) lub (ii) osób, których dane dotyczą i które mieszkają w Unii, przez administratora danych lub podmiot przetwarzający dane z siedzibą poza Unią, w przypadku gdy działalność związana z przetwarzaniem dotyczy: a) oferowania towarów lub usług takim osobom, których dane dotyczą, w Unii, bez względu na to, czy wymagana jest płatność przez osobę, której dane dotyczą lub b) monitorowania ich zachowania, o ile do zachowania tego dochodzi w Unii. Zob. art. 3 ust. 1 i 2 rozporządzenia 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) (Dz.U. L 119 z 4.5.2016, s. 1).

(16) Ochrona zapewniana danym osobowym w ramach Tarczy Prywatności ma zastosowanie do wszystkich osób z UE, których dane dotyczą ([17]) i których dane osobowe zostały przekazane z Unii do podmiotów w USA, które przyjęły zasady w drodze samocertyfikacji w Departamencie Handlu.

(17) Zasady mają zastosowanie niezwłocznie po certyfikacji. Jedyny wyjątek odnosi się do zasady odpowiedzialności za wtórne przekazywanie, w przypadku gdy podmiot dokonujący samocertyfikacji w ramach Tarczy Prywatności łączą istniejące stosunki handlowe z osobami trzecimi. Jako że zapewnienie zgodności tych stosunków handlowych z regułami mającymi zastosowanie na mocy zasady odpowiedzialności za wtórne przekazywanie może nieco potrwać, podmiot będzie zobowiązany do zapewnienia tej zgodności jak najszybciej, a w żadnym razie nie później niż dziewięć miesięcy od daty certyfikacji (pod warunkiem że nastąpi to w ciągu pierwszych dwóch miesięcy następujących po dniu, w którym Tarcza Prywatności zacznie obowiązywać). W czasie tego okresu przejściowego podmiot musi stosować zasady powiadomienia i wyboru (umożliwiając tym samym wycofanie zgody przez osobę z UE, której dane dotyczą) oraz – w przypadku danych osobowych przekazywanych osobie trzeciej działającej w charakterze przedstawiciela – muszą upewnić się, że przedstawiciel zapewnia przynajmniej taki sam stopień ochrony, jaki jest wymagany w zasadach ([18]). Ten okres przejściowy zapewnia racjonalną i odpowiednią równowagę pomiędzy przestrzeganiem prawa podstawowego do ochrony danych i uzasadnionymi potrzebami przedsiębiorstw, aby miały one wystarczająco dużo czasu na dostosowanie się do nowych ram, w przypadku gdy jest to również uzależnione od ich stosunków handlowych z osobami trzecimi.

(18) Systemem będzie zarządzał i będzie go monitorował Departament Handlu na podstawie jego zobowiązań przedstawionych w oświadczeniach amerykańskiej sekretarz handlu (załącznik I do niniejszej decyzji). W kwestii egzekwowania zasad Federalna Komisja Handlu (FTC) i Departament Transportu złożyły oświadczenia zawarte w załącznikach IV i V do niniejszej decyzji.

2.1. *Zasady ochrony prywatności*

(19) Aby dokonać samocertyfikacji w ramach Tarczy Prywatności UE-USA, podmioty muszą zobowiązać się do przestrzegania zasad ([19]).

(20) Zgodnie z *zasadą powiadomienia* podmioty są zobowiązane przekazać osobom, których dane dotyczą, informacje na temat szeregu najważniejszych elementów związanych z przetwarzaniem ich danych osobowych (np. rodzaj gromadzonych danych, cel przetwarzania, prawo dostępu i wyboru, warunki wtórnego przekazywania i odpowiedzialności). Zastosowanie mają dodatkowe gwarancje, w szczególności zobowiązanie podmiotów do upubliczniania swoich strategii politycznych w obszarze ochrony prywatności (odzwierciedlających zasady) oraz do zamieszczania linków do strony internetowej Departamentu Handlu (wraz z dalszymi szczegółowymi informacjami na temat samocertyfikacji, praw osób, których dane dotyczą, oraz dostępnych mechanizmów ochrony prawnej), wykazu podmiotów uczestniczących w programie Tarczy Prywatności (o którym mowa w motywie 30), oraz strony internetowej odpowiedniego podmiotu świadczącego usługi w zakresie pozasądowego rozstrzygania sporów.

(21) Zgodnie z *zasadą integralności danych i celowości* dane osobowe muszą być ograniczone do tego, co jest istotne dla celu przetwarzania danych, muszą być zgodne ze swoim przeznaczeniem, dokładne, kompletne i aktualne. 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. Podmioty muszą zapewnić, aby dane osobowe były zgodne z ich przeznaczeniem, dokładne, kompletne i aktualne.

([17]) 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. Unijne prawodawstwo dotyczące ochrony danych, w tym dyrektywa 95/46/WE, jest objęte Porozumieniem EOG i zostało włączone do jego załącznika XI. Wspólny Komitet EOG musi podjąć decyzję o włączeniu niniejszej decyzji do Porozumienia EOG. Po rozpoczęciu stosowania niniejszej decyzji do Islandii, Liechtensteinu i Norwegii Tarcza Prywatności UE-USA obejmie również te trzy państwa, a odniesienia w pakiecie Tarczy Prywatności do UE i jej państw członkowskich rozumie się jako obejmujące Islandię, Liechtenstein i Norwegię.

([18]) Zob. załącznik II sekcja III pkt 6 lit. e).

([19]) Zasady szczególne zapewniające dodatkowe gwarancje mają zastosowanie do danych o zasobach ludzkich gromadzonych w kontekście zatrudnienia, jak określono w zasadzie uzupełniającej „Dane o zasobach ludzkich"zasad ochrony prywatności – (zob. załącznik II sekcja III pkt 9). Na przykład pracodawcy powinni uwzględniać preferencje pracowników w obszarze ochrony prywatności poprzez ograniczanie dostępu do danych osobowych, anonimizację pewnych danych lub przypisywanie kodów lub pseudonimów. Co istotniejsze, podmioty są zobowiązane do współpracy i przestrzegania porad unijnych organów ochrony danych, jeżeli chodzi o takie dane.

(22) Jeżeli nowy (zmieniony) cel jest znacząco różny od pierwotnego celu, ale nadal z nim zgodny, *zasada wyboru* zapewnia osobom, których dane dotyczą, prawo do sprzeciwu (wycofania zgody). *Zasada wyboru* nie zastępuje wyraźnego zakazu przetwarzania danych w sposób niezgodny z zasadami ([20]). Zasady szczególne zasadniczo umożliwiające wycofanie zgody na używanie danych osobowych „w dowolnym czasie" mają zastosowanie do marketingu bezpośredniego ([21]). W przypadku danych wrażliwych podmioty muszą zazwyczaj uzyskać wyraźną zgodę osoby, której dane dotyczą.

(23) Mimo to na podstawie *zasady integralności danych i celowości* dane osobowe można przechowywać w postaci identyfikującej osobę fizyczną lub umożliwiającej jej zidentyfikowanie (a zatem w postaci danych osobowych) wyłącznie dopóty, dopóki służy to celowi lub celom, dla których dane te pierwotnie zgromadzono lub następnie zatwierdzono. Obowiązek ten nie uniemożliwia organizacjom uczestniczącym w programie Tarczy Prywatności 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: archiwizacji w interesie publicznym, badań na potrzeby dziennikarstwa, literatury i sztuki, nauki i historii oraz analizy statystycznej. Dłuższe przechowywanie danych osobowych do jednego z tych celów będzie podlegać gwarancjom zapewnianym przez zasady.

(24) Zgodnie z *zasadą bezpieczeństwa* podmioty tworzące, przechowujące, wykorzystujące lub rozpowszechniające dane osobowe muszą podejmować „zasadne i odpowiednie" środki bezpieczeństwa, biorąc pod uwagę zagrożenia związane z przetwarzaniem danych osobowych i ich charakterem. W przypadku dalszego przetwarzania podmioty muszą zawrzeć umowę z podmiotem dokonującym dalszego przetwarzania, gwarantującą taki sam stopień ochrony jak stopień zapewniany przez zasady oraz muszą podjąć działania w celu zapewnienia prawidłowego wykonania tej umowy.

(25) Zgodnie z *zasadą dostępu* ([22]) osoby, których dane dotyczą, mają prawo, bez konieczności uzasadnienia i tylko po uiszczeniu niezawyżonej opłaty, uzyskać od podmiotu potwierdzenie, że przetwarza on ich dane osobowe oraz uzyskać te dane w rozsądnym terminie. Prawo to można ograniczyć jedynie w wyjątkowych okolicznościach; każda odmowa lub każde ograniczenie prawa dostępu musi być koniecznie i należycie uzasadnione, przy czym to na podmiocie spoczywa obowiązek wykazania spełnienia wspomnianych wymogów. Osoby, których dane dotyczą, muszą być w stanie skorygować, zmienić lub usunąć dane osobowe, w przypadku gdy są one nieprawidłowe lub przetwarzane z naruszeniem zasad. 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), w prawie amerykańskim zagwarantowano szczególne środki ochrony przed niekorzystnymi decyzjami ([23]). 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 niedokładnych informacji (i podważenia faktu powołania się na czynniki niezgodne z prawem) oraz prawo do ochrony prawnej. Przepisy te zapewniają środki ochrony w prawdopodobnej ograniczonej liczbie przypadków, w których sam podmiot uczestniczący w programie Tarczy Prywatności podjąłby automatyczne decyzje ([24]). Niemniej, mając na uwadze rosnące stosowanie zautomatyzowanego przetwarzania danych (w tym profilowania) jako podstawy podejmowania decyzji mających wpływ na osoby fizyczne w nowoczesnej gospodarce cyfrowej, jest to obszar, który wymaga ścisłego monitorowania. Aby ułatwić to monitorowanie, uzgodniono z organami USA, że dialog dotyczący zautomatyzowanego procesu decyzyjnego, w tym wymiana informacji na temat różnic i podobieństw między podejściem UE a USA w tym względzie, będzie stanowił część pierwszego corocznego przeglądu oraz, w stosownych przypadkach, kolejnych przeglądów.

([20]) Ma to zastosowanie do każdorazowego przekazywania danych w ramach Tarczy Prywatności, w tym jeżeli dotyczy to danych zgromadzonych w związku ze stosunkiem pracy. Chociaż amerykański podmiot samocertyfikowany może 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 tylko zgodnie z *zasadami powiadomienia* i *wyboru*. 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.

([21]) Zob. załącznik II sekcja III pkt 12.

([22]) Zob. również zasada uzupełniająca „Dostęp" (załącznik II sekcja III pkt 8).

([23]) 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.).

([24]) W kontekście przekazywania danych osobowych, które zgromadzono w UE, stosunek umowny w większości przypadków obowiązuje między osobą fizyczną (klientem) a unijnym administratorem danych, który musi przestrzegać unijnych zasad ochrony danych – w związku z tym wszelkie decyzje oparte na zautomatyzowanym przetwarzaniu danych zazwyczaj podejmuje unijny administrator danych. Obejmuje to scenariusze, w których za przetwarzanie odpowiada podmiot uczestniczący w programie Tarczy Prywatności działający w charakterze przedstawiciela w imieniu unijnego administratora danych.

(26) Zgodnie z *zasadą dotyczącą ochrony prawnej, egzekwowania prawa oraz odpowiedzialności* ([25]) uczestniczące podmioty muszą przedstawić solidne mechanizmy służące zapewnieniu zgodności z pozostałymi zasadami i środki ochrony prawnej dla osób z UE, których dane osobowe zostały przetworzone w sposób niezgodny z zasadami, w tym skuteczne środki odwoławcze. Jeżeli podmiot dobrowolnie zdecyduje się na samocertyfikację ([26]) w ramach Tarczy Prywatności UE-USA, ma obowiązek skutecznie przestrzegać zasad. Aby móc nadal korzystać z Tarczy Prywatności w celu otrzymywania danych osobowych z Unii, podmiot taki musi co roku ponownie dokonywać certyfikacji swojego uczestnictwa w przedmiotowych ramach. Podmioty muszą również podjąć środki w celu sprawdzenia ([27]), czy opublikowana przez nie 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 danej organizacji oraz przeprowadzanie okresowego, obiektywnego przeglądu zgodności lub zewnętrznych przeglądów zgodności, które mogą odbywać się w formie audytów lub kontroli wyrywkowych. Ponadto podmiot musi wdrożyć skuteczny mechanizm ochrony prawnej w celu rozpatrywania wszelkich skarg (zob. w tym kontekście także motyw 43) i musi podlegać uprawnieniom dochodzeniowym i wykonawczym FTC, Departamentu Transportu lub jakiegokolwiek innego amerykańskiego uprawnionego organu ustawowego, który skutecznie zapewni przestrzeganie zasad.

(27) Zasady szczególne mają zastosowanie do tzw. „wtórnego przekazywania", tj. przekazywania danych osobowych od podmiotu do administratora danych lub podmiotu przetwarzającego dane będących osobą trzecią, bez względu na to, czy ten administrator lub podmiot przetwarzający ma siedzibę w USA lub w państwie trzecim poza USA (i Unią). Celem tych zasad jest zapewnienie, by środki ochrony przyznane w przypadku danych osobowych osób z UE, których dane dotyczą, nie były naruszane i aby nie można było ich obejść poprzez przeniesienie ich na osoby trzecie. Ma to szczególne znaczenie w bardziej złożonych łańcuchach przetwarzania, które są typową cechą współczesnej gospodarki cyfrowej.

(28) Zgodnie z *zasadą odpowiedzialności za wtórne przekazywanie* ([28]) jakiekolwiek wtórne przekazywanie danych osobowych może się odbywać wyłącznie: (i) do ograniczonych i określonych celów; (ii) na podstawie umowy (lub porównywalnych uzgodnień wewnątrz grupy przedsiębiorstw ([29])) oraz (iii) tylko wtedy, gdy dana umowa zapewnia taki sam stopień ochrony jak stopień gwarantowany przez zasady i zawiera wymóg, zgodnie z którym zasady mogą zostać ograniczone wyłącznie w zakresie niezbędnym do osiągnięcia celów bezpieczeństwa narodowego, egzekwowania prawa i innych celów interesu publicznego ([30]). Zasadę tę należy interpretować w związku z *zasadą powiadomienia*, a w przypadku wtórnego przekazywania do administratora danych będącego osobą trzecią ([31]) – *zasadą wyboru*; zgodnie z tymi zasadami osoby, których dane dotyczą, muszą być (między innymi) informowane o rodzaju/tożsamości jakiegokolwiek odbiorcy będącego osobą trzecią do celu wtórnego przekazywania oraz o oferowanym im wyborze, a także mogą sprzeciwić się (wycofać zgodę) lub w przypadku danych wrażliwych udzielić „wyraźnej zgody" na wtórne przekazywanie. W świetle *zasady integralności danych i celowości* obowiązek zapewnienia takiego samego stopnia ochrony jak stopień zagwarantowany w zasadach oznacza, że osoba 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.

(29) Obowiązek zapewnienia takiego samego stopnia ochrony jak stopień wymagany w zasadach ma zastosowanie do wszystkich osób 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 osobą trzecią sam przekazuje te dane innemu odbiorcy będącemu osobą trzecią przykładowo do celów dalszego przetwarzania. We wszystkich przypadkach w umowie z odbiorcą będącym osobą trzecią należy przewidzieć, aby ten odbiorca powiadomił podmiot uczestniczący w programie Tarczy Prywatności, jeżeli ustali, że nie jest w stanie dłużej spełniać tego obowiązku. W przypadku dokonania takiego ustalenia przetwarzanie przez osobę trzecią ustanie lub konieczne będzie podjęcie innych zasadnych i właściwych środków, aby znaleźć rozwiązanie

([25]) Zob. również zasada uzupełniająca „Rozstrzyganie sporów i egzekwowanie" (załącznik II sekcja III pkt 11).
([26]) Zob. również zasada uzupełniająca „Samocertyfikacja" (załącznik II sekcja III pkt 6).
([27]) Zob. również zasada uzupełniająca „Kontrola" (załącznik II sekcja III pkt 7).
([28]) Zob. również zasada uzupełniająca „Obowiązkowe umowy dotyczące wtórnego przekazywania" (załącznik II sekcja III pkt 10).
([29]) Zob. zasada uzupełniająca „Obowiązkowe umowy dotyczące wtórnego przekazywania" (załącznik II 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 Tarczy Prywatności". Co więcej, przyjmując że amerykański podmiot samocertyfikowany pozostanie odpowiedzialny za zgodność z zasadami, będzie on miał silną motywację do stosowania instrumentów, które istotnie są skuteczne w praktyce.
([30]) Zob. załącznik II sekcja I pkt 5.
([31]) Osoby fizyczne nie będą miały prawa do wycofania zgody, jeżeli dane osobowe przekazuje się osobie trzeciej, która działa jako przedstawiciel upoważniony do wykonania czynności w imieniu i zgodnie z poleceniami 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 poleceń.

zaistniałej sytuacji ([32]). W przypadku problemów związanych ze zgodnością w łańcuchu (dalszego) przetwarzania podmiot uczestniczący w programie Tarczy Prywatności działający jako administrator danych osobowych będzie musiał udowodnić, że nie jest odpowiedzialny za zdarzenie powodujące szkodę ani w żaden inny sposób nie ponosi odpowiedzialności, jak określono w *zasadzie dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności*. Dodatkowe środki ochrony mają zastosowanie w przypadku wtórnego przekazywania danych przedstawicielowi będącemu osobą trzecią ([33]).

2.2. *Przejrzystość Tarczy Prywatności UE-USA, zarządzanie i nadzór nad nią*

(30) W ramach Tarczy Prywatności UE-USA przewidziano mechanizmy nadzoru i egzekwowania zasad w celu kontroli i zapewnienia przestrzegania zasad przez amerykańskie przedsiębiorstwa samocertyfikowane oraz usunięcie każdego przypadku nieprzestrzegania zasad. Wspomniane mechanizmy opisano w zasadach (załącznik II) i zobowiązaniach podjętych przez Departament Handlu (załącznik I), FTC (załącznik IV) i Departament Transportu (załącznik V).

(31) W celu zagwarantowania prawidłowego stosowania Tarczy Prywatności 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 tym celu Departament Handlu podjął się prowadzenia i publicznego udostępniania wykazu podmiotów, które przyjęły zasady w drodze samocertyfikacji oraz podlegają właściwości co najmniej jednego organu egzekwowania prawa wymienionego w załącznikach I i II do niniejszej decyzji („wykaz podmiotów uczestniczących w programie Tarczy Prywatności") ([34]). Departament Handlu będzie aktualizował wykaz na podstawie dokonywanych przez podmioty corocznych zgłoszeń dotyczących ponownej certyfikacji oraz gdy dany podmiot wycofa się lub zostanie usunięty z programu Tarczy Prywatności UE-USA. Departament będzie również prowadził i publicznie udostępniał oficjalny rejestr podmiotów, które usunięto z wykazu, za każdym razem przedstawiając powód takiego usunięcia. Ponadto umieści link do wykazu spraw dotyczących egzekwowania prawa prowadzonych przez FTC w związku z Tarczą Prywatności, który znajduje się na stronie internetowej FTC.

(32) Departament Handlu poda do wiadomości publicznej na specjalnej stronie internetowej zarówno wykaz podmiotów uczestniczących w programie Tarczy Prywatności, jak i zgłoszenia ponownej certyfikacji. Samocertyfikowane podmioty muszą z kolei udostępnić adres internetowy strony Departamentu, na której zamieszczono wykaz podmiotów uczestniczących w programie Tarczy Prywatności. Ponadto, jeżeli polityka ochrony prywatności jest dostępna na stronie internetowej podmiotu, musi znaleźć się w niej link do strony internetowej poświęconej Tarczy Prywatności oraz link do strony internetowej lub formularza skargi w ramach mechanizmu niezależnej ochrony prawnej, który umożliwia badanie nierozstrzygniętych skarg. Departament Handlu będzie systematycznie sprawdzał, w kontekście certyfikacji i ponownej certyfikacji podmiotu w celu objęcia ramami, czy jego polityka ochrony prywatności jest zgodna z zasadami.

(33) Podmioty, które uporczywie nie przestrzegały zasad, zostaną usunięte z wykazu organizacji uczestniczących w programie Tarczy Prywatności i będą zobowiązane do zwrócenia lub usunięcia danych osobowych, które otrzymały w ramach Tarczy Prywatności UE-USA. W innych przypadkach usunięcia, np. w przypadku dobrowolnego wycofania się z udziału w programie Tarczy Prywatności lub niedopełnienia obowiązku odnowienia certyfikacji, podmiot może zatrzymać takie dane, jeżeli co roku przedstawi Departamentowi Handlu 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). W takim przypadku podmiot musi wskazać osobę odpowiedzialną za kontakty w obrębie podmiotu, która odpowie na wszystkie zapytania związane z Tarczą Prywatności.

(34) Departament Handlu będzie monitorował podmioty, które nie są już członkami programu Tarczy Prywatności UE-USA, ponieważ dobrowolnie się wycofały albo wygasła ich certyfikacja, w celu sprawdzenia, czy zwróciły, usunęły lub zatrzymały ([35]) dane osobowe otrzymane wcześniej w ramach programu. Jeżeli podmioty zatrzymają

([32]) Sytuacja przedstawia się różnie w zależności od tego, czy osoba trzecia jest administratorem danych, czy też podmiotem przetwarzającym dane (przedstawicielem). W pierwszym scenariuszu w umowie z osobą trzecią należy przewidzieć, że podmiot przetwarzający zaprzestanie przetwarzania lub podejmie inne zasadne i właściwe środki, aby znaleźć rozwiązanie zaistniałej sytuacji. W drugim scenariuszu to podmiot uczestniczący w programie Tarczy Prywatności – jako podmiot kontrolujący przetwarzanie, którego polecenia wiążą przedstawiciela w jego działaniach – ma podjąć te środki.

([33]) W takim przypadku amerykański podmiot musi również podjąć zasadne i właściwe środki: (i) w celu zapewnienia skutecznego przetwarzania przez przedstawiciela danych osobowych przekazanych w sposób zgodny z obowiązkami tego podmiotu na mocy zasadach oraz (ii) w celu zaprzestania nieuprawnionego przetwarzania i naprawienia zaistniałej sytuacji, po otrzymaniu stosownego wniosku.

([34]) Informacje na temat zarządzania wykazem podmiotów uczestniczących w programie Tarczy Prywatności można znaleźć w załączniku I i II (sekcja I pkt 3, sekcja I pkt 4, sekcja III pkt 6 lit. d) i sekcja III pkt 11 lit. g)).

([35]) Zob. np. załącznik II sekcja I pkt 3, sekcja III pkt 6 lit. f) i sekcja III pkt 11 lit. g) ppkt (i).

te dane, będą zobowiązane do dalszego stosowania zasad w odniesieniu do tych danych. W przypadkach, w których Departament Handlu usunął podmioty z przedmiotowych ram ze względu na uporczywe nieprzestrzeganie zasad, dopilnuje on, aby wspomniane podmioty zwróciły lub usunęły dane osobowe, które otrzymały w przedmiotowych ramach.

(35) Podmiot, który z jakiegokolwiek powodu wycofuje się z programu Tarczy Prywatności UE-USA, musi usunąć wszelkie oświadczenia publiczne, które sugerują, że podmiot wciąż aktywnie uczestniczy w programie Tarczy Prywatności UE-USA lub jest uprawniony do przywilejów wynikających z Tarczy Prywatności, w szczególności wszelkich odniesień do Tarczy Prywatności UE-USA w jego opublikowanej polityce ochrony prywatności. Departament Handlu będzie wyszukiwał fałszywe oświadczenia dotyczące uczestnictwa w programie składane m. in. przez byłych członków ([36]) oraz będzie podejmował działania zaradcze. 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, Departament Transportu lub inny odpowiedni organ egzekwowania prawa Stanów Zjednoczonych; podanie fałszywych informacji Departamentowi Handlu stanowi podstawę wszczęcia postępowania na podstawie ustawy o fałszywych oświadczeniach (tytuł 18 § 1001 U.S.C.) ([37]).

(36) Departament Handlu będzie z urzędu monitorował wszelkie fałszywe oświadczenia dotyczące uczestnictwa w programie Tarczy Prywatności lub nieprawidłowego korzystania ze znaku certyfikacyjnego Tarczy Prywatności, zaś organy ochrony danych mogą skierować podmiot do wyznaczonej osoby odpowiedzialnej za kontakty w Departamencie celem przeprowadzenia przeglądu. Jeżeli podmiot wycofa się z programu Tarczy Prywatności UE-USA, nie dokona ponownej certyfikacji lub zostanie usunięty z wykazu podmiotów uczestniczących w programie Tarczy Prywatności, Departament Handlu będzie na bieżąco sprawdzał, czy dany podmiot usunął z opublikowanej przez siebie polityki prywatności wszelkie odniesienia do Tarczy Prywatności, które sugerowałyby aktywny udział, przy czym jeżeli nadal składa fałszywe oświadczenia, Departament Handlu przekaże sprawę FTC, Departamentowi Transportu lub innym właściwym organom w celu ewentualnego przeprowadzenia działań służących egzekwowaniu przepisów prawnych. Wyśle również kwestionariusze do podmiotów, których samocertyfikacje wygasły lub które dobrowolnie wycofały się z programu Tarczy Prywatności UE-USA, aby zweryfikować, czy dany podmiot ponownie zacznie stosować jej zasady, zaprzestanie ich stosowania lub nadal będzie je stosować do danych osobowych, które otrzymał w czasie, gdy uczestniczył w programie Tarczy Prywatności UE-USA, a jeżeli dane osobowe zostaną zatrzymane, zweryfikuje, kto w ramach podmiotu będzie pełnił funkcję osoby odpowiedzialnej za bieżące kontakty w przypadku zapytań związanych z Tarczą Prywatności.

(37) Departament Handlu będzie na bieżąco prowadził z urzędu przeglądy zgodności ([38]) samocertyfikowanych podmiotów, w tym poprzez wysyłanie szczegółowych kwestionariuszy. Departament będzie również systematycznie przeprowadzał przeglądy, ilekroć otrzyma konkretną (poważną) skargę, podmiot nie zareaguje w zadowalający sposób na jego zapytania lub będą istniały przekonujące dowody na to, że podmiot może nie przestrzegać zasad. W stosownych przypadkach Departament Handlu zasięgnie również opinii organów ochrony danych w kwestii tego rodzaju przeglądów zgodności.

2.3. *Mechanizmy ochrony prawnej, rozpatrywanie skarg i egzekwowanie prawa*

(38) Tarcza Prywatności 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 UE, których dane dotyczą, skarg na nieprzestrzeganie zasad przez samocertyfikowane przedsiębiorstwa amerykańskie, a także możliwości rozpatrzenia tych skarg, w razie potrzeby w drodze decyzji zapewniającej skuteczny środek ochrony prawnej.

(39) W ramach podejmowanych we własnym zakresie działań w obszarze samocertyfikacji podmioty muszą spełnić wymogi przewidziane w zasadzie dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności, zapewniając możliwość skorzystania ze skutecznych i łatwo dostępnych mechanizmów niezależnej ochrony prawnej umożliwiających badanie i szybkie rozstrzyganie skarg oraz sporów poszczególnych osób fizycznych bez konieczności ponoszenia przez nie jakichkolwiek kosztów.

(40) Podmioty mogą wybrać mechanizmy niezależnej ochrony prawnej w Unii albo w Stanach Zjednoczonych. Mogą również podjąć dobrowolne zobowiązanie do współpracy z unijnymi organami ochrony danych. Podmioty nie

([36]) Zob. załącznik I sekcja „Wyszukiwanie fałszywych oświadczeń dotyczących uczestnictwa w programie i podejmowanie działań zaradczych".
([37]) Zob. załącznik II sekcja III pkt 6 lit. h) i sekcja III pkt 11 lit. f).
([38]) Zob. załącznik I.

dysponują jednak swobodą uznania w przypadku, gdy przetwarzają dane o zasobach ludzkich, ponieważ w takiej sytuacji współpraca z organami ochrony danych jest obowiązkowa. Wśród innych rozwiązań alternatywnych należy wymienić niezależne pozasądowe rozstrzyganie sporów lub *programy prywatności* opracowane przez podmioty sektora prywatnego, w które wbudowano zasady ochrony prywatności. Wspomniane programy muszą obejmować skuteczne mechanizmy egzekwowania prawa zgodne z wymogami zasady dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności. Podmioty są zobowiązane do rozwiązania wszelkich problemów związanych z nieprzestrzeganiem zasad. Podmioty muszą również wskazać, że podlegają uprawnieniom dochodzeniowym i wykonawczym FTC, Departamentu Transportu lub jakiegokolwiek innego amerykańskiego uprawnionego organu ustawowego.

(41) Tym samym ramy Tarczy Prywatności zapewniają osobom, których dane dotyczą, szereg środków służących egzekwowaniu przysługujących im praw, składaniu skarg na nieprzestrzeganie zasad przez samocertyfikowane przedsiębiorstwa amerykańskie, a także uzyskanie rozstrzygnięcia takich skarg, w razie konieczności 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 lub FTC.

(42) 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 panelu ds. Tarczy Prywatności (załącznik 1 do załącznika II 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 ochrony prawnej lub wszystkich tych mechanizmów jednocześnie i nie są zobowiązane do ograniczenia się wyłącznie do jednego mechanizmu ani do korzystania z nich w określonym porządku. Istnieje jednak pewien porządek logiczny, którego osoby fizyczne powinny się trzymać, jak przedstawiono poniżej.

(43) Po pierwsze, osoby z UE, których dane dotyczą, mogą zgłaszać roszczenia dotyczące nieprzestrzegania zasad za pośrednictwem osób odpowiedzialnych za bezpośrednie kontakty w *amerykańskim przedsiębiorstwie, które dokonało samocertyfikacji*. Aby ułatwić rozstrzygnięcie sporu, podmiot musi wdrożyć skuteczny mechanizm ochrony prawnej 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 niezależnych mechanizmów rozpatrywania skarg.

(44) Po otrzymaniu skargi złożonej przez osobę fizyczną bezpośrednio lub za pośrednictwem Departamentu Handlu w następstwie zgłoszenia przez organ ochrony danych podmiot musi, w terminie 45 dni, udzielić odpowiedzi osobie z UE, której dane dotyczą. Odpowiedź ta musi zawierać ocenę zasadności skargi oraz informacje na temat tego, w jaki sposób podmiot rozwiąże problem. Podobnie podmioty są zobowiązane do bezzwłocznego reagowania na zapytania i inne wnioski o udzielenie informacji złożone przez Departament Handlu lub organ ochrony danych ([39]) (jeżeli podmiot zobowiązał się do współpracy z organami ochrony danych) dotyczące przestrzegania przez nie zasad. Podmioty muszą zachowywać swoje dokumenty dotyczące wdrażania polityki ochrony prywatności oraz udostępniać je na żądanie mechanizmowi niezależnej ochrony prawnej lub FTC (lub innemu amerykańskiemu organowi właściwemu do badania nieuczciwych i wprowadzających w błąd praktyk) w kontekście dochodzenia lub skargi dotyczącej nieprzestrzegania zasad.

(45) 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. 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. Wyznaczone przez podmiot niezależne organy ds. rozpatrywania sporów będą zobowiązane do umieszczania na swoich ogólnodostępnych stronach internetowych stosownych informacji na temat Tarczy Prywatności UE-USA i usług, jakie świadczą w ramach tego programu. Co roku muszą publikować sprawozdanie roczne zawierające zagregowane dane statystyczne dotyczące takich usług ([40]).

([39]) Tj. organ zajmujący się zapytaniami wyznaczony przez grupę organów ochrony danych przewidzianą w ramach zasady uzupełniającej dotyczącej „Roli organów ochrony danych" (załącznik II, sekcja III.5).

([40]) Sprawozdanie roczne musi zawierać następujące informacje: 1) łączną liczbę skarg związanych z Tarczą Prywatności 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.

(46) W ramach swoich procedur kontroli zgodności Departament Handlu sprawdzi, czy amerykańskie przedsiębiorstwa samocertyfikowane faktycznie zarejestrowały się, jak twierdzą, w mechanizmach niezależnej ochrony prawnej. Zarówno podmioty, jak i odpowiedzialne mechanizmy niezależnej ochrony prawnej są zobowiązane do bezzwłocznego reagowania na złożone przez Departament Handlu zapytania i wnioski o informacje dotyczące Tarczy Prywatności.

(47) W przypadkach, w których podmiot nie zastosuje się do orzeczenia organu ds. rozstrzygania sporów lub organu samoregulacyjnego, ten ostatni musi zgłosić taki przypadek Departamentowi Handlu i FTC (lub innemu amerykańskiemu organowi właściwemu do badania nieuczciwych i wprowadzających w błąd praktyk) lub właściwemu sądowi ([41]). 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 zostanie uznana za uporczywe nieprzestrzeganie zasad, w rezultacie czego Departament Handlu – po przekazaniu podmiotowi nieprzestrzegającemu zasad stosownego powiadomienia z trzydziestodniowym wyprzedzeniem, aby zapewnić mu możliwość ustosunkowania się do zarzutów – skreśli ten podmiot z wykazu ([42]). Jeżeli po usunięciu podmiotu z wykazu w dalszym ciągu będzie on deklarował zgodność z zasadami Tarczy Prywatności, departament przekaże sprawę do rozpoznania FTC lub innemu organowi egzekwowania prawa ([43]).

(48) Po trzecie, osoby fizyczne mogą również wnosić swoje skargi do krajowego *organu ochrony danych*. 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. 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.

(49) Porady organów ochrony danych będą udzielane za pośrednictwem nieformalnej grupy organów ochrony danych ustanowionej na poziomie Unii ([44]), co pomoże zapewnić rozpatrywanie poszczególnych spraw w skoordynowany i spójny sposób. Porady zostaną udzielone dopiero wówczas, gdy obie strony sporu miały należytą możliwość wypowiedzenia się i przedstawienia wszystkich dowodów zgodnie z własnym uznaniem. Panel przekaże porady tak szybko, jak stanowi wymóg należytej procedury, i co do zasady w ciągu 60 dni po otrzymaniu skargi. Jeżeli podmiot nie zastosuje się do porad w ciągu 25 dni od ich otrzymania i nie poda zadowalającego usprawiedliwienia takiego opóźnienia, panel zawiadomi go o swoim zamiarze przekazania sprawy FTC (lub innemu właściwemu amerykańskiemu organowi egzekwowania prawa) lub o zamiarze stwierdzenia poważnego naruszenia zobowiązania do współpracy. W pierwszym przypadku może to prowadzić do podjęcia działania służącego egzekwowaniu na podstawie sekcji 5 ustawy o FTC (lub podobnej ustawy). W drugim przypadku panel poinformuje Departament Handlu, 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 uczestniczących w programie Tarczy Prywatności.

(50) 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.

(51) 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 Departament Handlu albo FTC. Aby ułatwić i pogłębić współpracę w kwestiach dotyczących skarg wnoszonych przez osoby fizyczne i nieprzestrzegania zasad przez podmioty uczestniczące w programie Tarczy Prywatności, Departament Handlu 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 ([45]). Podobnie FTC zobowiązało się do ustanowienia specjalnej osoby odpowiedzialnej za kontakty ([46]) oraz do zapewniania organom ochrony danych wsparcia w prowadzeniu dochodzeń zgodnie z amerykańską ustawą o bezpieczeństwie w sieci ([47]).

([41]) Zob. załącznik II sekcja III pkt 11 lit. e).
([42]) Zob. załącznik II sekcja III pkt 11 lit. g), w szczególności ppkt (ii) i (iii).
([43]) Zob. załącznik I sekcja „Wyszukiwanie fałszywych oświadczeń dotyczących uczestnictwa w programie i podejmowanie działań zaradczych".
([44]) Organy ochrony danych powinny przyjąć regulamin nieformalnego panelu organów ochrony danych w oparciu o ich zdolność do organizacji pracy i wzajemnej współpracy.
([45]) Zob. załącznik I sekcje dotyczące „Pogłębiania współpracy z organami ochrony danych" i „Ułatwienia rozstrzygania skarg na nieprzestrzeganie zasad" oraz załącznik II sekcja II pkt 7 lit. e).
([46]) Zob. załącznik IV, s. 6.
([47]) Tamże.

(52) Po czwarte, *Departament Handlu* zobowiązał się do przyjmowania i rozpatrywania skarg oraz dokładania wszelkich starań w celu rozstrzygnięcia skarg dotyczących nieprzestrzegania zasad przez podmioty. W tym celu Departament Handlu zapewnia organom ochrony danych szczegółowe procedury przekazywania skarg osobie wyznaczonej do kontaktów, śledzenia ich oraz kontaktowania się z przedsiębiorstwami w celu ułatwienia procesu rozstrzygania skarg. Aby przyspieszyć proces rozpatrywania skarg osób fizycznych, osoba wyznaczona do kontaktów będzie współpracować bezpośrednio z odpowiednim organem ochrony danych w kwestiach przestrzegania zasad, a w szczególności będzie przekazywać mu aktualne informacje na temat statusu skarg w okresie nie dłuższym niż 90 dni od daty zgłoszenia. Dzięki temu osoby, których dane dotyczą, będą mogły składać skargi dotyczące nieprzestrzegania zasad przez amerykańskie przedsiębiorstwa samocertyfikowane bezpośrednio ich krajowemu organowi ochrony danych, który następnie przekaże je Departamentowi Handlu jako amerykańskiemu organowi zarządzającemu Tarczą Prywatności UE-USA. Departament Handlu zobowiązał się również do opracowania, w ramach rocznego przeglądu funkcjonowania Tarczy Prywatności UE-USA, sprawozdania zawierającego zbiorczą analizę skarg otrzymanych każdego roku ([48]).

(53) Jeżeli, na podstawie kontroli przeprowadzonej z urzędu, skarg lub innych informacji, Departament Handlu stwierdzi, że podmiot uporczywie nie przestrzega zasad ochrony prywatności, wówczas usunie taki podmiot z wykazu podmiotów uczestniczących w programie Tarczy Prywatności. 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.

(54) Po piąte, podmiot uczestniczący w programie Tarczy Prywatności musi respektować uprawnienia organów amerykańskich, w szczególności *Federalnej Komisji Handlu* ([49]), w zakresie prowadzenia dochodzeń i egzekwowania prawa, co skutecznie zapewni przestrzeganie zasad przez ten podmiot. FTC będzie priorytetowo traktowało zgłoszenia dotyczące nieprzestrzegania zasad ochrony prywatności otrzymane od niezależnego organu ds. rozstrzygania sporów lub organu samoregulacyjnego, Departamentu Handlu i organów ochrony danych (działających z własnej inicjatywy lub na podstawie skarg), aby ustalić, czy doszło do naruszenia przepisów sekcji 5 ustawy o FTC ([50]). 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 będzie przyjmowało skargi bezpośrednio od osób fizycznych i z własnej inicjatywy będzie przeprowadzić dochodzenia dotyczące Tarczy Prywatności, w szczególności w ramach szerzej zakrojonych dochodzeń dotyczących kwestii prywatności.

(55) FTC może wyegzekwować przestrzeganie zasad za pomocą zarządzeń administracyjnych („ugód") i systematycznie będzie monitorować stosowanie się do takich zarządzeń. Jeżeli podmioty nie przestrzegają zarządzeń, FTC może skierować sprawę do właściwego sądu w celu nałożenia sankcji cywilnych i innych środków ochrony prawnej, w tym za wszelkie szkody spowodowane niezgodnym z prawem postępowaniem. FTC może również bezpośrednio wystąpić do sądu federalnego o nałożenie wstępnego lub stałego nakazu lub zakazu sądowego lub innych środków ochrony prawnej. Każda ugoda wystawiona na rzecz podmiotu uczestniczącego w programie Tarczy Prywatności będzie zawierała przepisy dotyczące samozgłaszania ([51]), a podmioty będą zobowiązane do podawania do wiadomości publicznej wszelkich istotnych i związanych z Tarczą Prywatności sekcji wszelkich przedłożonych FTC sprawozdań dotyczących przestrzegania zasad lub sprawozdań z oceny. Ponadto FTC będzie prowadziło internetowy wykaz przedsiębiorstw podlegających orzeczeniom FTC lub sądu w sprawach dotyczących Tarczy Prywatności.

(56) 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 UE, której dane dotyczą, może poddać sprawę pod arbitraż *panelu ds. Tarczy Prywatności*. Podmioty muszą poinformować osoby fizyczne o możliwości wystąpienia – po spełnieniu określonych warunków – o arbitraż i są zobowiązane do udzielenia odpowiedzi, w przypadku gdy dana osoba fizyczna zdecyduje się skorzystać z tej możliwości, przekazując powiadomienie stosownemu podmiotowi ([52]).

([48]) Zob. załącznik I sekcja „Ułatwienia rozstrzygania skarg na nieprzestrzeganie zasad".

([49]) Podmiot uczestniczący w programie Tarczy Prywatności 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. Brak zgodności można wyegzekwować 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.

([50]) 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.

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

([52]) Zob. załącznik II sekcja II pkt 1 ppkt (xi) i sekcja III pkt 7 lit. c).

(57) Wspomniany panel arbitrażowy będzie się składał z co najmniej 20 arbitrów wyznaczonych przez Departament Handlu 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 wybiorą z tej grupy panel złożony z jednego arbitra lub trzech ([53]) arbitrów. Postępowanie będzie prowadzone zgodnie ze standardowymi zasadami arbitrażu uzgodnionymi przez Departament Handlu i Komisję. Zasady te będą uzupełniały obowiązujące ramy, w których przewidziano szereg elementów przyczyniających się do zwiększenia dostępności tego mechanizmu dla osób z UE, 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 UE, 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 z reguły ([54]) zapewnione nieodpłatnie; (iv) chociaż każda ze stron musi ponieść własne koszty zastępstwa procesowego, jeżeli jest reprezentowana przed panelem przez pełnomocnika, Departament Handlu ustanowi fundusz zasilany rocznymi składkami wpłacanymi przez podmioty uczestniczące w programie Tarczy Prywatności, który pokryje kwalifikujące się koszty procedury arbitrażowej, do kwot maksymalnych, które zostaną ustalone przez organy amerykańskie w porozumieniu z Komisją.

(58) Panel ds. Tarczy Prywatności będzie uprawniony do przyznania „niepieniężnego godziwego zadośćuczynienia danej osobie fizycznej" ([55]), które jest niezbędne do usunięcia niezgodności z zasadami. Chociaż panel, podejmując decyzję, uwzględni inne środki ochrony prawnej uzyskane już w ramach innych mechanizmów Tarczy Prywatności, osoby fizyczne mogą nadal wnieść o arbitraż, jeżeli uznają te inne środki ochrony prawnej za niewystarczające. Pozwoli to osobom z UE, których dane dotyczą, wszczęcie arbitrażu we wszystkich przypadkach, gdy działanie lub bezczynność 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 amerykańskiego przedsiębiorstwa samocertyfikowanego, 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 przedsiębiorstwo nie wywiąże się ze spoczywających na nim zobowiązań.

(59) 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 poszczególnych stanów USA, w których przewidziano środki ochrony prawnej na mocy prawa deliktów oraz w przypadkach podania fałszywych informacji w celu wprowadzenia w błąd, podejmowania nieuczciwych lub oszukańczych działań lub stosowania nieuczciwych lub oszukańczych praktyk lub naruszenia umowy.

(60) Ponadto, jeżeli organ ochrony danych, po otrzymaniu skargi złożonej przez osobę z UE, której dane dotyczą, uzna, że dane osobowe osoby fizycznej przekazywano podmiotowi ze Stanów Zjednoczonych z naruszeniem przepisów UE dotyczących ochrony danych, w tym jeżeli podmiot eksportujący dane z UE ma podstawy, by przypuszczać, że odnośny podmiot nie przestrzega przedmiotowych zasad, może skorzystać ze swoich uprawnień również względem podmiotu przekazującego dane oraz, w razie potrzeby, zarządzić zawieszenie przekazywania danych.

(61) W świetle informacji przedstawionych w niniejszej sekcji Komisja stwierdza, że zasady opublikowane przez Departament Handlu Stanów Zjednoczonych jako takie zapewniają stopień ochrony danych osobowych, który jest zasadniczo równoważny stopniowi ochrony gwarantowanemu zgodnie z podstawowymi zasadami ustanowionymi w dyrektywie 95/46/WE.

(62) Ponadto ustanowienie zobowiązań w zakresie przejrzystości, zarządzanie Tarczą Prywatności oraz przeprowadzanie przeglądu zgodności z zasadami przez Departament Handlu gwarantuje skuteczne stosowanie zasad.

(63) Ponadto Komisja stwierdza, że mechanizmy nadzoru, mechanizmy odwoławcze i mechanizmy egzekwowania prawa przewidziane w Tarczy Prywatności – rozumiane jako całość – zapewniają możliwość identyfikowania przypadków naruszenia zasad przez podmioty uczestniczące w programie Tarczy Prywatności i nakładania za nie kar w praktyce i oferują osobom, których dane dotyczą, możliwość skorzystania ze środków ochrony prawnej w celu uzyskania dostępu do danych na ich temat oraz – ostatecznie – skorygowania lub usunięcia takich danych.

([53]) Liczba arbitrów w danym panelu zostanie uzgodniona między stronami.

([54]) Panel może jednak uznać, że w okolicznościach konkretnego arbitrażu pokrycie kosztów doprowadziłoby do nieuzasadnionych lub nieproporcjonalnych kosztów.

([55]) Osoby fizyczne nie mogą dochodzić odszkodowania w postępowaniu arbitrażowym, ale też wszczęcie postępowania arbitrażowego nie uniemożliwia dochodzenia odszkodowania przed amerykańskimi sądami powszechnymi.

3. DOSTĘP DO DANYCH OSOBOWYCH PRZEKAZYWANYCH PRZEZ AMERYKAŃSKIE ORGANY PUBLICZNE W RAMACH TARCZY PRYWATNOŚCI UE-USA I KORZYSTANIE Z TYCH DANYCH

(64) Zgodnie z załącznikiem II sekcja I pkt 5 przestrzeganie zasad ogranicza się do zakresu, w jakim jest to konieczne do spełnienia wymogów bezpieczeństwa narodowego, interesu publicznego lub egzekwowania prawa.

(65) Komisja oceniła przewidziane w prawie amerykańskim ograniczenia i gwarancje w zakresie dostępu do danych osobowych przekazywanych przez amerykańskie organy publiczne w ramach Tarczy Prywatności UE-USA i korzystania z tych danych do celów bezpieczeństwa narodowego, egzekwowania prawa i innych celów leżących w interesie publicznym. Ponadto rząd Stanów Zjednoczonych – za pośrednictwem Urzędu Dyrektora Krajowych Służb Wywiadowczych ([56]) – przekazał Komisji szczegółowe oświadczenia i zobowiązania, które zawarto w załączniku VI do niniejszej decyzji. Na mocy pisma podpisanego przez sekretarza stanu i dołączonego jako załącznik III do niniejszej decyzji rząd Stanów Zjednoczonych zobowiązał się również do utworzenia nowego mechanizmu nadzoru nad przypadkami ingerencji ze względu na bezpieczeństwo narodowe, tj. do powołania Rzecznika ds. Tarczy Prywatności, który jest organem niezależnym od Wspólnoty Wywiadowczej. W oświadczeniu Departamentu Sprawiedliwości Stanów Zjednoczonych zawartym w załączniku VII do niniejszej decyzji opisano ograniczenia i gwarancje mające zastosowanie do dostępu organów publicznych do danych w celu egzekwowania prawa i w innych celach leżących w interesie publicznym oraz korzystania z tych danych przez organy publiczne. Aby zwiększyć przejrzystości i odzwierciedlić prawny charakter tych zobowiązań, każdy z dokumentów zamieszczonych w wykazie i załączonych do niniejszej decyzji zostanie opublikowany w amerykańskim Rejestrze Federalnym.

(66) Poniżej bardziej szczegółowo opisano ustalenia Komisji w kwestii ograniczeń dostępu do danych osobowych przekazywanych z Unii Europejskiej do Stanów Zjednoczonych przez amerykańskie organy publiczne i ograniczeń w zakresie korzystania z tych danych, a także ustalenia w kwestii istnienia skutecznych środków ochrony prawnej w tym zakresie.

3.1. *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*

(67) Przeprowadzona przez Komisję analiza wykazała, że w prawie amerykańskim ustanowiono szereg ograniczeń dostępu do danych osobowych przekazywanych w ramach Tarczy Prywatności UE-USA do celów związanych z bezpieczeństwem narodowym oraz ograniczenia w zakresie korzystania z tych danych, a także mechanizmy nadzoru i ochrony prawnej, które w dostatecznym stopniu gwarantują, że dane te będą należycie chronione przed bezprawną ingerencją i ryzykiem dopuszczania się wobec nich nadużyć ([57]). Jak opisano poniżej, wspomniane ramy prawne zostały istotnie wzmocnione od 2013 r., kiedy Komisja opublikowała swoje dwa komunikaty (zob. motyw 7).

3.1.1. Ograniczenia

(68) Zgodnie z konstytucją Stanów Zjednoczonych odpowiedzialność za zapewnienie bezpieczeństwa narodowego spoczywa na Prezydencie, który pełni funkcję Naczelnego Wodza i Zwierzchnika Sił Zbrojnych i który jest uprawniony do kształtowania polityki zagranicznej Stanów Zjednoczonych w obszarze wywiadu zagranicznego ([58]). Choć Kongres posiada kompetencje do nakładania ograniczeń i wielokrotnie korzystał z tego uprawnienia, Prezydent jest uprawniony do kierowania działalnością Wspólnoty Wywiadowczej Stanów Zjednoczonych w tym obszarze, w szczególności za pomocą rozporządzeń wykonawczych lub dyrektyw Prezydenta. Dotyczy to oczywiście również tych obszarów, w odniesieniu do których Kongres nie opublikował żadnych wytycznych. Obecnie można wskazać dwa kluczowe instrumenty prawne w tym obszarze: rozporządzenie wykonawcze 12333 („rozporządzenie wykonawcze 12333") ([59]) i dyrektywę polityczną Prezydenta nr 28.

([56]) Dyrektor Krajowych Służb Wywiadowczych stoi na czele Wspólnoty Wywiadowczej i pełni funkcję głównego doradcy Prezydenta oraz Rady Bezpieczeństwa Narodowego. Zob. ustawa o reformie służby wywiadowczej i zwalczaniu terroryzmu z 2004 r., Zbiór ustaw publicznych nr 108–458 z dnia 17 grudnia 2004 r. Urząd Dyrektora Krajowych Służb Wywiadowczych ustanawia m.in. wymogi w zakresie podziału zadań oraz gromadzenia, analizowania, opracowywania i rozpowszechniania krajowych danych wywiadowczych przez Wspólnotę Wywiadowczą, a także zarządzania działaniami Wspólnoty Wywiadowczej w tym zakresie i nadawania kierunku tym działaniom, a także opracowuje wytyczne dotyczące sposobu oceniania, wykorzystywania i udostępniania informacji lub danych wywiadowczych. Zob. sekcja 1.3 lit. a) i b) rozporządzenia wykonawczego 12333.

([57]) Zob. wyrok w sprawie Schrems, pkt 91.

([58]) Artykuł II konstytucji Stanów Zjednoczonych. Zob. również wstęp do dyrektywy politycznej Prezydenta nr 28.

([59]) Rozporządzenie wykonawcze 12333: Działalność wywiadowcza Stanów Zjednoczonych, Rejestr Federalny t. 40, nr 235 (8 grudnia 1981 r.). W zakresie, w jakim rozporządzenie wykonawcze jest publicznie dostępne, określono w nim cele, kierunki prac, zadania i obowiązki amerykańskich agencji wywiadowczych (a także funkcje określonych jednostek Wspólnoty Wywiadowczej), a także ustanowiono ogólne parametry regulujące działalność agencji wywiadowczych (w szczególności ustanowiono obowiązek podawania przepisów proceduralnych do wiadomości publicznej). Zgodnie z sekcją 3.2 rozporządzenia wykonawczego 12333 Prezydent, korzystając ze wsparcia Rady Bezpieczeństwa Narodowego i Dyrektora Krajowych Służb Wywiadowczych, wydaje dyrektywy, ustanawia procedury i publikuje wytyczne konieczne do wykonania tego rozporządzenia.

(69) W dyrektywie politycznej Prezydenta nr 28 wydanej w dniu 17 stycznia 2014 r. na operacje w obszarze „rozpoznania radioelektronicznego" nałożono szereg ograniczeń ([60]). Dyrektywa Prezydenta jest wiążąca dla amerykańskich organów wywiadowczych ([61]) i pozostaje w mocy po zmianie administracji Stanów Zjednoczonych ([62]). Dyrektywa polityczna Prezydenta nr 28 ma szczególne znaczenie dla osób niebędących obywatelami ani rezydentami amerykańskimi, uwzględniając osoby z UE, których dane dotyczą. Dyrektywa ta stanowi m.in., że:

a) dane pochodzące z rozpoznania radioelektronicznego muszą być gromadzone zgodnie z przepisami ustawy lub zgodnie z upoważnieniem wydanym przez Prezydenta, a działania w obszarze rozpoznania radioelektronicznego muszą być podejmowane zgodnie z konstytucją Stanów Zjednoczonych (w szczególności zgodnie z czwartą poprawką) i zgodnie z prawem amerykańskim;

b) wszystkie osoby powinny być traktowane z godnością i szacunkiem, niezależnie od ich narodowości lub miejsca zamieszkania;

c) wszystkie osoby posiadają uzasadniony interes w dążeniu do zapewnienia poszanowania ich prywatności przy przetwarzaniu dotyczących ich danych osobowych;

d) kwestie związane z prywatnością i wolnościami obywatelskimi mają kluczowe znaczenie w kontekście planowania działań Stanów Zjednoczonych w obszarze rozpoznania radioelektronicznego;

e) dlatego też przy podejmowaniu działań w obszarze rozpoznania radioelektronicznego organy amerykańskie muszą uwzględnić odpowiednie gwarancje w zakresie ochrony danych osobowych wszystkich osób fizycznych, niezależnie od ich narodowości lub miejsca zamieszkania.

(70) Dyrektywa polityczna Prezydenta nr 28 stanowi, że dane pochodzące z rozpoznania radioelektronicznego można gromadzić wyłącznie w celach związanych z prowadzeniem działalności w obszarze wywiadu lub kontrwywiadu zagranicznego, aby wesprzeć organy krajowe i organy wchodzące w skład departamentów w realizacji powierzonych im zadań i że nie można ich gromadzić w żadnych innych celach (np. w celu przyznania korzyści konkurencyjnej przedsiębiorstwom amerykańskim). W tym kontekście Urząd Dyrektora Krajowych Służb Wywiadowczych wyjaśnił, że jednostki Wspólnoty Wywiadowczej „powinny ustanowić wymóg, aby w miarę możliwości koncentrować się na konkretnych celach lub zagadnieniach związanych z wywiadem zagranicznym, stosując obowiązujące wyróżniki (np. określone urządzenia, terminy umożliwiające selekcję i kryteria identyfikujące)" ([63]). Ponadto w oświadczeniach zagwarantowano, że podmiotami odpowiedzialnymi za podjęcie decyzji w kwestii gromadzenia danych wywiadowczych nie będą poszczególni przedstawiciele służb wywiadowczych – kwestie te zostaną uregulowane w politykach i procedurach stosowanych przez różne jednostki (agencje) Wspólnoty Wywiadowczej Stanów Zjednoczonych, które agencje te są zobowiązane przyjąć w celu wdrożenia dyrektywy politycznej Prezydenta nr 28 ([64]). W związku z powyższym proces analizowania i ustanawiania odpowiednich selektorów odbywa się w kontekście ogólnych „ram amerykańskich priorytetów wywiadowczych", które zapewniają wyznaczanie priorytetów wywiadowczych przez decydentów wysokiego szczebla i poddawanie ich regularnym przeglądom, aby w odpowiedni sposób odnosiły się do bieżących zagrożeń dla bezpieczeństwa narodowego i uwzględniały potencjalne czynniki ryzyka, w tym czynniki ryzyka stwarzające zagrożenie dla prywatności ([65]). Na tej podstawie personel agencji wyszukuje i identyfikuje konkretne terminy umożliwiające selekcję, co do których oczekuje się, że pomogą zgromadzić zagraniczne dane wywiadowcze stosownie do priorytetów ([66]). Terminy umożliwiające selekcję, czyli „selektory" muszą być regularnie ocenianie, aby ustalić, czy w dalszym ciągu dostarczają wartościowych danych wywiadowczych zgodnie z priorytetami ([67]).

([60]) Zgodnie z rozporządzeniem wykonawczym 12333 Dyrektor Agencji Bezpieczeństwa Narodowego pełni funkcję Kierownika Merytorycznego ds. Rozpoznania Radioelektronicznego i zarządza działalnością jednolitej organizacji ds. działań w obszarze rozpoznania radioelektronicznego.

([61]) Definicję terminu „Wspólnota Wywiadowcza" przedstawiono w sekcji 3.5 lit. h) rozporządzenia wykonawczego 12333 i w sekcji 1 dyrektywy politycznej Prezydenta nr 28.

([62]) Zob. memorandum Biura Doradztwa Prawnego w Departamencie Sprawiedliwości adresowane do prezydenta Clintona z dnia 29 stycznia 2000 r. Zgodnie z opinią prawną przedstawioną w tej opinii prawnej dyrektywy Prezydenta „wywierają taki sam materialny skutek prawny co rozporządzenie wykonawcze".

([63]) Oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 3.

([64]) Zob. sekcja 4 lit. b) i c) dyrektywy politycznej Prezydenta nr 28. Zgodnie z informacjami podanymi do wiadomości publicznej w przeglądzie za 2015 r. potwierdzono sześć aktualnie obowiązujących celów. Zob. Urząd Dyrektora Krajowych Służb Wywiadowczych, reforma systemu rozpoznania radioelektronicznego, sprawozdanie okresowe za 2016 r.

([65]) Oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 6 (w odniesieniu do dyrektywy Wspólnoty Wywiadowczej nr 204). Zob. również sekcja 3 dyrektywy politycznej Prezydenta nr 28.

([66]) Oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 6. Zob. np. Biuro Wolności Obywatelskich i Ochrony Prywatności w ramach Agencji Bezpieczeństwa Narodowego, opracowane przez Agencję Bezpieczeństwa Narodowego sprawozdanie dotyczące środków ochrony wolności obywatelskich i prywatności na potrzeby ukierunkowanych działań w obszarze SIGINT na mocy rozporządzenia wykonawczego nr 12333 z dnia 7 października 2014 r. Zob. również sprawozdanie Urzędu Dyrektora Krajowych Służb Wywiadowczych z postępu prac w 2014 r. Jeżeli chodzi o wnioski o udostępnienie danych składane zgodnie z sekcją 702 ustawy o kontroli wywiadu, zapytania przetwarza się zgodnie z procedurami minimalizacji zatwierdzonymi przez Sąd ds. Inwigilacji Obcych Wywiadów. Zob. Biuro Wolności Obywatelskich i Ochrony Prywatności w ramach Agencji Bezpieczeństwa Narodowego, sprawozdanie dotyczące wdrażania sekcji 702 ustawy o kontroli wywiadu przez Agencję Bezpieczeństwa Narodowego z dnia 16 kwietnia 2014 r.

([67]) Zob. reforma systemu rozpoznania radioelektronicznego, sprawozdanie roczne za 2015 r. Zob. również oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 6, 8–9, 11.

(71) Ponadto ustanowione w dyrektywie politycznej Prezydenta nr 28 wymogi, zgodnie z którymi proces gromadzenia danych wywiadowczych musi być zawsze ([68])„w jak największym stopniu dostosowany do indywidualnych potrzeb", a Wspólnota Wywiadowcza musi w pierwszej kolejności podjąć próbę wyszukania innych informacji lub pozyskania poszukiwanych informacji z innych odpowiednich źródeł ([69]), odzwierciedlają ogólną zasadę nadrzędności ukierunkowanego gromadzenia danych nad hurtowym gromadzeniem danych. Zgodnie z gwarancją przedstawioną przez Urząd Dyrektora Krajowych Służb Wywiadowczych Urząd dopilnowuje, aby hurtowe gromadzenie danych nie miało „powszechnego" ani „bezkrytycznego" charakteru oraz aby wyjątek nie stał się regułą ([70]).

(72) Choć w dyrektywie politycznej Prezydenta nr 28 wyjaśniono, że jednostki Wspólnoty Wywiadowczej muszą w określonych przypadkach hurtowo gromadzić dane pochodzące z rozpoznania radioelektronicznego, na przykład w celu zidentyfikowania i oceny nowych lub pojawiających się zagrożeń, podmiotom tym zaleca się korzystanie w pierwszej kolejności z rozwiązań umożliwiających ukierunkowane gromadzenie danych pochodzących z rozpoznania radioelektronicznego ([71]). Oznacza to, że hurtowe gromadzenie danych będzie miało miejsce wyłącznie w przypadku, gdy przeprowadzenie ukierunkowanego gromadzenia danych przy zastosowaniu obowiązujących wyróżników – tj. kryterium identyfikujące związane z namierzaną osobą (np. adresu e-mail lub numeru telefonicznego danej osoby) – nie będzie możliwe „ze względów natury technicznej lub operacyjnej" ([72]). Dotyczy to zarówno sposobu gromadzenia danych pochodzących z rozpoznania radioelektronicznego, jak i danych, które faktycznie zostały zgromadzone ([72]).

(73) Zgodnie z oświadczeniami Urzędu Dyrektora Krajowych Służb Wywiadowczych nawet jeżeli Wspólnota Wywiadowcza nie może korzystać z określonych kryteriów identyfikujących w celu ukierunkowania gromadzenia, będzie dążyła do „jak największego" zawężenia gromadzonych danych. Aby to zapewnić, „stosuje filtry i inne narzędzia techniczne w celu skoncentrowania procesu gromadzenia danych na tych urządzeniach, które mogą zawierać komunikaty mające znaczenie dla wywiadu" (a więc będzie reagować na wymogi sformułowane przez amerykańskich decydentów zgodnie z procesem opisanym powyżej w motywie 70). W rezultacie hurtowe gromadzenie danych będzie ukierunkowywane na co najmniej dwa sposoby: po pierwsze, masowe gromadzenie danych zawsze będzie odnosić się do konkretnych celów obcego wywiadu (np. pozyskiwanie danych w ramach rozpoznania radioelektronicznego na temat działań grupy terrorystycznej działającej w danym regionie) oraz gromadzenie będzie ukierunkowywane na komunikaty, które są powiązane w dany sposób. Według zapewnień Urzędu Dyrektora Krajowych Służb Wywiadowczych znajduje to odzwierciedlenie w fakcie, że działania USA w zakresie rozpoznania radioelektronicznego dotykają jedynie ułamka komunikacji odbywającej się w internecie ([73]). Po drugie, w oświadczeniach Urzędu Dyrektora Krajowych Służb Wywiadowczych wyjaśniono, że stosowane filtry i inne narzędzia techniczne będą zaprojektowane na gromadzenie jak najdokładniejszych danych w celu zapewnienia zminimalizowania ilości „nieistotnych informacji".

(74) Ponadto nawet w przypadku, gdy Stany Zjednoczone stwierdzą, że hurtowe gromadzenie danych pochodzących z rozpoznania radioelektronicznego jest konieczne, biorąc pod uwagę warunki ustanowione w motywach 70–73, w dyrektywie politycznej Prezydenta nr 28 ograniczono możliwość wykorzystywania takich informacji wyłącznie do sześciu celów w obszarze bezpieczeństwa narodowego, aby zapewnić ochronę prywatności i wolności obywatelskich wszystkim osobom, niezależnie od ich narodowości i miejsca zamieszkania ([74]). Te dopuszczalne

([68]) Zob. oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 3.

([69]) Należy również podkreślić, że zgodnie z sekcją 2.4 rozporządzenia wykonawczego 12333 jednostki Wspólnoty Wywiadowczej „muszą stosować możliwie jak najmniej inwazyjne metody gromadzenia danych na terytorium Stanów Zjednoczonych". Aby uzyskać dodatkowe informacje na temat ograniczeń związanych z możliwością zastąpienia wszystkich przypadków hurtowego gromadzenia danych ukierunkowanym gromadzeniem danych, zob. wyniki oceny przeprowadzonej przez Krajową Radę ds. Badań przekazane Agencji Praw Podstawowych Unii Europejskiej zawarte w dokumencie pt. Nadzór nad służbami wywiadowczymi: gwarancje i środki ochrony prawnej w zakresie praw podstawowych w UE (Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU) (2015), s. 18.

([70]) Oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 4.

([71]) Zob. również sekcja 5 lit. d) dyrektywy politycznej Prezydenta nr 28, w której Dyrektora Krajowych Służb Wywiadowczych – współpracującego z jednostkami Wspólnoty Wywiadowczej i Urzędem ds. Polityki w dziedzinie Nauki i Technologii – zobowiązano do przekazywania Prezydentowi „sprawozdania dotyczące możliwości opracowania oprogramowania, które pozwoliłoby Wspólnocie Wywiadowczej usprawnić metodę ukierunkowanego gromadzenia danych, aby zapoczątkować proces odchodzenia od hurtowego gromadzenia danych". Z informacji podanych do wiadomości publicznej wynika, że w sprawozdaniu stwierdzono, iż „obecnie nie istnieje żadne bazujące na oprogramowaniu rozwiązanie alternatywne, które mogłoby w pełni zastąpić metodę hurtowego gromadzenia danych na potrzeby wykrywania określonych zagrożeń dla bezpieczeństwa narodowego". Zob. reforma systemu rozpoznania radioelektronicznego, sprawozdanie roczne za 2015 r.

([72]) Zob. przypis 68.

([73]) Oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI). Dotyczy to przede wszystkim obaw wyrażonych przez krajowe organy ochrony danych w opinii dotyczącej projektu decyzji w sprawie odpowiedniej ochrony danych osobowych. Zob. opinia 01/2016 Grupy Roboczej Art. 29 dotycząca projektu decyzji w sprawie odpowiedniej ochrony danych osobowych w ramach Tarczy Prywatności UE-USA (przyjęta w dniu 13 kwietnia 2016 r.), s. 38, nr 47.

([74]) Zob. sekcja 2 dyrektywy politycznej Prezydenta nr 28.

cele obejmują środki służące wykrywaniu i przeciwdziałaniu zagrożeniom spowodowanym działalnością szpiegowską, terroryzmem, bronią masowego rażenia i zagrożeniom dla bezpieczeństwa cybernetycznego oraz dla sił zbrojnych lub personelu wojskowego, a także zagrożeniom spowodowanym przestępczością transgraniczną powiązanym z pozostałymi pięcioma celami – działania w tym obszarze będą poddawane przeglądowi przeprowadzanemu przynajmniej raz w roku. Zgodnie z oświadczeniami rządu Stanów Zjednoczonych jednostki Wspólnoty Wywiadowczej udoskonaliły swoje praktyki i standardy analityczne w celu zapewnienia zgodności niepoddanych ocenie danych pochodzących z rozpoznania radioelektronicznego z tymi wymogami; korzystanie z ukierunkowanych zapytań „pozwala zagwarantować, że wśród danych przekazywanych analitykom do zbadania znajdą się wyłącznie informacje o potencjalnej wartości wywiadowczej" ([75]).

(75) Wspomniane ograniczenia mają szczególnie istotne znaczenie w kontekście przekazywania danych osobowych w ramach Tarczy Prywatności UE-USA, zwłaszcza w przypadku gdy gromadzenie danych osobowych ma miejsce poza terytorium Stanów Zjednoczonych, np. w trakcie przesyłania danych kablami transatlantyckimi z Unii do Stanów Zjednoczonych. Zgodnie z zapewnieniami organów amerykańskich przedstawionymi w oświadczeniach Urzędu Dyrektora Krajowych Służb Wywiadowczych w przypadku gromadzenia danych w opisany powyżej sposób zastosowanie mają ograniczenia i gwarancje ustanowione w tych oświadczeniach – uwzględniając postanowienia dyrektywy politycznej Prezydenta nr 28 ([76]).

(76) Zasady te odpowiadają zasadzie konieczności i proporcjonalności, mimo że nie mają takiego samego brzmienia. Nacisk kładzie się przede wszystkim na ukierunkowane gromadzenie danych, ograniczając hurtowe gromadzenie danych do (wyjątkowych) przypadków, w których gromadzenie danych w ukierunkowany sposób nie jest możliwe ze względów technicznych lub operacyjnych. Nawet w przypadkach, w których nie da się uniknąć *hurtowego gromadzenia* danych, możliwość dalszego „wykorzystywania" tych danych poprzez uzyskiwanie do nich dostępu jest *ściśle ograniczona* do konkretnych, zgodnych z prawem celów związanych z bezpieczeństwem narodowym ([77]).

(77) Z uwagi na fakt, że wymogi te zostały zawarte w dyrektywie wydanej przez Prezydenta, który pełni funkcję dyrektora wykonawczego, są wiążące dla całej Wspólnoty Wywiadowczej i zostały wdrożone w ramach przepisów i procedur agencyjnych przekładających ogólne zasady na konkretne wskazówki dotyczące codziennej działalności. Ponadto, choć Kongres sam w sobie nie jest związany postanowieniami dyrektywy politycznej Prezydenta nr 28, podjął również kroki na rzecz zagwarantowania, aby dane osobowe w Stanach Zjednoczonych były gromadzone w ukierunkowany sposób i aby uzyskiwano do nich dostęp w ukierunkowany sposób, a nie na „zasadzie ogólnej".

(78) Z dostępnych informacji, w tym z oświadczenia otrzymanego od rządu Stanów Zjednoczonych, wynika, że po przekazaniu danych podmiotom mającym swoją siedzibę w Stanach Zjednoczonych, które dokonały samocertyfikacji w ramach Tarczy Prywatności UE-USA, amerykańskie agencje wywiadowcze mogą ([78]) wystąpić o udostępnienie im danych osobowych wyłącznie w przypadku, gdy złożony przez nie wniosek będzie zgodny z przepisami ustawy o kontroli wywiadu, lub w przypadku gdy wniosek zostanie złożony przez Federalne Biuro Śledcze (FBI) w oparciu o tzw. wezwanie do przedstawienia informacji do celów bezpieczeństwa narodowego ([79]). W ustawie o kontroli wywiadu przewidziano szereg podstaw prawnych, na których można się oprzeć przy

([75]) Oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 4. Zob. również dyrektywa Wspólnoty Wywiadowczej nr 203.

([76]) Oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 2. W tym kontekście zastosowanie mają również ograniczenia ustanowione w rozporządzeniu wykonawczym nr 12333 (np. wymóg zapewnienia zgodności gromadzonych informacji z priorytetami wywiadowczymi wyznaczonymi przez Prezydenta).

([77]) Zob. wyrok w sprawie Schrems, pkt 93.

([78]) Ponadto Federalne Biuro Śledcze może również gromadzić dane na podstawie zezwoleń w zakresie egzekwowania prawa (zob. sekcja 3.2 niniejszej decyzji).

([79]) Aby uzyskać dodatkowe informacje na temat korzystania z wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego, zob. oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 13–14, nr 38. Jak wskazano w tych oświadczeniach, Federalne Biuro Śledcze może skorzystać z wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego wyłącznie w celu zwrócenia się o przekazanie informacji niedotyczących treści istotnych w kontekście zatwierdzonego krajowego postępowania sprawdzającego prowadzonego w celu zapewnienia ochrony przed terroryzmem międzynarodowym lub tajnymi działaniami wywiadowczymi. Jeżeli chodzi o przekazywanie danych w ramach Tarczy Prywatności UE-USA, za najistotniejsze upoważnienie prawne należałoby uznać ustawę o ochronie danych w łączności elektronicznej (tytuł 18 § 2709 U.S.C.), w której ustanowiono wymóg opatrzenia każdego wniosku o przekazanie informacji na temat abonenta lub o udostępnienie rejestrów transakcji „elementem umożliwiającym bezpośrednią identyfikację danej osoby, podmiotu, numeru telefonicznego lub rachunku".

gromadzeniu (i późniejszym przetwarzaniu) danych osobowych osób z UE, których dane dotyczą, przekazywanych w ramach Tarczy Prywatności UE-USA. Poza sekcją 104 ustawy o kontroli wywiadu ([80]) obejmującą tradycyjne, zindywidualizowane środki dozoru elektronicznego i sekcją 402 ([81]) dotyczącą urządzeń rejestrujących wybierane numery oraz urządzeń śledzących dwa kluczowe instrumenty zostały ustanowione w sekcji 501 ustawy o kontroli wywiadu (dawna sekcja 215 amerykańskiej ustawy antyterrorystycznej (U.S. Patriot Act)) oraz w sekcji 702 ustawy o kontroli wywiadu ([82]).

(79) W tym kontekście w amerykańskiej ustawie o wolności, którą uchwalono w dniu 2 czerwca 2015 r., zabrania się hurtowego gromadzenia dokumentacji na podstawie sekcji 402 ustawy o kontroli wywiadu (podstawa prawna do stosowania urządzeń rejestrujących wybierane numery oraz urządzeń śledzących), sekcji 501 ustawy o kontroli wywiadu (dawna sekcja 215 amerykańskiej ustawy antyterrorystycznej) ([83]) oraz poprzez korzystanie z wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego, a zamiast tego wymaga się stosowania konkretnych „terminów umożliwiających selekcję" ([84]).

(80) Chociaż w ustawie o kontroli wywiadu przewiduje się dodatkowe dokumenty stanowiące podstawę prawną do prowadzenia krajowych działań wywiadowczych, w tym rozpoznania radioelektronicznego, z oceny Komisji wynika, że w zakresie, w jakim chodzi o dane osobowe przekazywane w ramach Tarczy Prywatności UE-USA, wspomniane dokumenty w równym stopniu ograniczają ingerencję organów publicznych w ukierunkowane gromadzenie i dostęp.

(81) Jest to wyraźnie widoczne w przypadku tradycyjnego zindywidualizowanego dozoru elektronicznego na mocy sekcji 104 ustawy o kontroli wywiadu ([85]). Jeżeli chodzi o sekcję 702 ustawy o kontroli wywiadu, która stanowi podstawę dwóch ważnych programów wywiadowczych prowadzonych przez agencje wywiadowcze Stanów Zjednoczonych (PRISM, UPSTREAM), przeszukiwania prowadzi się w sposób ukierunkowany dzięki wykorzystaniu indywidualnych selektorów, które identyfikują konkretne środki umożliwiające komunikację, takie jak adres e-mail lub numer telefoniczny danej osoby, a nie kluczowe słowa ani nawet imiona i nazwiska osób fizycznych, na które są ukierunkowane takie działania ([86]). W związku z powyższym, jak zauważyła Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi, sekcja 702 ustawy o kontroli wywiadu „w całości

([80]) Tytuł 50 § 1804 U.S.C. Choć ta podstawa prawna wymaga „przedstawienia stanu faktycznego i okoliczności, na które wnioskodawca powołał się, aby uzasadnić swoje przekonanie, że a) podmiot objęty dozorem elektronicznym jest kontrolowany przez obce państwo lub jest agentem obcego państwa", ta ostania kategoria może obejmować osoby niebędące obywatelami ani rezydentami amerykańskimi, 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.). Istnieje jednak tylko teoretyczne powiązanie z danymi osobowymi przekazywanymi w ramach Tarczy Prywatności UE-USA, zważywszy, że przedstawienie stanu faktycznego musi także uzasadnić przekonanie, iż „każdy obiekt lub każde miejsce, na które ukierunkowany jest dozór elektroniczny, są użytkowane lub wkrótce będą użytkowane przez obce państwo lub przez agenta obcego państwa". W każdym razie skorzystanie z tej podstawy prawnej wymaga złożenia wniosku do Sądu ds. Inwigilacji Obcych Wywiadów, który oceni m.in. czy na podstawie przedstawionych faktów istnieje uzasadnione podejrzenie, że dane zdarzenie faktycznie miało miejsce.

([81]) Tytuł 50 § 1842 i § 1841 ust. 2 i tytuł 18 sekcja 3127 U.S.C. 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). Wymaga ona złożenia wniosku o wydanie nakazu przez Sąd ds. Inwigilacji Obcych Wywiadów (lub amerykańskiego sędziego pokoju) i zastosowanie konkretnego terminu identyfikującego w rozumieniu § 1841 ust. 4, tj. terminu, który w konkretny sposób identyfikuje daną osobę, konto itd. i jest stosowany w celu ograniczenia w jak największym stopniu zakresu żądanych informacji.

([82]) Chociaż w sekcji 501 ustawy o kontroli wywiadu (dawna sekcja 215 amerykańskiej ustawy antyterrorystycznej) upoważnia się FBI do wystąpienia o nakaz sądowy mający na celu przedstawienie „przedmiotów materialnych" (w szczególności metadanych telefonicznych, ale również dokumentacji dotyczącej prowadzonej działalności) do celów wywiadu zagranicznego, zgodnie z sekcją 702 ustawy o kontroli wywiadu jednostki amerykańskiej Wspólnoty Wywiadowczej mogą starać się o uzyskanie dostępu do informacji, w tym treści komunikatów internetowych, od Stanów Zjednoczonych, skupiając się jednak na określonych osobach niebędących obywatelami ani rezydentami amerykańskimi przebywających poza Stanami Zjednoczonymi.

([83]) Na podstawie tego przepisu FBI może zażądać wydania „przedmiotów materialnych" (np. rejestrów, opracowań, dokumentów) na podstawie wykazania przed Sądem ds. Inwigilacji Obcych Wywiadów, że istnieją uzasadnione przesłanki, aby przypuszczać, że mają one istotne znaczenie dla konkretnego dochodzenia prowadzonego przez FBI. Prowadząc takie poszukiwania, FBI musi korzystać z terminów umożliwiających selekcję zatwierdzonych przez Sąd ds. Inwigilacji Obcych Wywiadów, w odniesieniu do których istnieje „uzasadnione, wyraźne podejrzenie", że taki termin jest powiązany z co najmniej jednym obcym państwem lub agentem obcego państwa zaangażowanego w międzynarodowy terroryzm lub związane z tym działania przygotowawcze. Zob. sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 215, s. 59; Biuro Wolności Obywatelskich i Ochrony Prywatności Agencji Bezpieczeństwa Narodowego, Sprawozdanie z przejrzystości: Wdrażanie zmian w zakresie dokumentacji dotyczącej prowadzonej działalności i ustawy o kontroli wywiadu wprowadzonych w amerykańskiej ustawie o wolności (Transparency Report: The USA Freedom Act Business Records FISA Implementation) z dnia 15 stycznia 2016 r., s. 4–6.

([84]) Oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 13 (nr 38).

([85]) Zob. przypis 81.

([86]) Sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 702, s. 32–33, z dalszymi odniesieniami. W uzgodnieniu ze swoim biurem ochrony prywatności 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.

polega na ukierunkowaniu działań na określone osoby [niebędące obywatelami Stanów Zjednoczonych], w odniesieniu do których przeprowadzono zindywidualizowane rozpoznanie" ([87]). Ze względu na klauzulę „wygaśnięcia" konieczne będzie dokonanie w 2017 r. przeglądu sekcji 702 ustawy o kontroli wywiadu i wówczas Komisja będzie musiała przeprowadzić ponowną ocenę gwarancji dostępnych dla osób z UE, których dane dotyczą.

(82) Ponadto w swoich oświadczeniach rząd Stanów Zjednoczonych wyraźnie zapewnił Komisję Europejską, że Wspólnota Wywiadowcza Stanów Zjednoczonych „nie prowadzi żadnego rodzaju bezkrytycznej inwigilacji żadnych osób fizycznych, w tym zwykłych obywateli Unii" ([88]). Jeżeli chodzi o dane osobowe gromadzone w Stanach Zjednoczonych, oświadczenie to jest poparte dowodami empirycznymi, z których wynika, że *wnioski o udostępnienie danych* poprzez wezwanie do przedstawienia informacji do celów bezpieczeństwa narodowego i na mocy ustawy o kontroli wywiadu zarówno osobno, jak i łącznie dotyczą tylko stosunkowo niewielkiej liczby celów w porównaniu z ogólnym przepływem danych w internecie ([89]).

(83) Jeżeli chodzi o *dostęp* do gromadzonych danych i *bezpieczeństwo danych*, w dyrektywie politycznej Prezydenta nr 28 wymaga się, aby dostęp „był ograniczony do upoważnionych pracowników, którzy potrzebują danych, aby wywiązywać się ze swoich obowiązków" oraz aby dane osobowe „były przetwarzane i przechowywane w warunkach, które zapewniają odpowiednią ochronę i uniemożliwiają dostęp osobom nieupoważnionym, zgodnie z obowiązującymi gwarancjami dotyczącymi danych wrażliwych". Pracownicy służb wywiadowczych przechodzą właściwe i odpowiednie szkolenie w zakresie zasad określonych w dyrektywie politycznej Prezydenta nr 28 ([90]).

(84) Ponadto, jeżeli chodzi o *przechowywanie* i dalsze *rozpowszechnianie* danych osobowych osób z UE, zgromadzonych przez amerykańskie organy wywiadowcze, dyrektywa polityczna Prezydenta nr 28 stanowi, że wszystkie osoby (w tym osoby niebędące obywatelami ani rezydentami Stanów Zjednoczonych) należy traktować z godnością i szacunkiem, że wszystkie osoby mają uzasadniony interes w dążeniu do zapewnienia poszanowania ich prywatności przy przetwarzaniu dotyczących ich danych osobowych oraz że jednostki Wspólnoty Wywiadowczej muszą zatem ustanowić strategie polityczne zapewniające odpowiednie gwarancje dla takich danych „odpowiednio zaplanowane w celu ograniczenia rozpowszechniania i przechowywania danych osobowych" ([91]).

([87]) Sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 702, s. 111; Zob. także oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 9 („Gromadzenie danych zgodnie z sekcją 702 [ustawy o kontroli wywiadu] nie jest »masowe i bezkrytyczne«, lecz jest ściśle ukierunkowane na gromadzenie zagranicznych informacji wywiadowczych od indywidualnie określonych, uzasadnionych osób wybranych jako cel działań wywiadowczych") oraz s. 13, nr 36 (wraz z odniesieniami do opinii Sądu ds. Inwigilacji Obcych Wywiadów z 2014 r.); Biuro Wolności Obywatelskich i Ochrony Prywatności w ramach Agencji Bezpieczeństwa Narodowego, Wdrażanie sekcji 702 ustawy o kontroli wywiadu przez Agencję Bezpieczeństwa Narodowego z dnia 16 kwietnia 2014 r. Nawet w przypadku UPSTREAM Agencja Bezpieczeństwa Narodowego może jedynie wystąpić o przechwytywanie komunikatów elektronicznych do określonych selektorów, od tych selektorów lub na ich temat.

([88]) Oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 18. Zob. także s. 6, zgodnie z którą mające zastosowanie procedury świadczą o „wyraźnym zaangażowaniu w zapobieganie gromadzeniu danych w ramach rozpoznania radioelektronicznego w sposób arbitralny i bezkrytyczny oraz we wdrażanie – począwszy od najwyższych szczebli naszego rządu – zasady rozsądnego działania".

([89]) Zob. statystyczne sprawozdanie z przejrzystości dotyczące korzystania z dokumentów stanowiących podstawę prawną do celów bezpieczeństwa narodowego (Statistical Transparency Report Regarding Use of National Security Authorities) z dnia 22 kwietnia 2015 r. W odniesieniu do ogólnego przepływu danych w internecie zob. np. Agencja Praw Podstawowych, Inwigilacja prowadzona przez służby wywiadowcze: gwarancje i środki ochrony prawnej w zakresie praw podstawowych w UE (Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU) (2015), s. 15–16. Jeżeli chodzi o program agencji UPSTREAM, zgodnie z odtajnioną opinią Sądu ds. Inwigilacji Obcych Wywiadów z 2011 r. ponad 90 % komunikatów elektronicznych zgromadzonych zgodnie z sekcją 702 ustawy o kontroli wywiadu pochodziło z programu agencji PRISM, podczas gdy mniej niż 10 % pochodziło z programu agencji UPSTREAM. Zob. Sąd ds. Inwigilacji Obcych Wywiadów, Opinia w sprawie memorandum, 2011 WL 10945618 (Sąd ds. Inwigilacji Obcych Wywiadów, z dnia 3 października 2011 r.), nr 21 (dokument dostępny na stronie internetowej: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) Zob. sekcja 4 lit. a) ppkt (ii) dyrektywy politycznej Prezydenta nr 28. Zob. także Urząd Dyrektora Krajowych Służb Wywiadowczych, Ochrona danych osobowych wszystkich osób: Sprawozdanie z postępu prac nad opracowywaniem i wdrażaniem procedur przewidzianych w dyrektywie politycznej Prezydenta nr 28 (Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28), lipiec 2014 r., s. 5, zgodnie z którym „polityka jednostek Wspólnoty Wywiadowczej powinna służyć wzmocnieniu istniejących praktyk i norm analitycznych, na mocy których analitycy muszą dążyć do strukturyzowania zapytań lub innych warunków i technik wyszukiwania w celu wskazania danych wywiadowczych istotnych z perspektywy ważnego zadania z zakresu działań wywiadowczych lub egzekwowania prawa; muszą zagwarantować, że zapytania dotyczące osób będą koncentrować się na tych kategoriach danych wywiadowczych, które odpowiadają wymogowi dotyczącemu działań wywiadowczych lub egzekwowania prawa; oraz zminimalizować przegląd danych osobowych niemających znaczenia z punktu widzenia wymogów dotyczących działań wywiadowczych lub egzekwowania prawa". Zob. np. CIA, Działalność w zakresie rozpoznania radioelektronicznego (Signals Intelligence Activities), s. 5; Federalne Biuro Śledcze, Strategie polityczne i procedury przewidziane w dyrektywie politycznej Prezydenta nr 28 (Presidential Policy Directive 28 Policies and Procedures), s. 3. Według sprawozdania z postępów z 2016 r. dotyczącego reformy systemu rozpoznania radioelektronicznego jednostki Wspólnoty Wywiadowczej (w tym FBI, CIA i Agencja Bezpieczeństwa Narodowego) podjęły kroki mające na celu uwrażliwienie pracowników na wymogi określone w dyrektywie politycznej Prezydenta nr 28 poprzez opracowanie nowych lub zmianę istniejących strategii szkoleniowych.

([91]) Zgodnie z oświadczeniami Urzędu Dyrektora Krajowych Służb Wywiadowczych ograniczenia te mają zastosowanie niezależnie od tego, czy informacje gromadzone są hurtowo czy poprzez ukierunkowane gromadzenie danych oraz niezależnie od narodowości osoby fizycznej.

(85) Rząd Stanów Zjednoczonych wyjaśnił, że ten wymóg zasadności oznacza, iż jednostki Wspólnoty Wywiadowczej nie będą musiały przyjmować „żadnych środków, które są teoretycznie możliwe", ale będą zobowiązane do „zrównoważenia swoich wysiłków służących ochronie uzasadnionych interesów w zakresie prywatności i wolności obywatelskich praktycznymi wymogami dotyczącymi działalności w zakresie rozpoznania radioelektronicznego" ([92]). W związku z tym osoby niebędące obywatelami ani rezydentami Stanów Zjednoczonych będą traktowane w taki sam sposób jak obywatele i rezydenci Stanów Zjednoczonych, w oparciu o procedury zatwierdzone przez Prokuratora Generalnego ([93]).

(86) Zgodnie z tymi zasadami dane mogą być zasadniczo przechowywane przez okres maksymalnie pięciu lat, chyba że istnieje konkretne wskazanie w prawie lub wyraźne wskazanie przez Dyrektora Krajowych Służb Wywiadowczych przedstawione po dokładnej ocenie względów prywatności – z uwzględnieniem poglądów urzędnika ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych oraz urzędników agencyjnych ds. prywatności i wolności obywatelskich – że dalsze przechowywanie danych leży w interesie bezpieczeństwa narodowego ([94]). Rozpowszechnianie jest ograniczone do przypadków, w których informacje są istotne z punktu widzenia podstawowego celu gromadzenia i w związku z tym odpowiadają wymogowi zatwierdzonych działań wywiadowczych lub zatwierdzonego egzekwowania prawa ([95]).

(87) Zgodnie z zapewnieniami udzielonymi przez rząd Stanów Zjednoczonych nie można rozpowszechniać danych osobowych tylko z tego względu, że dana osoba fizyczna nie jest obywatelem ani rezydentem Stanów Zjednoczonych, a „dane zgromadzone w wyniku rozpoznania radioelektronicznego dotyczące rutynowych czynności osoby obcego pochodzenia nie zostałyby uznane za dane wywiadowcze, które mogłyby być stale rozpowszechniane lub przechowywane jedynie z tego tytułu, chyba że jest to zgodne z jednym z zatwierdzonych wymogów dotyczących działań wywiadowczych" ([96]).

(88) Na podstawie powyższego Komisja stwierdza, że w Stanach Zjednoczonych wdrożono przepisy służące ograniczeniu wszelkiej ingerencji do celów bezpieczeństwa narodowego w prawa podstawowe osób, których dane osobowe są przekazywane z Unii do Stanów Zjednoczonych w ramach Tarczy Prywatności UE-USA, do tego, co jest ściśle niezbędne, aby osiągnąć uzasadniony cel.

(89) Jak wynika z powyższej analizy, prawo Stanów Zjednoczonych zapewnia stosowanie środków nadzoru wyłącznie w celu pozyskania danych wywiadowczych – co stanowi uzasadniony cel polityki ([97]) – i ich maksymalne

([92]) Zob. oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI).

([93]) Zob. sekcja 4 lit. a) ppkt (i) dyrektywy politycznej Prezydenta nr 28 oraz sekcja 2.3 rozporządzenia wykonawczego 12333.

([94]) Sekcja 4 lit. a) ppkt (i) dyrektywy politycznej Prezydenta nr 28; oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 7. Na przykład w odniesieniu do danych osobowych gromadzonych na podstawie sekcji 702 ustawy o kontroli wywiadu w ramach procedur minimalizacji Agencji Bezpieczeństwa Narodowego zatwierdzonych przez Sąd ds. Inwigilacji Obcych Wywiadów przewiduje się zasadę, zgodnie z którą metadane i nieocenione treści na potrzeby programu PRISM są przechowywane przez okres nie dłuższy niż pięć lat, zaś dane z programu UPSTREAM są przechowywane nie dłuższej niż dwa lata. Agencja Bezpieczeństwa Narodowego przestrzega tych terminów przechowywania dzięki zautomatyzowanemu procesowi, w ramach którego usuwa się zgromadzone dane po zakończeniu odpowiedniego okresu przechowywania. Zob. procedury minimalizacji Agencji Bezpieczeństwa Narodowego określone w sekcji 702 ustawy o kontroli wywiadu oraz sekcja 7 i sekcja 6 lit. a) pkt 1; Biuro Wolności Obywatelskich i Ochrony Prywatności Agencji Bezpieczeństwa Narodowego, sprawozdanie dotyczące wdrażania sekcji 702 ustawy o kontroli wywiadu przez Agencję Bezpieczeństwa Narodowego z dnia 16 kwietnia 2014 r. Podobnie przechowywanie danych na mocy sekcji 501 ustawy o kontroli wywiadu (dawna sekcja 215 amerykańskiej ustawy antyterrorystycznej) jest ograniczone do pięciu lat, chyba że dane osobowe są objęte należycie zatwierdzonym rozpowszechnianiem danych wywiadowczych lub Departament Sprawiedliwości doradzi Agencji Bezpieczeństwa Narodowego na piśmie, że rejestry podlegają obowiązkowi zachowania w związku z toczącym się lub przewidywanym postępowaniem sądowym. Zob. Biuro Wolności Obywatelskich i Ochrony Prywatności Agencji Bezpieczeństwa Narodowego, Sprawozdanie z przejrzystości: Wdrażanie zmian w zakresie dokumentacji dotyczącej prowadzonej działalności i ustawy o kontroli wywiadu wprowadzonych w amerykańskiej ustawie o wolności z dnia 15 stycznia 2016 r.

([95]) W szczególności w przypadku sekcji 501 ustawy o kontroli wywiadu (dawna sekcja 215 amerykańskiej ustawy antyterrorystycznej) dane osobowe można rozpowszechniać jedynie do celów walki z terroryzmem lub jako dowód przestępstwa; w przypadku sekcji 702 ustawy o kontroli wywiadu – tylko jeżeli istnieje ważny cel działań wywiadowczych lub działań z zakresu egzekwowania prawa. Por. Biuro Wolności Obywatelskich i Ochrony Prywatności Agencji Bezpieczeństwa Narodowego, sprawozdanie dotyczące wdrażania sekcji 702 ustawy o kontroli wywiadu przez Agencję Bezpieczeństwa Narodowego z dnia 16 kwietnia 2014 r.; Sprawozdanie z przejrzystości: Wdrażanie zmian w zakresie dokumentacji dotyczącej prowadzonej działalności i ustawy o kontroli wywiadu wprowadzonych w amerykańskiej ustawie o wolności z dnia 15 stycznia 2016 r. Zob. także opracowane przez Agencję Bezpieczeństwa Narodowego sprawozdanie dotyczące środków ochrony wolności obywatelskich i prywatności na potrzeby ukierunkowanych działań w obszarze SIGINT na mocy rozporządzenia wykonawczego nr 12333 z dnia 7 października 2014 r.

([96]) Oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 7 (w odniesieniu do dyrektywy Wspólnoty Wywiadowczej nr 203).

([97]) Trybunał Sprawiedliwości wyjaśnił, że bezpieczeństwo narodowe stanowi uzasadniony cel polityki. Zob. wyrok w sprawie Schrems, pkt 88. Zob. także wyrok w sprawie Digital Rights Ireland i in., pkt 42–44 i 51, w którym Trybunał Sprawiedliwości uznał, że walka z poważną przestępczością, a zwłaszcza z przestępczością zorganizowaną i terroryzmem, może w dużym stopniu zależeć od wykorzystania nowoczesnych technik dochodzeniowo-śledczych. Ponadto w przeciwieństwie do czynności dochodzeniowo-śledczych, które zazwyczaj dotyczą retrospektywnego ustalenia odpowiedzialności i winy za czyny popełnione w przeszłości, działania wywiadowcze często polegają na zapobieganiu zagrożeniom dla bezpieczeństwa narodowego przed wystąpieniem szkody. Dlatego takie dochodzenia często muszą obejmować szerszy krąg ewentualnych zaangażowanych podmiotów („namierzanych osób") oraz większy obszar geograficzny. Por. wyrok Europejskiego Trybunału Praw Człowieka w sprawie Weber i Saravia przeciwko Niemcom z dnia 29 czerwca 2006 r., skarga nr 54934/00, pkt 105–118 (w sprawie tzw. „monitorowania strategicznego").

dostosowanie do specyfiki prowadzonych działań. W szczególności hurtowe gromadzenie danych będzie dozwolone tylko w wyjątkowych przypadkach, gdy ukierunkowane gromadzenie danych jest niewykonalne, oraz będzie zabezpieczone dodatkowymi gwarancjami w celu zminimalizowania ilości gromadzonych danych i późniejszego dostępu (który będzie ukierunkowany na konkretne dane i dozwolony jedynie do określonych celów).

(90) W ocenie Komisji jest to zgodne z normą określoną przez Trybunał Sprawiedliwości w wyroku w sprawie Schrems, zgodnie z którą uregulowania stanowiące ingerencję w prawa podstawowe gwarantowane w art. 7 i 8 karty muszą ustanawiać „minimalne zabezpieczenia" ([98]), a ponadto uregulowanie „umożliwiające generalnie przechowywanie wszelkich danych osobowych wszystkich osób fizycznych, których dane zostały przekazane z Unii Europejskiej do Stanów Zjednoczonych bez jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od zamierzonego celu i bez przewidzenia obiektywnych kryteriów, które pozwoliłyby na ograniczenie dostępu władz publicznych do danych oraz na ich późniejsze wykorzystanie do określonych celów, ściśle ograniczonych, które mogą uzasadnić ingerencję, jaką stanowi zarówno dostęp, jak i wykorzystanie tych danych, nie ogranicza się do tego, co absolutnie konieczne" ([99]). Nie będzie też nieograniczonego gromadzenia i przechowywania danych wszystkich osób bez jakichkolwiek ograniczeń ani nie będzie nieograniczonego dostępu. Ponadto oświadczenia przekazane Komisji, w tym zapewnienia, że działania USA w zakresie rozpoznania radioelektronicznego dotykają jedynie ułamka komunikacji odbywającej się w internecie, wykluczają „generalny" ([100]) dostęp do treści komunikatów elektronicznych.

3.1.2. Skuteczna ochrona prawna

(91) Komisja oceniła zarówno mechanizmy nadzoru, które istnieją w Stanach Zjednoczonych w odniesieniu do ewentualnej ingerencji amerykańskich organów wywiadowczych w dane osobowe przekazywane Stanom Zjednoczonym, jak i możliwości indywidualnego dochodzenia roszczeń dostępne osobom z UE, których dane dotyczą.

Nadzór

(92) Amerykańska Wspólnota Wywiadowcza podlega różnym mechanizmom przeglądu i nadzoru w ramach trzech gałęzi władzy federalnej. Obejmują one organy wewnętrzne i zewnętrzne w strukturze władzy wykonawczej, szereg komisji Kongresu oraz kontrolę sądową, przy czym ta ostatnia w szczególności dotyczy działań prowadzonych w ramach ustawy o kontroli wywiadu.

(93) Po pierwsze, działania wywiadowcze prowadzone przez organy Stanów Zjednoczonych objęte są szeroko zakrojonym nadzorem ze strony władzy wykonawczej.

(94) Zgodnie z sekcją 4 lit. a) ppkt (iv) dyrektywy politycznej Prezydenta nr 28 strategie polityczne i procedury jednostek Wspólnoty Wywiadowczej „obejmują właściwe środki ułatwiające nadzór nad wdrażaniem gwarancji chroniących dane osobowe"; środki te powinny obejmować okresowe audyty ([101]).

([98]) Zob. wyrok w sprawie Schrems, pkt 91 z dalszymi odniesieniami.
([99]) Wyrok w sprawie Schrems, pkt 93.
([100]) Por. wyrok w sprawie Schrems, pkt 94.
([101]) Urząd Dyrektora Krajowych Służb Wywiadowczych, Ochrona danych osobowych wszystkich osób: Sprawozdanie z postępu prac nad opracowywaniem i wdrażaniem procedur przewidzianych w dyrektywie politycznej Prezydenta nr 28, s. 7. Zob. np. CIA, Działalność w zakresie rozpoznania radioelektronicznego, s. 6 (Zgodność); Federalne Biuro Śledcze, Strategie polityczne i procedury przewidziane w dyrektywie politycznej Prezydenta nr 28, sekcja III pkt A ust. 4, sekcja III pkt B ust. 4; Agencja Bezpieczeństwa Narodowego, Procedury przewidziane w sekcji 4 dyrektywy politycznej Prezydenta nr 28 (PPD-28 Section 4 Procedures) z dnia 12 stycznia 2015 r., sekcja 8.1, 8.6 lit. c).

(95) W tym zakresie wdrożono wiele poziomów nadzoru obejmujących m.in. urzędników ds. wolności obywatelskich lub ochrony prywatności, Inspektorów Generalnych, Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych, Radę Nadzoru nad Prywatnością i Wolnościami Obywatelskimi oraz prezydencką Radę Nadzoru nad Służbami Wywiadowczymi. Wspomniane funkcje nadzorcze wspierają pracownicy ds. zgodności we wszystkich agencjach ([102]).

(96) Jak wyjaśnił rząd Stanów Zjednoczonych ([103]), *urzędnicy ds. wolności obywatelskich lub ochrony prywatności* odpowiedzialni za nadzór pracują w różnych departamentach odpowiedzialnych za działania wywiadowcze i w agencjach wywiadowczych ([104]). 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 (w niektórych przypadkach, podobnie jak Urząd Dyrektora Krajowych Służb Wywiadowczych, sami mogą mieć uprawnienia do badania skarg ([105])). Z kolei dyrektor departamentu/agencji musi zapewnić, aby urzędnik otrzymał wszystkie dane oraz dostęp do wszystkich materiałów niezbędnych do wykonywania swoich funkcji. Urzędnicy ds. wolności obywatelskich i ochrony prywatności składają Kongresowi i Radzie Nadzoru nad Prywatnością i Wolnościami Obywatelskimi 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 ([106]). Zgodnie z oceną krajowych organów ochrony danych nadzór wewnętrzny sprawowany przez urzędników ds. wolności obywatelskich lub ochrony prywatności można uznać za „stosunkowo dokładny", nawet jeżeli ich zdaniem nie spełniają one wymaganego poziomu niezależności ([107]).

(97) Ponadto każda jednostka Wspólnoty Wywiadowczej posiada własnego *Inspektora Generalnego* odpowiadającego m. in. za nadzorowanie działań wywiadowczych ([108]). Obejmuje to, w obrębie Urzędu Dyrektora Krajowych Służb Wywiadowczych, Biuro Inspektora Generalnego, 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 ([109]). Inspektorzy Generalni są ustawowo niezależnymi ([110]) jednostkami odpowiedzialnymi za przeprowadzanie audytów i dochodzeń dotyczących programów i działań prowadzonych przez odpowiednią agencję do krajowych celów wywiadowczych, w tym nadużyć lub naruszeń prawa ([111]). Są uprawnieni do wglądu we wszystkie rejestry, sprawozdania, audyty, przeglądy, dokumenty, opracowania, zalecenia lub inne istotne materiały, w razie potrzeby na mocy

([102]) Na przykład Agencja Bezpieczeństwa Narodowego zatrudnia ponad 300 pracowników ds. zgodności w Dyrekcji ds. Zgodności. Zob. oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 7.

([103]) Zob. pismo dotyczące urzędu Rzecznika (załącznik III), sekcja 6 lit. b) ppkt (i)–(iii).

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

([105]) Według rządu Stanów Zjednoczonych, jeżeli Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych otrzyma skargę, będzie również współpracowało z innymi jednostkami Wspólnoty Wywiadowczej nad sposobem rozpatrzenia skargi w ramach Wspólnoty Wywiadowczej. Zob. pismo dotyczące urzędu Rzecznika (załącznik III), sekcja 6 lit. b) ppkt (ii).

([106]) Zob. tytuł 42 § 2000ee-1 lit. f) pkt 1 i 2 U.S.C.

([107]) Zob. opinia 01/2016 Grupy Roboczej Art. 29 dotycząca projektu decyzji w sprawie odpowiedniej ochrony danych osobowych w ramach Tarczy Prywatności UE-USA (przyjęta w dniu 13 kwietnia 2016 r.), s. 41.

([108]) Oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 7. Zob. np. Agencja Bezpieczeństwa Narodowego, Procedury przewidziane w sekcji 4 dyrektywy politycznej Prezydenta nr 28 z dnia 12 stycznia 2015 r., sekcja 8.1; CIA, Działalność w zakresie rozpoznania radioelektronicznego, s. 7 (Obowiązki).

([109]) Inspektora Generalnego (urząd ten utworzono w październiku 2010 r.) powołuje Prezydent za zgodą Senatu; Inspektor może zostać odwołany wyłącznie przez Prezydenta – takie uprawnienie nie przysługuje Dyrektorowi Krajowych Służb Wywiadowczych.

([110]) Wspomniani 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. ustawa o Inspektorze Generalnym z 1978 r., § 8 (Inspektor Generalny Departamentu Obrony); § 8E (Inspektor Generalny Departamentu Sprawiedliwości), § 8G lit. d) pkt 2 ppkt A, B (Inspektor Generalny Agencji Bezpieczeństwa Narodowego); tytuł 50 § 403q lit. b) U.S.C. (Inspektor Generalny Centralnej Agencji Wywiadowczej); ustawa o autoryzacji działań wywiadowczych na rok budżetowy 2010, sekcja 405 lit. f) (Inspektor Generalny Wspólnoty Wywiadowczej). Zgodnie z oceną krajowych organów ochrony danych Inspektorzy Generalni „mogą spełnić kryterium dotyczące niezależności organizacyjnej, jak określił Trybunał Sprawiedliwości Unii Europejskiej i Europejski Trybunał Praw Człowieka, przynajmniej od momentu gdy nowa procedura nominacji będzie miała zastosowanie do wszystkich organów". Zob. opinia 01/2016 Grupy Roboczej Art. 29 dotycząca projektu decyzji w sprawie odpowiedniej ochrony danych osobowych w ramach Tarczy Prywatności UE-USA (przyjęta w dniu 13 kwietnia 2016 r.), s. 40.

([111]) Zob. oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 7. Zob. również ustawa o Inspektorze Generalnym z 1978 r., z późniejszymi zmianami, Zbiór ustaw publicznych nr 113–126 z dnia 7 lipca 2014 r.

wezwania, oraz mogą odbierać zeznania ([112]). Chociaż Inspektorzy Generalni mogą wydawać jedynie niewiążące zalecenia dotyczące działań naprawczych, ich sprawozdania, m.in. na temat działań następczych (lub braku takich działań), są podawane do publicznej wiadomości, a ponadto wysyłane do Kongresu, który na ich podstawie może wykonywać swoją funkcję nadzorczą ([113]).

(98) Ponadto *Radzie Nadzoru nad Prywatnością i Wolnościami Obywatelskimi*, będącej niezależną agencją ([114]) w strukturze władzy wykonawczej, na którą składa się pięcioosobowa Rada reprezentująca obie partie ([115]), powołana na okres sześciu lat przez Prezydenta za zgodą Senatu, powierzono obowiązki w obszarze kształtowania i wdrażania polityki walki z terroryzmem, aby zapewnić ochronę prywatności i wolności obywatelskich. W swoim przeglądzie działalności Wspólnoty Wywiadowczej 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. Rada otrzymuje sprawozdania od urzędników ds. wolności obywatelskich i prywatności z szeregu departamentów/agencji federalnych ([116]), może wydawać zalecenia skierowane do tych urzędników i regularnie sporządza sprawozdania dla komisji Kongresu i dla Prezydenta ([117]). Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi jest również zobowiązana – działając w zakresie przysługujących jej uprawnień – do przygotowania sprawozdania z wdrażania dyrektywy politycznej Prezydenta nr 28.

(99) Uzupełnieniem wspomnianych mechanizmów nadzoru jest *Rada Nadzoru nad Służbami Wywiadowczymi* ustanowiona w ramach prezydenckiej Rady Konsultacyjnej ds. Wywiadu i odpowiedzialna za monitorowanie przestrzegania przepisów konstytucji i wszystkich mających zastosowanie przepisów przez amerykańskie organy wywiadowcze.

(100) Aby usprawnić działania w tym obszarze, zachęca się jednostki Wspólnoty Wywiadowczej do opracowania systemów informatycznych zapewniających możliwość monitorowania, rejestrowania i przeprowadzania przeglądu zapytań lub korzystania z innych metod wyszukiwania danych osobowych ([118]). Organy ds. nadzoru i monitorowania zgodności będą okresowo kontrolowały praktyki stosowane przez jednostki Wspólnoty Wywiadowczej w celu zapewnieniu ochrony danych osobowych pochodzących z rozpoznania radioelektronicznego oraz przestrzeganie tych procedur przez te jednostki ([119]).

(101) Opisanym funkcjom nadzorczym towarzyszą ponadto dodatkowe rozbudowane wymogi w zakresie sprawozdawczości w odniesieniu do nieprzestrzegania zasad. W szczególności procedury stosowane przez agencje muszą zapewniać niezwłoczne zgłoszenie poważnego problemu związanego z przestrzeganiem zasad w odniesieniu do danych osobowych dowolnej osoby – niezależnie od jej narodowości – gromadzonych w drodze rozpoznania radioelektronicznego kierownikowi jednostki Wspólnoty Wywiadowczej, który z kolei powiadomi o tym fakcie Dyrektora Krajowych Służb Wywiadowczych, który – zgodnie z dyrektywą polityczną Prezydenta nr 28 – ustali, czy w danym przypadku zachodzi konieczność podjęcia jakichkolwiek działań naprawczych ([120]). Ponadto zgodnie z rozporządzeniem wykonawczym nr 12333 wszystkie jednostki Wspólnoty Wywiadowczej są zobowiązane zgłaszać Radzie Nadzoru nad Służbami Wywiadowczymi wszelkie przypadki nieprzestrzegania zasad ([121]). Opisane mechanizmy zapewniają rozwiązanie zaistniałego problemu na najwyższym szczeblu

([112]) Zob. ustawa o Inspektorze Generalnym z 1978 r., § 6.

([113]) Zob. oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 7. Zob. również ustawa o Inspektorze Generalnym z 1978 r., § 4 ust. 5 i § 5. Zgodnie z sekcją 405 lit. b) pkt 3 i 4 ustawy o autoryzacji działań wywiadowczych na rok budżetowy 2010, Zbiór ustaw publicznych nr 111–259 z dnia 7 października 2010 r., Inspektor Generalny Wspólnoty Wywiadowczej przekazuje Dyrektorowi Krajowych Służb Wywiadowczych i Kongresowi informacje na temat konieczności podjęcia działań naprawczych oraz na temat postępów w realizacji tych działań.

([114]) Zgodnie z oceną krajowych organów ochrony danych Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi „wykazała się w przeszłości swoją niezależnością". Zob. opinia 01/2016 Grupy Roboczej Art. 29 dotycząca projektu decyzji w sprawie odpowiedniej ochrony danych osobowych w ramach Tarczy Prywatności UE-USA (przyjęta w dniu 13 kwietnia 2016 r.), s. 42.

([115]) Ponadto w Radzie Nadzoru nad Prywatnością i Wolnościami Obywatelskimi zatrudnionych jest na stałe około 20 pracowników. Zob. https://www.pclob.gov/about-us/staff.html.

([116]) Należy wśród nich wymienić przynajmniej Departament Sprawiedliwości, Departament Obrony, Departament Bezpieczeństwa Krajowego, Dyrektora Krajowych Służb Wywiadowczych i Centralną Agencję Wywiadowczą, a także wszelkie inne departamenty, agencje lub jednostki struktury władzy wykonawczej wskazane jako właściwe przez Radę Nadzoru nad Prywatnością i Wolnościami Obywatelskimi.

([117]) Zob. tytuł 42 § 2000ee U.S.C. Zob. również pismo dotyczące urzędu Rzecznika (załącznik III), sekcja 6 lit. b) ppkt (iv). Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi jest m.in. zobowiązana do informowania, gdy władza wykonawcza agencji odmówi stosowania się do jej rad.

([118]) Urząd Dyrektora Krajowych Służb Wywiadowczych, Ochrona danych osobowych wszystkich osób: sprawozdanie z postępu prac nad opracowywaniem i wdrażaniem procedur przewidzianych w dyrektywie politycznej Prezydenta nr 28, s. 7–8.

([119]) Tamże s. 8. Zob. również oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 9.

([120]) Urząd Dyrektora Krajowych Służb Wywiadowczych, Ochrona danych osobowych wszystkich osób: Sprawozdanie z postępu prac nad opracowywaniem i wdrażaniem procedur przewidzianych w dyrektywie politycznej Prezydenta nr 28, s. 7. Zob. np. Agencja Bezpieczeństwa Narodowego, Procedury przewidziane w sekcji 4 dyrektywy politycznej Prezydenta nr 28 z dnia 12 stycznia 2015 r., sekcja 7.3, sekcja 8.7 lit. c) i d); Federalne Biuro Śledcze, Strategie polityczne i procedury przewidziane w dyrektywie politycznej Prezydenta nr 28, sekcja III pkt A ust. 4, sekcja III pkt B ust. 4; CIA, Działalność w zakresie rozpoznania radioelektronicznego, s. 6 (Zgodność) i s. 8 (Obowiązki).

([121]) Zob. rozporządzenie wykonawcze 12333, sekcja 1.6 lit. c).

w ramach Wspólnoty Wywiadowczej. Jeżeli problem taki dotyczy osoby niebędącej obywatelem ani rezydentem Stanów Zjednoczonych, Dyrektor Krajowych Służb Wywiadowczych – działając w porozumieniu z Sekretarzem Stanu i dyrektorem zgłaszającego departamentu lub agencji – ustala, czy należy podjąć kroki w celu powiadomienia odpowiedniego rządu zagranicznego zgodnie z przepisami w zakresie ochrony źródeł informacji i metod prowadzenia działalności oraz ochrony pracowników Stanów Zjednoczonych ([122]).

(102) Po drugie, niezależnie od opisanych powyżej mechanizmów nadzoru funkcjonujących w strukturze władzy wykonawczej, Kongres Stanów Zjednoczonych, a w szczególności *Komisje ds. Wywiadu i Sprawiedliwości w Izbie Reprezentantów i w Senacie*, jest zobowiązany do sprawowania nadzoru nad wszystkimi działaniami w obszarze wywiadu zagranicznego, uwzględniając prowadzoną przez Stany Zjednoczone działalność w obszarze rozpoznania radioelektronicznego. 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" ([123]). 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" ([124]). Członkowie tych komisji są uprawnieni do uzyskania dostępu do informacji niejawnych oraz do zapoznania się z metodami i programami wywiadowczymi ([125]).

(103) W późniejszych ustawach rozszerzono i udoskonalono wymagania sprawozdawcze, zarówno jeżeli chodzi o jednostki Wspólnoty Wywiadowczej, jak i o odpowiednich Inspektorów Generalnych i Prokuratora Generalnego. Na przykład zgodnie z ustawą o kontroli wywiadu Prokurator Generalny jest zobowiązany do przekazywania Komisjom ds. Wywiadu i Sprawiedliwości w Senacie i Izbie Reprezentantów „pełnych informacji" na temat działań podejmowanych przez rząd zgodnie z określonymi sekcjami ustawy o kontroli wywiadu ([126]). Na mocy ustawy o kontroli wywiadu rząd został również zobowiązany do przekazywania komisjom Kongresu kopii „wszystkich orzeczeń, zarządzeń lub opinii Sądu ds. Inwigilacji Obcych Wywiadów lub Sądu Apelacyjnego ds. Inwigilacji Obcych Wywiadów, w których dokonano istotnej interpretacji przepisów ustawy o kontroli wywiadu lub w których dokonano wykładni tych przepisów". W szczególności jeżeli chodzi o sprawowanie nadzoru, o którym mowa w sekcji 702 ustawy o kontroli wywiadu, taki nadzór sprawuje się za pośrednictwem sprawozdań, które zgodnie z przepisami ustawy należy przekazywać Komisjom ds. Wywiadu i 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 w szczególności sprawozdania Departamentu Sprawiedliwości i Urzędu Dyrektora Krajowych Służb Wywiadowczych dotyczące przestrzegania zasad oraz opis wszelkich przypadków nieprzestrzegania zasad ([127]), a także odrębną ocenę półroczną przeprowadzaną przez Prokuratora Generalnego i przygotowywany przez Departament Sprawiedliwości dokument dotyczący zgodności z procedurami ukierunkowywania i minimalizacji, uwzględniając zgodność z procedurami służącymi zapewnieniu gromadzenia danych wyłącznie w przypadku, gdy służy to realizacji ważnego celu związanego z wywiadem zagranicznym ([128]). Kongres otrzymuje również sprawozdania przekazywane przez Inspektorów Generalnych, którzy są uprawnieni do oceniania zgodności agencji z procedurami ukierunkowywania i minimalizacji oraz z wytycznymi Prokuratora Generalnego.

(104) Zgodnie z amerykańską ustawą o wolności z 2015 r. rząd Stanów Zjednoczonych musi co roku ujawniać Kongresowi (i społeczeństwu) liczbę nakazów i dyrektyw na mocy ustawy o kontroli wywiadu, o które się ubiegano i które otrzymano, a także szacunki dotyczące m.in. liczby obywateli i rezydentów amerykańskich oraz liczby osób niebędących obywatelami ani rezydentami amerykańskimi objętych nadzorem ([129]). W ustawie przewidziano również dodatkowy wymóg podawania do wiadomości publicznej liczby wydanych wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego, ponowne w odniesieniu do obywateli i rezydentów amerykańskich i osób niebędących obywatelami ani rezydentami amerykańskimi (zapewniając jednocześnie odbiorcom nakazów i certyfikatów wydanych na mocy ustawy o kontroli wywiadu oraz wezwań do

([122]) Dyrektywa polityczna Prezydenta nr 28, sekcja 4 lit. a) ppkt (iv).
([123]) Zob. sekcja 501 lit. a) pkt 1 (tytuł 50 § 413 lit. a) pkt 1 U.S.C.). W przywołanym punkcie ustanowiono ogólne wymogi dotyczące nadzoru Kongresu nad kwestiami związanymi z bezpieczeństwem narodowym.
([124]) Zob. sekcja 501 lit. b) (tytuł 50 § 413 lit. b) U.S.C.).
([125]) Por. sekcja 501 lit. d) (tytuł 50 § 413 lit. d) U.S.C.).
([126]) Zob. tytuł 50 § 1808, 1846, 1862, 1871 i 1881f U.S.C.
([127]) Zob. tytuł 50 § 1881f U.S.C.
([128]) Zob. tytuł 50 § 1881a lit. l) pkt 1 U.S.C.
([129]) Zob. amerykańska ustawa o wolności z 2015 r., Zbiór ustaw publicznych nr 114-23, sekcja 602 lit. a). 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. Inwigilacji Obcych Wywiadów lub przez Sąd Apelacyjny ds. Inwigilacji Obcych Wywiadów (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 identyfikującego«, i – zgodnie z wynikami tego przeglądu – podaje takie orzeczenie, zarządzenie lub opinię do wiadomości publicznej w jak najszerszym zakresie".

przedstawienia informacji do celów bezpieczeństwa możliwość opublikowania – w określonych przypadkach – sprawozdań z przejrzystości) ([130]).

(105) Po trzecie, w ramach działalności wywiadowczej prowadzonej przez amerykańskie organy publiczne zgodnie z ustawą o kontroli wywiadu dopuszcza się możliwość przeprowadzenia przeglądu, a w niektórych przypadkach wcześniejszego zatwierdzenia środków przez *Sąd ds. Inwigilacji Obcych Wywiadów* ([131]), tj. niezależny sąd ([132]), którego orzeczenia można zaskarżyć przed Sądem Odwoławczym ds. Inwigilacji Obcych Wywiadów ([133]), a ostatecznie przed Sądem Najwyższym Stanów Zjednoczonych ([134]). W przypadku wcześniejszego zatwierdzenia środków organy wnioskujące (Federalne Biuro Śledcze, Agencja Bezpieczeństwa Narodowego, Centralne Agencje Wywiadowcze itp.) będą zobowiązane do przekazania projektu wniosku prawnikom Departamentu Bezpieczeństwa Narodowego w Departamencie Sprawiedliwości, którzy zbadają ten projekt i – w stosownych przypadkach – zwrócą się o przekazanie dodatkowych informacji ([135]). Po zakończeniu prac nad wnioskiem będzie on musiał zostać zatwierdzony przez Prokuratora Generalnego, Zastępcę Prokuratora Generalnego lub Asystenta Prokuratora Generalnego ds. Bezpieczeństwa Narodowego ([136]). Następnie Departament Sprawiedliwości przekaże wniosek Sądowi ds. Inwigilacji Obcych Wywiadów, który podda go ocenie i podejmie wstępną decyzję w kwestii dalszych działań ([137]). W przypadku zorganizowania rozprawy Sąd ds. Inwigilacji Obcych Wywiadów jest uprawniony do przyjmowania zeznań, uwzględniając opinie biegłych ([138]).

(106) Sąd ds. Inwigilacji Obcych Wywiadów (oraz Sąd Odwoławczy ds. Inwigilacji Obcych Wywiadów) korzysta ze wsparcia stałego zespołu składającego się z pięciu ekspertów w dziedzinie bezpieczeństwa narodowego i wolności obywatelskich ([139]). 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 ([140]). 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* ([141]).

([130]) Sekcja 602 lit. a) i sekcja 603 lit. a) amerykańskiej ustawy o wolności.

([131]) W przypadku niektórych rodzajów inwigilacji uprawnienie do rozpatrzenia wniosków i wydania zarządzeń może przysługiwać amerykańskiemu sędziemu pokoju powołanemu publicznie przez Prezesa Sądu Najwyższego Stanów Zjednoczonych.

([132]) W Sądzie ds. Inwigilacji Obcych Wywiadów zasiada jedenastu sędziów powołanych 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. Inwigilacji Obcych Wywiadów 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. sekcja 103 ustawy o kontroli wywiadu (tytuł 50 § 1803 lit. a) U.S.C.); sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 215, s. 174–187. 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. sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 215, s. 178; Pismo sędziego Reggiego B. Waltona, przewodniczącego składu sędziowskiego w Sądzie Stanów Zjednoczonych ds. Inwigilacji Obcych Wywiadów, do senatora Patricka J. Leathyego, przewodniczącego Komisji Sądownictwa w Senacie Stanów Zjednoczonych (z dnia 29 lipca 2013 r.) („pismo Waltona"), s. 2–3.

([133]) W Sądzie Odwoławczym ds. Inwigilacji Obcych Wywiadów zasiada trzech sędziów powołanych przez prezesa Sądu Najwyższego Stanów Zjednoczonych, pochodzących z amerykańskich sądów dystryktowych lub sądów apelacyjnych, którzy sprawują swój urząd w ramach naprzemiennych siedmioletnich kadencji. Zob. sekcja 103 ustawy o kontroli wywiadu (tytuł 50 § 1803 lit. b) U.S.C.).

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

([135]) Na przykład dodatkowe szczegółowe informacje faktograficzne na temat obiektu inwigilacji, informacje techniczne dotyczące metody inwigilacji lub gwarancje dotyczące sposobu wykorzystywania i rozpowszechniania pozyskanych informacji. Zob. sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 215, s. 177.

([136]) Tytuł 50 § 1804 lit. a) i § 1801 lit. g) U.S.C.

([137]) Sąd ds. Inwigilacji Obcych Wywiadów może zatwierdzić wniosek, zwrócić się o przekazanie dodatkowych informacji, stwierdzić konieczność przeprowadzenia wysłuchania lub wskazać, że wniosek w jego obecnym kształcie może zostać odrzucony. Na podstawie tych wstępnych ustaleń rząd przygotowuje ostateczną wersję wniosku. W przypadku uwzględnienia wstępnych uwag sędziego ostateczna wersja wniosku może istotnie różnić się od jego pierwotnej wersji. Choć Sąd ds. Inwigilacji Obcych Wywiadów zatwierdza dużą liczbę ostatecznych wersji wniosków, znaczną część tych wniosków stanowią wnioski, w których wprowadzono istotne zmiany w porównaniu z ich pierwotnym brzmieniem – np. w okresie od lipca do września 2013 r. dotyczyło to 24 % zatwierdzonych wniosków. Zob. sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 215, s. 179; pismo Waltona, s. 3.

([138]) Sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 215, s. 179, nr 619.

([139]) Tytuł 50 § 1803 lit. i) pkt 1 i tytuł 50 § 1803 lit. i) pkt 3 ppkt A U.S.C. W tych nowych przepisach zawarto zalecenia Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące utworzenia zespołu ekspertów ds. prywatności i wolności obywatelskich, który będzie mógł pełnić funkcję *amicus curiae* i dostarczać sądowi argumentów prawnych przyczyniających się do zapewnienia lepszej ochrony prywatności i wolności obywatelskich. Zob. sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 215, s. 183–187.

([140]) Tytuł 50 § 1803 lit. i) pkt 2 ppkt A U.S.C. Zgodnie z informacjami przekazanymi przez Urząd Dyrektora Krajowych Służb Wywiadowczych dokonano już tego rodzaju powołań. Zob. reforma systemu rozpoznania radioelektronicznego, sprawozdanie okresowe za 2016 r.

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

(107) Istnieją pewne różnice, jeżeli chodzi o nadzór Sądu ds. Inwigilacji Obcych Wywiadów nad udzielaniem dwóch typów zezwoleń na prowadzenie inwigilacji, przewidziane w ustawie o kontroli wywiadu, które mają największe znaczenie dla przekazywania danych w ramach Tarczy Prywatności UE-USA.

(108) Zgodnie z sekcją 501 ustawy o kontroli wywiadu ([142]), w której dopuszcza się możliwość gromadzenia „wszelkich przedmiotów materialnych (uwzględniając księgi, rejestry, opracowania, dokumenty i inne przedmioty)", wniosek skierowany do Sądu ds. Inwigilacji Obcych Wywiadów musi zawierać wykaz okoliczności faktycznych świadczących o tym, że istnieją uzasadnione przesłanki, by przypuszczać, że żądane przedmioty materialne mają istotne znaczenie w kontekście prowadzonego zgodnie z prawem dochodzenia (innego niż ocena zagrożenia) w celu pozyskaniu zagranicznych informacji wywiadowczych, które nie dotyczą obywatela ani rezydenta Stanów Zjednoczonych, lub zapewnienia ochrony przed terroryzmem międzynarodowym lub tajnymi działaniami wywiadowczymi. Ponadto we wniosku należy zawrzeć wykaz procedur ograniczających, przyjętych przez Prokuratora Generalnego do celów zatrzymywania i rozpowszechniania gromadzonych danych wywiadowczych ([143]).

(109) Natomiast zgodnie z sekcją 702 ustawy o kontroli wywiadu ([144]) Sąd ds. Inwigilacji Obcych Wywiadów nie jest uprawniony do zatwierdzania poszczególnych środków nadzoru; może jednak zatwierdzać programy nadzoru (takie jak PRISM, UPSTREAM) w oparciu o roczne certyfikacje przygotowywane przez Prokuratora Generalnego i Dyrektora Krajowych Służb Wywiadowczych. Zgodnie z przepisami sekcji 702 ustawy o kontroli wywiadu dopuszcza się możliwość namierzania osób, co do których istnieje uzasadnione podejrzenie, że przebywają poza terytorium Stanów Zjednoczonych w celu pozyskiwania zagranicznych informacji wywiadowczych ([145]). Agencja Bezpieczeństwa Narodowego przeprowadza takie namierzanie w dwóch etapach: w pierwszej kolejności analitycy Agencji Bezpieczeństwa Narodowego identyfikują osoby niebędące obywatelami ani rezydentami Stanów Zjednoczonych przebywające za granicą, których objęcie nadzorem – w ocenie analityków – umożliwi pozyskanie stosownych zagranicznych informacji wywiadowczych określonych w certyfikacji. Następnie, po zidentyfikowaniu tych poszczególnych osób i zatwierdzeniu ich namierzania w ramach rozbudowanego mechanizmu przeglądu wykorzystywanego przez Agencję Bezpieczeństwa Narodowego ([146]) przydziela się (tj. opracowuje i wdraża) selektory identyfikujące narzędzia komunikacyjne (takie jak adresy e-mail), które są wykorzystywane przez namierzane osoby ([147]). Jak już wskazano, certyfikacje, które mają zostać zatwierdzone przez Sąd ds. Inwigilacji Obcych Wywiadów, nie zawierają żadnych informacji na temat poszczególnych osób, które mają być namierzane – służą one identyfikowaniu kategorii zagranicznych informacji wywiadowczych ([148]). Choć Sąd ds. Inwigilacji Obcych Wywiadów nie ocenia – na podstawie uzasadnionego podejrzenia lub innej normy – czy osoby fizyczne są odpowiednio namierzane do celów pozyskiwania zagranicznych informacji wywiadowczych ([149]), zakres kontroli przeprowadzanej przez ten sąd obejmuje również warunek, zgodnie z którym „istotnym celem gromadzenia informacji jest pozyskanie zagranicznych informacji wywiadowczych" ([150]). Zgodnie z sekcją 702 ustawy o kontroli wywiadu Agencja Bezpieczeństwa Narodowego może gromadzić wiadomości osób niebędących obywatelami ani rezydentami Stanów Zjednoczonych, które przebywają poza terytorium Stanów Zjednoczonych i co do których istnieje uzasadnione podejrzenie, że korzystają z określonego środka komunikacji w celu przekazywania zagranicznych informacji wywiadowczych (np. informacje związane z terroryzmem międzynarodowym, rozprzestrzenianiem broni jądrowej lub wrogimi działaniami w obszarze cyberprzestępczości). Ustalenia w tej kwestii są poddawane kontroli sądowej ([151]). Certyfikacje również muszą zapewniać możliwość stosowania procedur ukierunkowywania i minimalizacji ([152]). Prokurator Generalny i Dyrektor Krajowych Służb Wywiadowczych weryfikują zgodność z zasadami, a agencje są zobowiązane do zgłaszania Sądowi ds. Inwigilacji Obcych

([142]) Tytuł 50 § 1861 U.S.C.
([143]) Tytuł 50 § 1861 lit. b) U.S.C.
([144]) Tytuł 50 § 1881 U.S.C.
([145]) Tytuł 50 § 1881a lit. a) U.S.C.
([146]) Sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 702, s. 46.
([147]) Tytuł 50 § 1881a lit. h) U.S.C.
([148]) Tytuł 50 § 1881a lit. g) U.S.C. Według Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi kategorie te dotyczyły do tej pory głównie międzynarodowego terroryzmu i zagadnień takich jak nabywanie broni masowego rażenia. Zob. sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 702, s. 25.
([149]) Sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 702, s. 27.
([150]) Tytuł 50 § 1881a U.S.C.
([151]) „Liberty and Security in a Changing World", sprawozdanie i zalecenia prezydenckiej grupy oceniającej ds. wywiadu i technologii komunikacyjnych z dnia 12 grudnia 2013 r., s. 152.
([152]) Tytuł 50 § 1881a lit. i) U.S.C.

Wywiadów ([153]) (a także Kongresowi i prezydenckiej Radzie Nadzoru nad Służbami Wywiadowczymi) wszelkich przypadków nieprzestrzegania zasad – na tej podstawie Sąd może wprowadzić zmiany w upoważnieniu ([154]).

(110) Co więcej, aby zwiększyć efektywność nadzoru prowadzonego przez Sąd ds. Inwigilacji Obcych Wywiadów, administracja Stanów Zjednoczonych zgodziła się wdrożyć zalecenie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące dostarczania Sądowi ds. Inwigilacji Obcych Wywiadów dokumentacji decyzji odnoszących się do sekcji 702, w tym losowych fragmentów formularzy zadaniowych, aby umożliwić Sądowi ds. Inwigilacji Obcych Wywiadów ocenę, w jakim stopniu praktycznie zrealizowano wymogi stawiane wobec wywiadu zagranicznego ([155]). Jednocześnie administracja Stanów Zjednoczonych przyjęła i wprowadziła środki służące dokonaniu przeglądu procedur Agencji Bezpieczeństwa Narodowego w zakresie ukierunkowania, aby lepiej dokumentować powody, dla których wywiad zagraniczny przyjął decyzje o ukierunkowaniu gromadzenia danych ([156]).

Dochodzenie roszczeń przez osoby fizyczne

(111) Osoby z UE, których dane dotyczą, mogą skorzystać z licznych możliwości dostępnych w prawie amerykańskim, jeżeli mają obawy co do tego, czy ich dane osobowe były przetwarzane (gromadzone, udostępniane itp.) przez jednostki Wspólnoty Wywiadowczej USA, a jeżeli miało to miejsce, czy przestrzegano ograniczeń mających zastosowanie na mocy prawa amerykańskiego. Odnoszą się one zasadniczo do trzech obszarów: ingerencji na mocy ustawy o kontroli wywiadu; bezprawnego, celowego uzyskania dostępu do danych osobowych przez urzędników rządowych; i dostępu do informacji na mocy ustawy o dostępie do informacji publicznej ([157]).

(112) Po pierwsze, w ustawie o kontroli wywiadu przewidziano liczne środki ochrony prawnej dla osób niebędących obywatelami ani rezydentami USA, dzięki którym mogą zakwestionować prowadzenie bezprawnego dozoru elektronicznego ([158]). Obejmuje to 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 ([159]); pozwania amerykańskich urzędników rządowych działających we własnym imieniu („pod przykrywką prawa") o odszkodowanie pieniężne ([160]); 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 ([161]).

(113) Po drugie, rząd USA przedstawił Komisji liczne dodatkowe możliwości, z których mogą skorzystać osoby z UE, których dane dotyczą, aby uzyskać ochronę prawną przeciwko urzędnikom rządowym ze względu na bezprawny

([153]) Zgodnie z zasadą 13 lit. b) regulaminu Sądu ds. Inwigilacji Obcych Wywiadów rząd ma obowiązek wystosować pisemne powiadomienie do Sądu niezwłocznie po ustaleniu, że jakiekolwiek upoważnienie lub zatwierdzenie przyznane przez Sąd zostało wykorzystane w sposób niezgodny z upoważnieniem lub zatwierdzeniem Sądu lub z mającym zastosowanie prawem. Zgodnie z tą samą zasadą rząd ma również obowiązek powiadomić Sąd na piśmie o sytuacji faktycznej i okolicznościach mających znaczenie dla takiego nieprzestrzegania zasad. Zazwyczaj rząd przedkłada ostateczne powiadomienie na podstawie zasady 13 lit. a) po ustaleniu istotnych okoliczności faktycznych i zniszczeniu wszelkich danych zgromadzonych w nieuprawniony sposób. Zob. pismo Waltona, s. 10.

([154]) Tytuł 50 § 1881 lit. l) U.S.C. Zob. również sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 702, s. 66–76. Biuro Wolności Obywatelskich i Ochrony Prywatności Agencji Bezpieczeństwa Narodowego, sprawozdanie dotyczące wdrażania sekcji 702 ustawy o kontroli wywiadu przez Agencję Bezpieczeństwa Narodowego z dnia 16 kwietnia 2014 r. Gromadzenie danych osobowych do celów wywiadowczych na podstawie sekcji 702 ustawy o kontroli wywiadu podlega zarówno wewnętrznemu, jak i zewnętrznemu nadzorowi w ramach uprawnień władzy wykonawczej. Nadzór wewnętrzny obejmuje między innymi wewnętrzne programy zgodności służące ocenie i nadzorowi przestrzegania procedur ukierunkowania i minimalizacji; zgłaszanie przypadków nieprzestrzegania zasad, zarówno wewnętrznych, jak i zewnętrznych, Urzędowi Dyrektora Krajowych Służb Wywiadowczych, Departamentowi Sprawiedliwości, Kongresowi i Sądowi ds. Inwigilacji Obcych Wywiadów; oraz coroczne przeglądy przedkładane tym samym podmiotom. Jeżeli chodzi o nadzór zewnętrzny, składa się on głównie z przeglądów ukierunkowania i minimalizacji przeprowadzanych przez Urząd Dyrektora Krajowych Służb Wywiadowczych, Departament Sprawiedliwości i Inspektorów Generalnych, którzy z kolei przedkładają sprawozdania Kongresowi i Sądowi ds. Inwigilacji Obcych Wywiadów, w tym informacje na temat przypadków nieprzestrzegania zasad. Przypadki poważnego nieprzestrzegania zasad należy bezzwłocznie zgłosić Sądowi ds. Inwigilacji Obcych Wywiadów, natomiast inne przypadki należy zgłaszać co kwartał. Zob. sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 702, s. 66–77.

([155]) Sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi w sprawie oceny zaleceń z dnia 29 stycznia 2015 r., s. 20.

([156]) Sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi w sprawie oceny zaleceń z dnia 29 stycznia 2015 r., s. 16.

([157]) Ponadto w § 10 ustawy o procedurach dotyczących informacji niejawnych przewidziano, że w każdym postępowaniu karnym, w którym Stany Zjednoczone muszą ustalić, czy materiał dowodowy stanowi informacje niejawne (np. jako że wymaga ochrony przed nieuprawnionym ujawnieniem ze względów bezpieczeństwa narodowego), Stany Zjednoczone informują oskarżonego o częściach materiału dowodowego, na których – zgodnie z rozsądnymi przewidywaniami – będą się opierać, aby ustalić, jaka część oskarżenia stanowi informacje niejawne.

([158]) Zob. oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 16.

([159]) Tytuł 18 § 2712 U.S.C.

([160]) Tytuł 50 § 1810 U.S.C.

([161]) Tytuł 50 § 1806 U.S.C.

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 ([162]); ustawa o prywatności w łączności elektronicznej ([163]); oraz ustawa o prawie do prywatności w kwestiach finansowych ([164])). Wszystkie te podstawy roszczeń 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) ([165]). W ustawie o postępowaniu administracyjnym przewiduje się bardziej ogólną możliwość dochodzenia roszczeń (tytuł 5 § 702 U.S.C.), 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. 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" ([166]).

(114) Ponadto rząd USA wskazał ustawę o dostępie do informacji publicznej jako środek, z którego osoby niebędące obywatelami ani rezydentami USA mogą skorzystać, aby uzyskać dostęp do istniejących rejestrów agencji federalnej, w tym jeżeli rejestry te zawierają dane osobowe tej osoby fizycznej ([167]). Mając na uwadze główny obszar regulowany ustawą o dostępie do informacji publicznej, nie daje ona możliwości skorzystania ze środków ochrony prawnej przez osobę fizyczną w przypadku samej ingerencji w dane osobowe, mimo że mogłaby zasadniczo umożliwić osobom fizycznym uzyskanie dostępu do odpowiednich informacji przechowywanych przez krajowe agencje wywiadowcze. Nawet w tym kontekście możliwości wydają się ograniczone, ponieważ 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 ([168]). W związku z tym powołanie się przez krajowe agencje wywiadowcze na takie wyjątki może być zakwestionowane przez osoby fizyczne poprzez zastosowanie administracyjnych i sądowych środków prawnych.

(115) Chociaż osoby fizyczne, w tym osoby z UE, których dane dotyczą, mają zatem liczne możliwości dochodzenia roszczeń, jeżeli zostały objęte bezprawnym dozorem (elektronicznym) do celów bezpieczeństwa narodowego, równie oczywiste jest, że nie uwzględniono przynajmniej niektórych podstaw prawnych, na jakie mogą powołać się amerykańskie organy wywiadowcze (np. rozporządzenie wykonawcze nr 12333). Co więcej, nawet jeżeli osoby niebędące obywatelami ani rezydentami USA mogą zasadniczo korzystać z sądowych środków odwoławczych, np. w przypadku nadzoru na mocy ustawy o kontroli wywiadu, dostępne podstawy wszczęcia powództwa są jednak ograniczone ([169]), a roszczenia zgłaszane przez osoby fizyczne (w tym osoby będące obywatelami lub rezydentami USA) zostaną uznane za niedopuszczalne, jeżeli osoby te nie mogą wykazać interesu prawnego ([170]), co ogranicza dostęp do sądów powszechnych ([171]).

(116) Aby zapewnić dodatkowe możliwości ochrony prawnej dostępne dla wszystkich osób z UE, których dane dotyczą, rząd USA podjął decyzję o utworzeniu nowego urzędu Rzecznika, jak wskazano w piśmie sekretarza stanu USA do Komisji, które znajduje się w załączniku III do niniejszej decyzji. Ten urząd opiera się na wyznaczeniu na podstawie dyrektywy politycznej Prezydenta nr 28 starszego koordynatora (na poziomie podsekretarza) w Departamencie Stanu jako osobę odpowiedzialną za kontakty dla rządów zagranicznych, aby mogły one wyrazić obawy dotyczące działań USA w zakresie rozpoznania radioelektronicznego; funkcja ta wykracza jednak daleko poza pierwotny zakres.

([162]) Tytuł 18 § 1030 U.S.C.
([163]) Tytuł 18 § 2701–2712 U.S.C.
([164]) Tytuł 12 § 3417 U.S.C.
([165]) Oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 17.
([166]) Tytuł 5 § 706 ust. 2 pkt A U.S.C.
([167]) Tytuł 5 § 552 U.S.C. Podobne przepisy obowiązują na szczeblu stanowym.
([168]) 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 przeciwko CIA, 710 F.3d 422 (D.C. Cir. 2014).
([169]) Zob. oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI), s. 16. Zgodnie z przedstawionymi wyjaśnieniami, aby móc skorzystać z dostępnych podstaw wszczęcia powództwa, musi wystąpić *szkoda* (tytuł 18 § 2712 U.S.C.; tytuł 50 § 1810 U.S.C.) lub należy wykazać, że *rząd zamierza wykorzystać lub ujawnić informacje* uzyskane lub pochodzące z dozoru elektronicznego danej osoby przeciwko tej osobie *w postępowaniu sądowym lub administracyjnym* w Stanach Zjednoczonych (tytuł 50 § 1806 U.S.C.). Jak Trybunał Sprawiedliwości jednak wielokrotnie podkreślał, dla stwierdzenia ingerencji w podstawowe prawo do prywatności nie ma znaczenia, czy dana osoba doświadczyła jakichkolwiek negatywnych konsekwencji w związku z tą ingerencją. Zob. wyrok w sprawie Schrems, pkt 89 z dalszymi odniesieniami.
([170]) To kryterium dopuszczalności wywodzi się z wymogu istnienia „sprawy lub sporu" (ang. *case or controversy*) z art. 3 konstytucji USA.
([171]) Zob. wyrok w sprawie Clapper przeciwko Amnesty International USA, Zbiór orzeczeń Sądu Najwyższego (S. Ct.) t. 133 s. 1138, 1144 (2013). Jeżeli chodzi o korzystanie z wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego, w amerykańskiej ustawie o wolności (sekcje 502 lit. f)–503) przewidziano, że należy dokonywać okresowego przeglądu wymogów nieujawniania informacji i że należy powiadomić *adresatów* wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego, jeżeli okoliczności faktyczne nie przemawiają już za zastosowaniem wymogu nieujawniania informacji (zob. oświadczenia Urzędu Dyrektora Krajowych Służb Wywiadowczych (załącznik VI) s. 13). Nie gwarantuje to jednak, że osoba z UE, której dane dotyczą, jest świadoma, iż wszczęto wobec niej dochodzenie.

(117) W szczególności – zgodnie z zobowiązaniami rządu USA – Rzecznik zapewni, aby indywidualne skargi zostały należycie zbadane i rozstrzygnięte oraz aby osoby fizyczne otrzymały niezależne potwierdzenie, że działano zgodnie z prawem amerykańskim lub że – w przypadku naruszenia takich przepisów – problem ten został rozwiązany ([172]). Urząd obejmuje również „Rzecznika ds. Tarczy Prywatności" w randze podsekretarza i dodatkowy personel oraz inne organy nadzorcze właściwe do nadzorowania różnych jednostek Wspólnoty Wywiadowczej, na współpracy z którymi będzie polegał Rzecznik ds. Tarczy Prywatności podczas rozpatrywania skarg. W szczególności, jeżeli wniosek danej osoby fizycznej dotyczy zgodności nadzoru z prawem Stanów Zjednoczonych, Rzecznik ds. Tarczy Prywatności będzie mógł polegać na niezależnych organach nadzorczych posiadających uprawnienia dochodzeniowe (takich jak Inspektorzy Generalni lub Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi). W każdym przypadku sekretarz stanu gwarantuje, że Rzecznik będzie posiadał środki umożliwiające zapewnienie, aby jego odpowiedź na wnioski osób fizycznych opierała się na wszystkich niezbędnych informacjach.

(118) Dzięki takiej złożonej strukturze urząd Rzecznika gwarantuje niezależny nadzór i środki ochrony prawnej dla osób fizycznych. Co więcej, współpraca z innymi organami nadzoru zapewnia dostęp do niezbędnej wiedzy fachowej. Ponadto, nakładając na Rzecznika ds. Tarczy Prywatności obowiązek potwierdzenia zgodności lub zastosowania środków zaradczych w odniesieniu do wszelkich przypadków nieprzestrzegania zasad, mechanizm odzwierciedla zobowiązanie rządu Stanów Zjednoczonych do przyjęcia i rozstrzygnięcia skarg osób fizycznych pochodzących z UE.

(119) Po pierwsze, w odróżnieniu od mechanizmu funkcjonującego wyłącznie na szczeblu międzyrządowym Rzecznik ds. Tarczy Prywatności będzie otrzymywał skargi od osób fizycznych i odpowiadał na nie. Tego rodzaju skargi można kierować do organów nadzorczych w państwach członkowskich właściwych w sprawach nadzoru nad służbami bezpieczeństwa narodowego lub przetwarzania danych osobowych przez organy publiczne, które przekażą je scentralizowanemu organowi UE, który z kolei przekieruje je do Rzecznika ds. Tarczy Prywatności ([173]). W praktyce przyniesie to korzyści osobom fizycznym pochodzącym z UE, które mogą zwrócić się do krajowego organu „w pobliżu miejsca zamieszkania" i w swoim języku ojczystym. Zadaniem takiego organu będzie wspieranie osoby fizycznej w składaniu wniosku do Rzecznika ds. Tarczy Prywatności, który to wniosek zawiera podstawowe informacje i może w związku z tym zostać uznany za „kompletny". Osoba fizyczna nie musi wykazywać, że rząd USA faktycznie pozyskał jej dane osobowe za pomocą działań w zakresie rozpoznania radioelektronicznego.

(120) Po drugie, rząd Stanów Zjednoczonych zobowiązuje się do zapewnienia, aby Rzecznik ds. Tarczy Prywatności — pełniąc swoje funkcje — mógł opierać się na współpracy z innymi istniejącymi w prawie amerykańskim mechanizmami niezależnego nadzoru i przeglądu zgodności. Niekiedy będzie to obejmowało krajowe organy wywiadowcze, w szczególności gdy wniosek należy interpretować jako dotyczący udzielenia dostępu do dokumentów na mocy ustawy o dostępie do informacji publicznej. W innych przypadkach, zwłaszcza gdy wnioski dotyczą zgodności nadzoru z prawem Stanów Zjednoczonych, tego rodzaju współpraca będzie obejmowała niezależne organy nadzoru (np. Inspektorów Generalnych) posiadające uprawnienia i odpowiedzialność w zakresie przeprowadzania gruntownego dochodzenia (w szczególności dzięki dostępowi do wszystkich istotnych dokumentów oraz uprawnieniu do żądania informacji i oświadczeń) oraz zaradzania wszelkim przypadkom nieprzestrzegania zasad ([174]). Ponadto Rzecznik ds. Tarczy Prywatności będzie mógł kierować sprawy do rozpatrzenia przez Radę Nadzoru nad Prywatnością i Wolnościami Obywatelskimi ([175]). Jeżeli jeden ze wypomnianych organów nadzorczych stwierdzi jakikolwiek przypadek nieprzestrzegania zasad, jednostka Wspólnoty Wywiadowczej (np. agencja wywiadowcza), której dotyczy ten zarzut, będzie musiała zaradzić takiemu nieprzestrzeganiu zasad, ponieważ tylko w taki sposób Rzecznik będzie mógł udzielić

([172]) Jeżeli skarżący ubiega się o uzyskanie dostępu do dokumentów będących w posiadaniu amerykańskich organów publicznych, zastosowanie mają przepisy i procedury określone w ustawie o dostępie do informacji publicznej. Obejmuje to możliwość wniesienia sądowych środków odwoławczych (zamiast prowadzenia niezależnego nadzoru) w przypadku odrzucenia wniosku, na warunkach określonych w ustawie o dostępie do informacji publicznej.

([173]) Zgodnie z sekcją 4 lit. f) pisma dotyczącego urzędu Rzecznika (załącznik III) Rzecznik ds. Tarczy Prywatności będzie kontaktował się bezpośrednio z organem rozpatrującym skargi obywateli Unii, który z kolei będzie odpowiedzialny za kontakty z osobą fizyczną składającą wniosek. Jeżeli bezpośrednia komunikacja jest częścią jednego z „podstawowych procesów", które mogą zapewnić rozwiązanie problemu, o jakie występuje wnioskodawca (np. w przypadku wniosku o udostępnienie danych na podstawie ustawy o dostępie do informacji publicznej, zob. sekcja 5), wówczas taka komunikacja będzie odbywała się zgodnie z mającymi zastosowanie procedurami.

([174]) Zob. pismo dotyczące urzędu Rzecznika (załącznik III), sekcja 2 lit. a). Zob. również motywy 0–0.

([175]) Zob. pismo dotyczące urzędu Rzecznika (załącznik III), sekcja 2 lit. c). Zgodnie z wyjaśnieniami przedstawionymi przez rząd USA Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi stale dokonuje przeglądu strategii politycznych i procedur tych organów amerykańskich, które odpowiadają za walkę z terroryzmem, a także przeglądu wdrażania tych strategii i procedur przez wspomniane organy, w celu ustalenia, czy takie działania „zapewniają odpowiednią ochronę prywatności i wolności obywatelskich oraz czy są zgodne z obowiązującymi przepisami prawa, regulacjami i polityką w zakresie prywatności i wolności obywatelskich". Rada Nadzoru otrzyma również od urzędników ds. prywatności i urzędników ds. wolności obywatelskich sprawozdania i inne informacje oraz dokona ich przeglądu, a w stosownych przypadkach przekaże im zalecenia dotyczące prowadzonych przez nich działań.

pozytywnej odpowiedzi osobie fizycznej (tj. że zaradzono ewentualnemu nieprzestrzeganiu zasad), do czego zobowiązał się rząd Stanów Zjednoczonych. Ponadto w ramach współpracy Rzecznik ds. Tarczy Prywatności będzie informowany o wynikach dochodzenia oraz będzie dysponował środkami gwarantującymi, że otrzyma wszystkie informacje niezbędne do przygotowania odpowiedzi.

(121) Ponadto Rzecznik ds. Tarczy Prywatności będzie niezależny od Wspólnoty Wywiadowczej USA, a zatem niezwiązany jej poleceniami ([176]). Ma to duże znaczenie, biorąc pod uwagę, że Rzecznik będzie musiał potwierdzić, iż (i) skarga została właściwie zbadana oraz że (ii) przestrzegano odpowiednich przepisów prawa amerykańskiego – w tym przede wszystkim ograniczeń i gwarancji opisanych w załączniku VI – lub – w przypadku nieprzestrzegania przepisów – problem ten został rozwiązany. Aby móc przedstawić takie niezależne potwierdzenie, Rzecznik ds. Tarczy Prywatności będzie musiał uzyskać wystarczające informacje na temat dochodzenia w celu przeprowadzenia oceny dokładności odpowiedzi na skargę. Ponadto sekretarz stanu zobowiązał się do zapewnienia, aby podsekretarz pełnił funkcję Rzecznika ds. Tarczy Prywatności w sposób obiektywny i wolny od jakiegokolwiek niewłaściwego wpływu, jaki mógłby zostać wywarty na udzieloną odpowiedź.

(122) Ogólnie rzecz biorąc, urząd ten zapewnia gruntowne zbadanie i rozstrzygnięcie skarg złożonych przez osoby fizyczne oraz zapewnia, aby w procesie tym, przynajmniej w dziedzinie nadzoru, uczestniczyły niezależne organy nadzorcze posiadające niezbędną wiedzę fachową i uprawnienia dochodzeniowe, a Rzecznik był w stanie pełnić swoje funkcje bez żadnego niewłaściwego, a zwłaszcza politycznego, wpływu. Ponadto osoby fizyczne będą mogły wnosić skargi bez konieczności wykazania, że są przedmiotem nadzoru, lub na podstawie samych tylko oznak sugerujących, że są przedmiotem nadzoru ([177]). W świetle powyższych okoliczności Komisja jest przekonana, że istnieją odpowiednie i skuteczne zabezpieczenia przed nadużyciami.

(123) Na podstawie powyższego Komisja stwierdza, że Stany Zjednoczone zapewniają skuteczną ochronę prawną przed ingerencją swoich organów wywiadowczych w prawa podstawowe osób, których dane są przekazywane z Unii do Stanów Zjednoczonych w ramach Tarczy Prywatności UE-USA.

(124) W tym kontekście Komisja zauważa, że Trybunał Sprawiedliwości w wyroku w sprawie Schrems stwierdził, iż „uregulowanie nieprzewidujące dla jednostek żadnej drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych nie zapewnia poszanowania zasadniczej istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 karty" ([178]). W ocenie Komisji potwierdzono, że w Stanach Zjednoczonych zapewniono takie środki ochrony prawnej, w tym poprzez wprowadzenie urzędu Rzecznika. Rzecznik sprawuje niezależny nadzór i ma uprawnienia dochodzeniowe. W ramach stałego monitorowania Tarczy Prywatności przez Komisję, w tym za pomocą corocznego wspólnego przeglądu, w którym uczestniczy również Rzecznik, skuteczność działania tego urzędu będzie przedmiotem ponownej oceny.

3.2. *Dostęp organów publicznych USA do danych i wykorzystywanie przez nie danych w celach związanych z egzekwowaniem prawa i interesem publicznym*

(125) Jeżeli chodzi o ingerencję w przekazywanie danych osobowych na podstawie Tarczy Prywatności UE-USA do celów egzekwowania prawa, rząd USA (za pośrednictwem Departamentu Sprawiedliwości) przedstawił zapewnienie dotyczące mających zastosowanie ograniczeń i gwarancji, które w ocenie Komisji gwarantują odpowiedni stopień ochrony.

([176]) Zob. wyrok w sprawie Roman Zakharov przeciwko Rosji z dnia 4 grudnia 2015 r. (Wielka Izba), skarga nr 47143/06, pkt 275 („chociaż co do zasady pożądane jest powierzenie kontroli nadzorczej sędziemu, nadzór prowadzony przez organy pozasądowe można uznać za zgodny z konwencją, pod warunkiem że organ nadzorczy działa niezależnie od organów prowadzących nadzór i posiada wystarczające i skuteczne uprawnienia nadzorcze").

([177]) Zob. wyrok w sprawie Kennedy przeciwko Zjednoczonemu Królestwu z dnia 18 maja 2010 r., skarga nr 26839/05, pkt 167.

([178]) Wyrok w sprawie Schrems, pkt 95. Jak wyraźnie wynika z pkt 91 i 96 wyroku, pkt 95 dotyczy stopnia ochrony gwarantowanego w unijnym porządku prawnym, któremu stopień ochrony w państwie trzecim musi być „merytorycznie równoważny". Zgodnie z pkt 73 i 74 wyroku nie oznacza to, że stopień ochrony lub środki, z jakich to państwo trzecie korzysta, muszą być identyczne, chociaż stosowane środki muszą okazać się skuteczne w praktyce.

(126) Zgodnie z tymi informacjami – na podstawie czwartej poprawki do konstytucji USA ([179]) – wyszukiwanie i pozyskiwanie informacji przez organy egzekwowania prawa wymaga zasadniczo ([180]) nakazu sądowego wydawanego po przedstawieniu „prawdopodobieństwa winy". W kilku dokładnie określonych i wyjątkowych przypadkach, w których obowiązek uzyskania nakazu nie ma zastosowania ([181]), działanie organów rządowych poddaje się testowi „zasadności" ([182]). O tym, czy wyszukiwanie lub pozyskiwanie informacji jest zasadne, „decyduje z jednej strony ocena stopnia, w jakim ingeruje ono w prywatność osoby fizycznej, a z drugiej strony – ocena stopnia, w jakim jest to potrzebne do wspierania uzasadnionych interesów rządowych" ([183]). Mówiąc bardziej ogólnie, czwarta poprawka zapewnia prywatność i godność oraz chroni przed arbitralnymi i ingerującymi działaniami urzędników rządowych ([184]). Te koncepcje uosabiają zasady konieczności i proporcjonalności obowiązujące w prawie Unii. Jeżeli organ egzekwowania prawa nie potrzebuje już korzystać z zatrzymanych przedmiotów do celów dowodowych, przedmioty te należy zwrócić ([185]).

(127) Chociaż prawo zapisane w czwartej poprawce nie przysługuje osobom niebędącym obywatelami USA, które nie mają miejsca zamieszkania w Stanach Zjednoczonych, osoby takie mogą pośrednio korzystać z praw ustanowionych w czwartej poprawce, jeżeli stosowne dane osobowe znajdują się w posiadaniu amerykańskich przedsiębiorstw, przy czym organy egzekwowania prawa muszą każdorazowo uzyskać zezwolenie sądowe (lub przynajmniej spełnić wymóg zasadności) ([186]). Dalszą ochronę gwarantują specjalne ustawowe dokumenty stanowiące podstawę prawną oraz wytyczne Departamentu Sprawiedliwości, które ograniczają dostęp do danych do celów egzekwowania prawa na podstawie równoważnej zasadom konieczności i proporcjonalności (np. poprzez wymóg, aby FBI stosowało jak najmniej inwazyjne metody dochodzeniowe, biorąc pod uwagę ich wpływ na prywatność i wolności obywatelskie) ([187]). Zgodnie z oświadczeniami przedstawionymi przez rząd USA te same lub większe zabezpieczenia mają zastosowanie do dochodzeń w sprawach egzekwowania prawa na szczeblu stanowym (w odniesieniu do dochodzeń prowadzonych na podstawie przepisów prawa stanowego) ([188]).

(128) Chociaż wcześniejsze zezwolenie sądowe wydane przez sąd lub wielką ławę przysięgłych (sądowe ciało dochodzeniowe wyznaczone przez sędziego) nie jest wymagane we wszystkich sprawach ([189]), wezwania administracyjne ograniczają się do określonych przypadków i będą podlegać niezależnej kontroli sądowej przynajmniej wtedy, gdy rząd dochodzi egzekwowania prawa w sądzie ([190]).

([179]) Zgodnie z czwartą poprawką „[p]rawa obywateli do nietykalności osobistej, mieszkania, dokumentów i mienia nie wolno naruszać przez bezzasadne rewizje i zatrzymanie; nakaz w tym przedmiocie można wystawić tylko wówczas, gdy zachodzi wiarygodna przyczyna potwierdzona przysięgą lub zastępującym ją przyrzeczeniem. Miejsce podlegające rewizji oraz osoby i rzeczy podlegające zatrzymaniu powinny być w nakazie szczegółowo określone". Tylko sędziowie mogą wydawać takie nakazy. Federalne nakazy wykonania kopii informacji przechowywanych elektronicznie zostały dodatkowo uregulowane w zasadzie 41 federalnego kodeksu postępowania karnego.

([180]) Sąd Najwyższy wielokrotnie podkreślał, że rewizje bez nakazu stanowią „wyjątkowe" przypadki. Zob. np. wyrok w sprawie Johnson przeciwko Stanom Zjednoczonym, Zbiór orzeczeń Stanów Zjednoczonych (U.S.) t. 333, s. 10, 14 (1948); wyrok w sprawie McDonald przeciwko Stanom Zjednoczonym, Zbiór orzeczeń Stanów Zjednoczonych (U.S.) t. 335, s. 451, 453 (1948); wyrok w sprawie Camara przeciwko Municipal Court, Zbiór orzeczeń Stanów Zjednoczonych (U.S.) t. 387, s. 523, 528–29 (1967); wyrok w sprawie G.M. Leasing Corp. przeciwko Stanom Zjednoczonym, Zbiór orzeczeń Stanów Zjednoczonych (U.S.) t. 429, s. 338, 352–53, 355 (1977). Podobnie Sąd Najwyższy regularnie powtarza, że „najbardziej podstawową zasadą konstytucyjną w tym obszarze jest to, że rewizje dokonywane poza postępowaniem sądowym, bez wcześniejszego zatwierdzenia przez sędziego, są jako takie bezpodstawne w świetle czwartej poprawki – z zastrzeżeniem zaledwie kilku utrwalonych i ściśle określonych wyjątków". Zob. np. wyrok w sprawie Coolidge przeciwko New Hampshire, Zbiór orzeczeń Stanów Zjednoczonych (U.S.) t. 403, s. 443, 454–55 (1971); wyrok w sprawie G.M. Leasing Corp. przeciwko Stanom Zjednoczonym, Zbiór orzeczeń Stanów Zjednoczonych (U.S.) t. 429, s. 338, 352–53, 358 (1977).

([181]) Wyrok w sprawie City of Ontario, Cal. przeciwko Quon, Zbiór orzeczeń Sądu Najwyższego (S. Ct.) t. 130 s. 2619, 2630 (2010).

([182]) Sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 215, s. 107, odniesienie do wyroku w sprawie Maryland przeciwko King, Zbiór orzeczeń Sądu Najwyższego (S. Ct.) t. 133 s. 1958, 1970 (2013).

([183]) Sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 215, s. 107, odniesienie do wyroku w sprawie Samson przeciwko Kalifornii, Zbiór orzeczeń Stanów Zjednoczonych (U.S.) t. 547, s. 843, 848 (2006).

([184]) Wyrok w sprawie City of Ontario, Cal. przeciwko Quon, Zbiór orzeczeń Sądu Najwyższego (S. Ct.) t. 130 s. 2619, 2630 (2010), 2627.

([185]) Zob. np. wyrok w sprawie Stany Zjednoczone przeciwko Wilsonowi, 540 F.2d 1100 (D.C. Cir. 1976).

([186]) Por. wyrok z dnia 4 grudnia 2015 r. w sprawie Roman Zakharov przeciwko Rosji (Wielka Izba), skarga nr 47143/06, pkt 269, zgodnie z którym „wymóg przedstawienia upoważnienia do przechwytywania danych dostawcy usług telekomunikacyjnych przed uzyskaniem dostępu do treści wymienianych przez daną osobę wiadomości stanowi jedną z istotnych gwarancji chroniących osoby przed nadużyciami ze strony organów egzekwowania prawa i służy zagwarantowaniu, że przechwytywanie wiadomości będzie możliwe wyłącznie po uzyskaniu stosownego upoważnienia".

([187]) Oświadczenia Departamentu Sprawiedliwości (załącznik VII), s. 4, wraz z dalszymi odniesieniami.

([188]) Oświadczenia Departamentu Sprawiedliwości (załącznik VII), s. 2.

([189]) Zgodnie z informacjami otrzymanymi przez Komisję i abstrahując od określonych obszarów, które prawdopodobnie nie mają dużego znaczenia z perspektywy przekazywania danych w ramach Tarczy Prywatności UE-USA (np. dochodzenia w sprawach oszustw związanych z ochroną zdrowia, znęcania się nad dziećmi lub substancji kontrolowanych), dotyczy to głównie pewnych dokumentów stanowiących podstawę prawną wydawanych na podstawie ustawy o ochronie danych w łączności elektronicznej, a mianowicie wniosków o podstawowe informacje dotyczące abonentów, informacje dotyczące połączeń i informacje bilingowe (tytuł 18 § 2703 lit. c) pkt 1 i 2 U.S.C., np. informacje dotyczące adresu i rodzaju/czasu świadczenia usługi) i wnioski o treść wiadomości e-mail starszych niż 180 dni (tytuł 18 § 2703 lit. a) i b) U.S.C.). W tym drugim przypadku dana osoba fizyczna musi zostać jednak poinformowana, a zatem ma możliwość podważenia wniosku w sądzie. Zob. również przegląd przeprowadzony przez Departament Sprawiedliwości „Rewizja i zajmowanie komputerów oraz pozyskiwanie dowodów elektronicznych w dochodzeniach" (Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations), rozdział 3: ustawa o przechowywanych danych przekazywanych za pomocą łączności elektronicznej, s. 115–138.

([190]) Zgodnie z oświadczeniami przedstawionymi przez rząd USA adresaci wezwań administracyjnych mogą podważyć je w sądzie na tej podstawie, że są one niezasadne, tj. przesadzone, opresyjne i uciążliwe. Zob. oświadczenie Departamentu Sprawiedliwości (załącznik VII), s. 2.

(129) To samo ma zastosowanie w przypadku wykorzystywania wezwań administracyjnych do celów interesu publicznego. Ponadto zgodnie z oświadczeniami przedstawionymi przez rząd USA zastosowanie mają podobne istotne ograniczenia, polegające na tym, że agencje mogą ubiegać się o dostęp jedynie do danych, które mają znaczenie w sprawach wchodzących w zakres ich uprawnień, i muszą przestrzegać standardu zasadności.

(130) 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. 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.

(131) Co do zasady, zgodnie z przepisami dotyczącymi kontroli sądowej ustanowionymi w ustawie o postępowaniu administracyjnym ([191])„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 ([192]). 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" ([193]).

(132) Ściślej rzecz ujmując, w tytule II ustawy o ochronie danych w łączności elektronicznej ([194]) 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 osobami trzecimi ([195]). 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.

(133) Ponadto zgodnie z ustawą o dostępie do informacji publicznej (tytuł 5 § 552 U.S.C.) każdy ma prawo do wglądu do rejestru prowadzonego przez agencję federalną, a 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 ([196]).

([191]) Tytuł 5 § 702 U.S.C.

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

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

([194]) Tytuł 18 §§ 2701–2712 U.S.C.

([195]) 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.

([196]) 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 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.).

(134) 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 ([197]), ustawa o oszustwach i nadużyciach komputerowych ([198]), ustawa federalna o roszczeniach z tytułu czynu niedozwolonego ([199]), ustawa o prawie do prywatności w kwestiach finansowych ([200]) oraz ustawa o rzetelnej sprawozdawczości kredytowej ([201]).

(135) Komisja stwierdza zatem, że w Stanach Zjednoczonych wdrożono przepisy służące ograniczeniu wszelkiej ingerencji do celów egzekwowania prawa ([202]) lub do celów innych interesów publicznych w prawa podstawowe osób, których dane osobowe są przekazywane z Unii do Stanów Zjednoczonych w ramach Tarczy Prywatności UE-USA, do tego, co jest ściśle niezbędne, aby osiągnąć dany uzasadniony cel i aby zapewnić skuteczną ochronę prawną przed taką ingerencją.

4. **ODPOWIEDNI STOPIEŃ OCHRONY W RAMACH TARCZY PRYWATNOŚCI UE-USA**

(136) W świetle tych ustaleń Komisja uznaje, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do samocertyfikowanych podmiotów w Stanach Zjednoczonych w ramach Tarczy Prywatności UE-USA.

(137) W szczególności Komisja stwierdza, że zasady opublikowane przez Departament Handlu Stanów Zjednoczonych rozumiane jako całość zapewniają stopień ochrony danych osobowych, który jest zasadniczo równoważny poziomowi gwarantowanemu podstawowymi zasadami ustanowionymi w dyrektywie 95/46/WE.

(138) Ponadto ustanowienie zobowiązań w zakresie przejrzystości oraz zarządzanie Tarczą Prywatności przez Departament Handlu gwarantuje skuteczne stosowanie zasad.

(139) Ponadto Komisja stwierdza, że mechanizmy nadzoru i mechanizmy odwoławcze przewidziane w Tarczy Prywatności – rozumiane jako całość – zapewniają możliwość identyfikowania przypadków naruszenia zasad przez podmioty uczestniczące w programie Tarczy Prywatności i nakładania za nie kar w praktyce i oferują osobom, których dane dotyczą, możliwość skorzystania ze środków ochrony prawnej w celu uzyskania dostępu do danych na ich temat oraz – ostatecznie – skorygowania lub usunięcia takich danych.

(140) Ponadto na podstawie dostępnych informacji na temat amerykańskiego porządku prawnego, w tym oświadczeń i zobowiązań rządu USA, Komisja stwierdza, że wszelkie ingerencje amerykańskich organów publicznych w prawa podstawowe osób, których dane osobowe są przekazywane z Unii do Stanów Zjednoczonych w ramach Tarczy Prywatności UE-USA do celów bezpieczeństwa narodowego, egzekwowania prawa lub innych celów interesu publicznego, a także wiążące się z nimi ograniczenia nałożone na samocertyfikowane podmioty w odniesieniu do przestrzegania przez nie zasad, będą ograniczać się do tego, co jest ściśle niezbędne, aby osiągnąć dany uzasadniony cel, oraz że istnieje skuteczna ochrona prawna przed taką ingerencją.

([197]) 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 adresów i innych 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).

([198]) 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.

([199]) 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".

([200]) 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.

([201]) 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.

([202]) Trybunał Sprawiedliwości uznał, że egzekwowanie prawa stanowi uzasadniony cel polityki. Zob. sprawy połączone C-293/12 i C-594/12, Digital Rights Ireland i in., EU:C:2014:238, pkt 42. Zob. także art. 8 ust. 2 europejskiej konwencji praw człowieka oraz wyrok Europejskiego Trybunału Praw Człowieka w sprawie Weber i Saravia przeciwko Niemcom, skarga nr 54934/00, pkt 104.

(141) Komisja stwierdza, że spełnia to normy art. 25 dyrektywy 95/46/WE interpretowanego w świetle Karty praw podstawowych Unii Europejskiej, jak wyjaśnił Trybunał Sprawiedliwości w szczególności w wyroku w sprawie Schrems.

5. DZIAŁANIA ORGANÓW OCHRONY DANYCH I INFORMACJE PRZEKAZYWANE KOMISJI

(142) W wyroku w sprawie Schrems Trybunał Sprawiedliwości wyjaśnił, że Komisja nie ma uprawnień, aby ograniczać kompetencje, które przysługują organom ochrony danych na mocy art. 28 dyrektywy 95/46/WE (w tym kompetencji do zawieszenia przekazywania danych), w przypadku gdy przy okazji skargi wnoszonej na mocy tego przepisu jednostka podważa zgodność wydanej przez Komisję decyzji w sprawie odpowiedniej ochrony danych osobowych z ochroną podstawowego prawa do prywatności i ochrony danych ([203]).

(143) Aby skutecznie monitorować funkcjonowanie Tarczy Prywatności, Komisja powinna być informowana przez państwa członkowskie o odpowiednich działaniach podejmowanych przez organy ochrony danych.

(144) Trybunał Sprawiedliwości stwierdził ponadto, że zgodnie z art. 25 ust. 6 akapit drugi dyrektywy 95/46/WE państwa członkowskie i ich organy muszą podejmować środki niezbędne w celu zapewnienia zgodności z aktami instytucji unijnych, ponieważ co do zasady przyjmuje się, że akty te są zgodne z prawem, a zatem wywołują skutki prawne do czasu ich uchylenia, stwierdzenia ich nieważności w postępowaniu o stwierdzenie nieważności lub orzeczenia ich nieważności w następstwie wniosku o wydanie orzeczenia w trybie prejudycjalnym lub zarzutu niezgodności z prawem. W rezultacie decyzja w sprawie odpowiedniej ochrony danych osobowych przyjęta przez Komisję na podstawie art. 25 ust. 6 dyrektywy 95/46/WE jest wiążąca dla wszystkich organów państw członkowskich, do których jest skierowana, w tym ich niezależnych organów nadzorczych ([204]). W przypadku gdy taki organ otrzymał skargę, w której podważono zgodność wydanej przez Komisję decyzji w sprawie odpowiedniej ochrony danych osobowych z ochroną podstawowego prawa do prywatności i ochrony danych, i organ ten uzna podniesione zarzuty za zasadne, w prawie krajowym należy zapewnić drogę prawną umożliwiającą mu podniesienie tych zarzutów przed sądem krajowym, który w razie wątpliwości jest zobowiązany zawiesić postępowanie i wystąpić z odesłaniem prejudycjalnym do Trybunału Sprawiedliwości ([205]).

6. OKRESOWY PRZEGLĄD USTALENIA DOTYCZĄCEGO ADEKWATNOŚCI

(145) W świetle tego, że stopień ochrony zapewniany w porządku prawnym USA może ulec zmianie, Komisja po przyjęciu niniejszej decyzji będzie okresowo sprawdzać, czy ustalenia odnoszące się do adekwatności stopnia ochrony gwarantowanego przez Stany Zjednoczone w ramach Tarczy Prywatności UE-USA są nadal faktycznie i prawnie uzasadnione. Taka kontrola jest wymagana w każdym przypadku, gdy Komisja pozyska informacje budzące uzasadnione wątpliwości w tym kontekście ([206]).

(146) W związku z tym Komisja będzie nieprzerwanie monitorować ogólne ramy przekazywania danych osobowych zapewnione przez Tarczę Prywatności UE-USA oraz przestrzeganie przez organy USA oświadczeń i zobowiązań zawartych w dokumentach dołączonych do niniejszej decyzji. Aby ułatwić ten proces, Stany Zjednoczone zobowiązały się informować Komisję o istotnych zmianach w prawie amerykańskim, gdy dotyczą one Tarczy Prywatności w dziedzinie ochrony danych i ograniczeń w zakresie gwarancji stosowanych w celu uzyskania dostępu do danych osobowych przez organy publiczne. Co więcej, niniejsza decyzja będzie podlegać corocznemu wspólnemu przeglądowi, który obejmie wszystkie aspekty funkcjonowania Tarczy Prywatności UE-USA, w tym funkcjonowania wyjątków w zakresie bezpieczeństwa narodowego i egzekwowania prawa od obowiązujących zasad. Ponadto, ze względu na fakt, że zmiany w prawie Unii również mogą wpłynąć na ustalenie dotyczące adekwatności, Komisja oceni stopień ochrony zapewniony w ramach Tarczy Prywatności po wejściu w życie ogólnego rozporządzenia o ochronie danych.

(147) Aby przeprowadzić coroczny wspólny przegląd, o którym mowa w załącznikach I, II i VI, Komisja spotka się z przedstawicielami Departamentu Handlu i FTC oraz – w stosownych przypadkach – z przedstawicielami innych departamentów i agencji zaangażowanych we wdrażanie ustaleń dotyczących Tarczy Prywatności oraz, w sprawach związanych z bezpieczeństwem narodowym, przedstawicielami Urzędu Dyrektora Krajowych Służb Wywiadowczych, innych jednostek Wspólnoty Wywiadowczej i Rzecznikiem. Uczestnictwo w tym spotkaniu będzie otwarte dla unijnych organów ochrony danych i przedstawicielu Grupy Roboczej Art. 29.

([203]) Wyrok w sprawie Schrems, pkt 40 i nast., pkt 101–103.
([204]) Wyrok w sprawie Schrems, pkt 51, 52 i 62.
([205]) Wyrok w sprawie Schrems, pkt 65.
([206]) Wyrok w sprawie Schrems, pkt 76.

(148) W ramach corocznego wspólnego przeglądu Komisja zwróci się do Departamentu Handlu o przedstawienie kompleksowych informacji dotyczących wszelkich istotnych aspektów funkcjonowania Tarczy Prywatności UE-USA, w tym zgłoszeń otrzymanych przez Departament Handlu od organów ochrony danych i wyników przeglądów przestrzegania zasad prowadzonych z urzędu. Komisja będzie również zwracać się o wyjaśnienia dotyczące wszelkich pytań lub kwestii związanych z Tarczą Prywatności UE-USA i jej funkcjonowaniem wynikających z wszelkich dostępnych informacji, w tym sprawozdań z przejrzystości dozwolonych na mocy amerykańskiej ustawy o wolności, ogólnodostępnych sprawozdań sporządzanych przez krajowe organy wywiadowcze USA, organy ochrony danych, grupy ds. ochrony prywatności, doniesień medialnych lub jakichkolwiek innych możliwych źródeł. Co więcej, aby ułatwić Komisji zadanie w tym względzie, państwa członkowskie powinny informować Komisję o przypadkach, w których działania organów odpowiedzialnych za zapewnienie przestrzegania zasad w Stanach Zjednoczonych nie zagwarantowały ich przestrzegania, oraz o wszelkich oznakach tego, że działania organów publicznych USA odpowiedzialnych za bezpieczeństwo narodowe lub zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych nie gwarantują wymaganego stopnia ochrony.

(149) Na podstawie corocznego wspólnego przeglądu Komisja przygotuje ogólnodostępne sprawozdanie, które przedłoży Parlamentowi Europejskiemu i Radzie.

7. ZAWIESZENIE DECYZJI W SPRAWIE ODPOWIEDNIEJ OCHRONY DANYCH OSOBOWYCH

(150) W przypadku gdy na podstawie kontroli lub jakichkolwiek innych dostępnych informacji Komisja stwierdzi, iż stopnia ochrony zapewnionego w ramach Tarczy Prywatności nie można zasadniczo uznać za równoważny stopniowi ochrony gwarantowanemu w Unii, lub gdy występują wyraźne oznaki tego, że w Stanach Zjednoczonych być może nie zapewnia się już skutecznego przestrzegania zasad lub że działania organów publicznych USA odpowiedzialnych za bezpieczeństwo narodowe lub zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych nie gwarantują wymaganego stopnia ochrony, Komisja poinformuje o tym Departament Handlu i zwróci się o szybkie podjęcie odpowiednich środków w celu zaradzenia potencjalnemu nieprzestrzeganiu zasad w określonym i rozsądnym terminie. Jeżeli po upływie określonego terminu organy USA nie wykażą w zadowalający sposób, że Tarcza Prywatności UE-USA nadal gwarantuje skuteczne przestrzeganie zasad i odpowiedni stopień ochrony, Komisja rozpocznie postępowanie prowadzące do częściowego lub pełnego zawieszenia lub uchylenia niniejszej decyzji ([207]). Komisja może ewentualnie zaproponować zmianę niniejszej decyzji na przykład poprzez ograniczenie zakresu ustalenia dotyczącego adekwatności wyłącznie do przekazywania danych podlegającego dodatkowym warunkom.

(151) W szczególności Komisje rozpocznie procedurę zawieszenia lub uchylania w przypadku:

a) oznak, że organy USA nie przestrzegają oświadczeń i zobowiązań zawartych w dokumentach dołączonych do niniejszej decyzji, w tym jeżeli chodzi o warunki i ograniczenia dostępu amerykańskich organów publicznych do danych osobowych przekazywanych w ramach Tarczy Prywatności do celów egzekwowania prawa, bezpieczeństwa narodowego i innych celów interesu publicznego;

b) nieskutecznego rozpatrywania skarg wnoszonych przez osoby, których dane dotyczą, pochodzące z UE; w tym kontekście Komisja uwzględni wszystkie okoliczności mające wpływ na możliwość egzekwowania praw osób, których dane dotyczą, pochodzących z UE, w tym w szczególności dobrowolne zobowiązanie się samocertyfikowanych organizacji amerykańskich do współpracy z organami ochrony danych i stosowania ich rad; lub

c) nieudzielania terminowych i stosownych odpowiedzi przez Rzecznika ds. Tarczy Prywatności na wnioski składane przez osoby, których dane dotyczą, pochodzące z UE.

(152) Komisja rozważy również wszczęcie postępowania prowadzącego do zmiany, zawieszenia lub uchylenia niniejszej decyzji, jeżeli w kontekście corocznego wspólnego przeglądu funkcjonowania Tarczy Prywatności UE-USA lub w inny sposób Departament Handlu lub inne departamenty lub agencje zaangażowane we wdrażanie Tarczy Prywatności lub, w sprawach związanych z bezpieczeństwem narodowym, przedstawiciele amerykańskiej Wspólnoty Wywiadowczej lub Rzecznik nie przedstawią informacji lub wyjaśnień niezbędnych do oceny przestrzegania zasad, skuteczności procedur rozpatrywania skarg lub obniżenia wymaganego stopnia ochrony w wyniku działań krajowych organów wywiadowczych USA, w szczególności w wyniku gromadzenia lub

([207]) Od dnia rozpoczęcia stosowania ogólnego rozporządzenia o ochronie danych Komisja będzie korzystała ze swoich uprawnień do przyjmowania – w należycie uzasadnionych i szczególnie pilnych przypadkach – aktu wykonawczego zawieszającego niniejszą decyzję, który stosuje się z efektem natychmiastowym bez uprzedniego przedkładania go odpowiedniemu komitetowi procedury komitetowej i który pozostaje w mocy przed okres nieprzekraczający sześciu miesięcy.

uzyskania dostępu do danych osobowych, które nie ograniczają się do tego, co jest ściśle niezbędne i proporcjonalne. W tym kontekście Komisja uwzględni zakres, w jakim odpowiednie informacje można uzyskać z innych źródeł, w tym za pomocą sprawozdań samocertyfikowanych przedsiębiorstw amerykańskich zgodnie z przepisami amerykańskiej ustawy o wolności.

(153) Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, powołana na mocy art. 29 dyrektywy 95/46/WE, wydała opinię w sprawie stopnia ochrony zapewnionego w ramach Tarczy Prywatności UE-USA ([208]), która została uwzględniona przy przygotowaniu niniejszej decyzji.

(154) Parlament Europejski przyjął rezolucję w sprawie transatlantyckich przepływów danych ([209]).

(155) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu ustanowionego na mocy art. 31 ust. 1 dyrektywy 95/46/WE,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

1. Do celów art. 25 ust. 2 dyrektywy 95/46/WE Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do podmiotów w Stanach Zjednoczonych w ramach Tarczy Prywatności UE-USA.

2. Na Tarczę Prywatności UE-USA składają się zasady wydane przez Departament Handlu Stanów Zjednoczonych w dniu 7 lipca 2016 r., jak wskazano w załączniku II, oraz oficjalne oświadczenia i zobowiązania zawarte w dokumentach przedstawionych w załącznikach I, III–VII.

3. Do celów ust. 1 dane osobowe są przekazywane w ramach Tarczy Prywatności UE-USA, w przypadku gdy przekazuje się je z Unii do podmiotów w Stanach Zjednoczonych, które figurują w „wykazie podmiotów uczestniczących w programie Tarczy Prywatności" prowadzonym i udostępnianym publicznie przez Departament Handlu Stanów Zjednoczonych zgodnie z sekcjami I i III zasad przedstawionych w załączniku II.

Artykuł 2

Niniejsza decyzja nie wpływa na stosowanie przepisów dyrektywy 95/46/WE innych niż art. 25 ust. 1, które dotyczą przetwarzania danych osobowych w państwach członkowskich, w szczególności jej art. 4.

Artykuł 3

W przypadku gdy właściwe organy w państwach członkowskich wykonują swoje uprawnienia na podstawie art. 28 ust. 3 dyrektywy 95/46/WE, co prowadzi do zawieszenia lub ostatecznego zakazu przepływu danych do podmiotu w Stanach Zjednoczonych, który figuruje w wykazie podmiotów uczestniczących w programie Tarczy Prywatności, zgodnie z sekcjami I i III zasad przedstawionych w załączniku II w celu ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, dane państwo członkowskie bezzwłocznie informuje o tym Komisję.

Artykuł 4

1. Komisja będzie stale monitorować funkcjonowanie Tarczy Prywatności UE-USA, aby ocenić, czy Stany Zjednoczone nadal zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do podmiotów w Stanach Zjednoczonych w ramach Tarczy.

([208]) Opinia nr 01/2016 dotycząca projektu decyzji w sprawie odpowiedniej ochrony danych osobowych w ramach Tarczy Prywatności UE-USA, przyjęta w dniu 13 kwietnia 2016 r.

([209]) Rezolucja Parlamentu Europejskiego z dnia 26 maja 2016 r. w sprawie transatlantyckich przepływów danych (2016/2727(RSP).

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

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

4. W ciągu roku od dnia powiadomienia państw członkowskich o wydaniu niniejszej decyzji, a następnie co roku Komisja będzie oceniać ustalenie, o którym mowa w art. 1 ust. 1, na podstawie wszystkich dostępnych informacji, w tym informacji otrzymanych w ramach corocznego wspólnego przeglądu, w którym mowa w załącznikach I, II i VI.

5. Komisja będzie zgłaszać wszelkie istotne ustalenia komitetowi ustanowionemu na mocy art. 31 dyrektywy 95/46/WE.

6. Komisja przedstawi projekt środków zgodnie z procedurą, o której mowa w art. 31 ust. 2 dyrektywy 95/46/WE, w celu między innymi zawieszenia, zmiany lub uchylenia niniejszej decyzji lub ograniczenia jej zakresu, jeżeli pojawią się przesłanki:

— wskazujące, że organy publiczne USA nie przestrzegają oświadczeń i zobowiązań zawartych w dokumentach dołączonych do niniejszej decyzji, w tym jeżeli chodzi o warunki i ograniczenia dostępu amerykańskich organów publicznych do danych osobowych przekazywanych w ramach Tarczy Prywatności UE-USA do celów egzekwowania prawa, bezpieczeństwa narodowego i innych celów interesu publicznego,

— wskazujące na systematyczne nieskuteczne rozpatrywanie skarg wnoszonych przez osoby z UE, których dane dotyczą, lub

— wskazujące na systematyczne nieudzielanie przez Rzecznika ds. Tarczy Prywatności terminowych i stosownych odpowiedzi na wnioski składane przez osoby z UE, których dane dotyczą, zgodnie z sekcją 4 lit. e) załącznika III.

Komisja przedstawi również taki projekt środków, jeżeli brak współpracy z zaangażowanymi podmiotami w zapewnianiu funkcjonowania Tarczy Prywatności UE-USA w Stanach Zjednoczonych uniemożliwi Komisji stwierdzenie, czy ma to wpływ na ustalenie, o którym mowa w art. 1 ust. 1.

Artykuł 5

Państwa członkowskie stosują wszelkie środki niezbędne do wykonania niniejszej decyzji.

Artykuł 6

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 12 lipca 2016 r.

W imieniu Komisji
Věra JOUROVÁ
Członek Komisji

ZAŁĄCZNIK I

Pismo sekretarz handlu Stanów Zjednoczonych Penny Pritzker

Dnia 7 lipca 2016 r.

Pani Věra Jourová
Komisarz ds. sprawiedliwości, konsumentów i równouprawnienia płci
Komisja Europejska
Rue de la Loi/Westraat 200
1049 Bruxelles/Brussel
Belgia

Szanowna Pani Komisarz!

W imieniu Stanów Zjednoczonych Ameryki mam przyjemność niniejszym przekazać pakiet materiałów dotyczących Tarczy Prywatności UE-USA, który stanowi efekt dwóch lat owocnych dyskusji między naszymi zespołami. Pakiet ten, wraz z innymi dostępnymi Komisji materiałami ze źródeł publicznych, daje bardzo solidną podstawę przyjęcia przez Komisję Europejską nowego ustalenia dotyczącego adekwatności ([1]).

Powinniśmy być dumni z udoskonalenia ram. Tarcza Prywatności opiera się na zasadach, które cieszą się silnym i solidarnym poparciem po obu stronach Atlantyku i których stosowanie usprawniliśmy. Nasza współpraca stworzyła realną możliwość zwiększenia ochrony prywatności na całym świecie.

Pakiet Tarczy Prywatności obejmuje zasady Tarczy Prywatności wraz z pismem, dołączonym jako załącznik 1, od Urzędu ds. Handlu Międzynarodowego Departamentu Handlu, który zarządza programem; w piśmie tym opisano zobowiązania, jakie nasz Departament podjął, aby zapewnić skuteczne funkcjonowanie Tarczy Prywatności. Pakiet obejmuje również załącznik 2, który zawiera inne zobowiązania Departamentu Handlu związane z nowym modelem arbitrażowym dostępnym w ramach Tarczy Prywatności.

Zwróciłam się do moich pracowników o wykorzystanie wszelkich niezbędnych zasobów, aby zapewnić szybkie i pełne wdrożenie ram Tarczy Prywatności oraz terminowe wypełnianie zobowiązań określonych w załącznikach 1 i 2.

Pakiet Tarczy Prywatności obejmuje również inne dokumenty pochodzące od innych agencji Stanów Zjednoczonych, mianowicie:

— pismo Federalnej Komisji Handlu (FTC), w którym Komisja opisuje sposób, w jaki egzekwuje zasady Tarczy Prywatności,

— pismo Departamentu Transportu, w którym Departament opisuje sposób, w jaki egzekwuje zasady Tarczy Prywatności,

— dwa pisma sporządzone przez Urząd Dyrektora Krajowych Służb Wywiadowczych dotyczące gwarancji i ograniczeń mających zastosowanie do amerykańskich aktów stanowiących podstawę prawną w sprawach bezpieczeństwa narodowego,

— pismo Departamentu Stanu i towarzyszące mu memorandum, w których opisano zobowiązanie Departamentu Stanu do ustanowienia nowego urzędu Rzecznika ds. Tarczy Prywatności, do którego będzie można kierować zapytania dotyczące praktyk rozpoznania radioelektronicznego stosowanych przez Stany Zjednoczone, oraz

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

Zapewniam, że Stany Zjednoczone traktują te zobowiązania poważnie.

([1]) Pod warunkiem że decyzja Komisji w sprawie adekwatności ochrony przewidzianej przez Tarczę Prywatności UE-USA ma zastosowanie do Islandii, Liechtensteinu i Norwegii, zasady Tarczę Prywatności UE-USA obejmują zarówno Unię Europejską, jak i te trzy kraje.

W terminie 30 dni od ostatecznego zatwierdzenia ustalenia dotyczącego adekwatności pełen pakiet Tarczy Prywatności zostanie przekazany do rejestru federalnego w celu publikacji.

Cieszymy się na współpracę z Państwem przy wdrażaniu Tarczy Prywatności oraz przy wchodzeniu razem w nową fazę tego procesu.

Z poważaniem

Penny Pritzker

Załącznik 1

Pismo pełniącego obowiązki podsekretarza handlu międzynarodowego Kena Hyatta

Szanowna Pani Věra Jourová
Komisarz ds. sprawiedliwości, konsumentów i równouprawnienia płci
Komisja Europejska
Rue de la Loi/Westraat 200
1049 Bruxelles/Brussel
Belgia

Szanowna Pani Komisarz!

W imieniu Urzędu ds. Handlu Międzynarodowego mam przyjemność przedstawić opis zwiększonej ochrony danych osobowych, jaką zapewniają ramy Tarczy Prywatności UE-USA („Tarcza Prywatności" lub „ramy"), i zobowiązań, jakie podjął Departament Handlu („Departament"), aby zapewnić skuteczne funkcjonowanie Tarczy Prywatności. Sfinalizowanie tego historycznego przedsięwzięcia jest niezwykle znaczącym osiągnięciem zarówno w kontekście prywatności, jak i dla przedsiębiorstw po obu stronach Atlantyku. 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. Daje pewność, która pozwoli na rozwój gospodarki transatlantyckiej poprzez zapewnienie, aby tysiące europejskich i amerykańskich przedsiębiorstw mogło dalej inwestować i prowadzić działalność poza naszymi granicami. Tarcza Prywatności jest skutkiem trwającej ponad dwa lata ciężkiej pracy oraz współpracy z Państwem, naszymi kolegami i koleżankami w Komisji Europejskiej („Komisja"). Liczymy na dalszą współpracę z Komisją w celu zapewnienia, by Tarcza Prywatności funkcjonowała zgodnie z zamierzeniami.

Współpracowaliśmy z Komisją w celu opracowania Tarczy Prywatności, aby umożliwić podmiotom z siedzibą w Stanach Zjednoczonych spełnienie wymogów adekwatności ochrony danych wynikających z prawa Unii. Nowe ramy przyniosą kilka istotnych 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. Wymagają od uczestniczących amerykańskich podmiotów, aby opracowały odpowiednią politykę ochrony prywatności, publicznie zobowiązały się do przestrzegania zasad Tarczy Prywatności, umożliwiając tym samym egzekwowanie zobowiązań na podstawie prawa amerykańskiego, 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 i podlegały kompetencji Federalnej Komisji Handlu („FTC"), Departamentu Transportu lub innego organu ochrony porządku publicznego. Po drugie, Tarcza Prywatności pozwoli tysiącom spółek w Stanach Zjednoczonych i jednostkom zależnym spółek europejskich w Stanach Zjednoczonych na uzyskiwanie danych osobowych z Unii Europejskiej, aby ułatwić przepływy danych, które przyczyniają się do rozwoju handlu transatlantyckiego. Transatlantyckie stosunki gospodarcze już teraz osiągnęły największą na świecie skalę, stanowiąc połowę światowej produkcji gospodarczej – wartość handlu towarami i usługami w ramach tych stosunków szacuje się na blisko trzy biliony dolarów, a ponadto przyczyniają się one do tworzenia 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 (MŚP). 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. Tarcza Prywatności przyczynia się do większego przestrzegania zasad udostępniania danych osobowych, niwelując różnice w naszych podejściach prawnych przy jednoczesnym wspomaganiu realizacji celów handlowych i gospodarczych zarówno Europy, jak i Stanów Zjednoczonych.

Chociaż decyzja przedsiębiorstwa o samocertyfikacji zobowiązującej je do przestrzegania niniejszych nowych ram jest dobrowolna, to w momencie, gdy publicznie zobowiąże się ono do stosowania Tarczy Prywatności, zobowiązanie takie może zostać wyegzekwowane na drodze prawnej na mocy prawa amerykańskiego przez Federalną Komisję Handlu albo Departament Transportu, w zależności od tego, który organ jest właściwy do rozstrzygania spraw danego podmiotu uczestniczącego w programie Tarczy Prywatności.

Udoskonalenia do zasad Tarczy Prywatności

Będąca skutkiem tych udoskonaleń Tarcza Prywatności wzmacnia ochronę prywatności poprzez:

— wprowadzony w zasadzie dotyczącej ogłaszania wymóg przekazywania dodatkowych informacji osobom fizycznym, obejmujących między innymi deklarację uczestnictwa podmiotu w programie Tarczy Prywatności, oświadczenie o prawie dostępu osoby fizycznej do danych osobowych i wskazanie odpowiedniego niezależnego organu rozstrzygania sporów,

— wzmocnienie ochrony danych osobowych, które podmiot uczestniczący w programie Tarczy Prywatności przekazuje administratorowi będącemu osobą trzecią, poprzez ustanowienie wobec stron wymogu zawarcia umowy, w której przewidziane zostanie, że takie dane można przetwarzać wyłącznie do ograniczonych i określonych celów, na które osoba fizyczna wyraziła zgodę, i że odbiorca zagwarantuje ten sam poziom ochrony co poziom wymagany zasadami,

— wzmocnienie ochrony danych osobowych, które podmiot uczestniczący w programie Tarczy Prywatności przekazuje przedstawicielowi będącemu osobą trzecią, w tym poprzez wymóg, aby podmiot uczestniczący w programie Tarczy Prywatności: podjął zasadne i odpowiednie kroki w celu zagwarantowania, że przedstawiciel będzie efektywnie przetwarzał dane osobowe przekazane mu w sposób zgodny z zobowiązaniami podmiotu wynikającymi z zasad; na wezwanie podjął zasadne i odpowiednie kroki w celu zatrzymania niedozwolonego przetwarzania i naprawienia szkód z niego wynikłych; oraz na wezwanie Departamentu przedstawił streszczenie lub poświadczoną kopię odpowiednich postanowień dotyczących prywatności zawartych w umowie z tym przedstawicielem,

— zapewnienie, aby podmiot uczestniczący w programie Tarczy Prywatności był odpowiedzialny za przetwarzanie danych osobowych, które otrzymuje zgodnie z Tarczą Prywatności, a następnie przekazuje osobie trzeciej działającej jako jej przedstawiciel, i aby podmiot uczestniczący w programie Tarczy Prywatności ponosił odpowiedzialność zgodnie z zasadami, jeżeli jej przedstawiciel przetwarza tego rodzaju dane osobowe w sposób niezgodny z zasadami, chyba że podmiot udowodni, że nie jest odpowiedzialny za zdarzenie, które spowodowało szkodę,

— wyjaśnienie, że podmioty uczestniczące w programie Tarczy Prywatności muszą ograniczyć dane osobowe do danych, które są istotne do celów przetwarzania,

— wymóg, aby podmiot co roku poświadczał w drodze certyfikacji w Departamencie swoje zobowiązanie do stosowania zasad do danych, które otrzymał, kiedy uczestniczył w programie Tarczy Prywatności, w przypadku gdy zrezygnuje ze stosowania zasad Tarczy Prywatności, a postanowi o zatrzymaniu takich danych,

— wymóg, aby zapewniono niezależny mechanizm ochrony prawnej z którego osoby fizyczne mogą skorzystać bez ponoszenia jakichkolwiek kosztów,

— wymóg, aby podmioty i wskazane przez nie niezależne mechanizmy ochrony prawnej bezzwłocznie reagowały na złożone przez Departament zapytania i wnioski o informacje dotyczące Tarczy Prywatności,

— wymóg, aby podmioty sprawnie reagowały na skargi dotyczące przestrzegania zasad złożone przez organy państwa członkowskiego UE za pośrednictwem Departamentu, oraz

— wymóg, aby podmiot uczestniczący w programie Tarczy Prywatności podawał do wiadomości publicznej wszelkie istotne związane z Tarczą Prywatności części jakichkolwiek sprawozdań dotyczących przestrzegania zasad lub sprawozdań oceniających, które przedłożono Federalnej Komisji Handlu, w przypadku gdy względem podmiotu wydano decyzję FTC lub orzeczenie sądowe w sprawie nieprzestrzegania zasad.

Zarządzanie i nadzór nad programem Tarczy Prywatności przez Departament Handlu

Departament podkreśla swoje zobowiązanie do prowadzenia i publicznego udostępniania oficjalnego wykazu amerykańskich podmiotów, które dokonały samocertyfikacji w Departamencie i zadeklarowały swoje zobowiązanie do przestrzegania zasad („wykaz podmiotów uczestniczących w programie Tarczy Prywatności"). Departament będzie aktualizował wykaz podmiotów uczestniczących w programie Tarczy Prywatności 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 wcześniej dokonały samocertyfikacji w Departamencie, ale które usunięto z wykazu podmiotów uczestniczących w programie Tarczy Prywatności, w tym podmiotów, które usunięto ze względu na uporczywe nieprzestrzeganie zasad. Departament określi powód, dla którego usunięto poszczególne podmioty.

Ponadto Departament zobowiązuje się do wzmocnienia zarządzania i nadzoru nad Tarczą Prywatności. Konkretnie Departament podejmie działania opisane poniżej.

Dostarczanie dodatkowych informacji na stronie internetowej Tarczy Prywatności:

— będzie prowadził wykaz podmiotów uczestniczących w programie Tarczy Prywatności oraz rejestr tych podmiotów, które wcześniej dokonały samocertyfikacji zobowiązującej je do przestrzegania zasad, ale które nie mogą dalej korzystać z przywilejów przysługujących w ramach Tarczy Prywatności,

— przedstawi uzasadnienie, umieszczając je w wyraźnie widocznym miejscu, w którym wyjaśni, że wszystkie podmioty usunięte z wykazu podmiotów uczestniczących w programie Tarczy Prywatności nie mogą już korzystać z przywilejów przysługujących w ramach Tarczy Prywatności, ale muszą mimo to nadal stosować jej zasady do danych osobowych, które otrzymały w czasie, gdy uczestniczyły w Tarczy Prywatności, dopóki są w posiadaniu takich danych, oraz

— umieści link do wykazu spraw prowadzonych przez FTC w związku z Tarczą Prywatności, który znajduje się na stronie FTC.

Weryfikacja wymogów samocertyfikacji:

— przed sfinalizowaniem samocertyfikacji podmiotu (lub corocznej ponownej certyfikacji) i umieszczeniem go w wykazie podmiotów uczestniczących w programie Tarczy Prywatności zweryfikuje, czy podmiot:

  — przekazał wymagane informacje kontaktowe,

  — przedstawił opis swojej działalności w odniesieniu do danych osobowych otrzymywanych z UE,

  — wskazał, jakie dane osobowe zostają objęte jego samocertyfikacją,

  — w przypadku gdy podmiot prowadzi ogólnodostępną stronę internetową – dostarczył adres strony internetowej, na której znajduje się polityka ochrony prywatności, i zapewnił, aby polityka ochrony prywatności była dostępna pod tym adresem – lub w przypadku gdy podmiot nie prowadzi ogólnodostępnej strony internetowej – informację o tym, gdzie polityka ochrony prywatności jest udostępniona do wglądu dla ogółu społeczeństwa,

  — zawarł w swojej odpowiedniej polityce ochrony prywatności oświadczenie, że przestrzega zasad, i jeżeli polityka ochrony prywatności jest dostępna na stronie internetowej – link do strony internetowej Departamentu poświęconej Tarczy Prywatności,

  — 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),

  — jeżeli podmiot zamierza spełnić wymogi określone w lit. a) ppkt (i) i lit. a) ppkt (iii) zasady dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności poprzez zobowiązanie się do współpracy z odpowiednimi unijnymi organami ochrony danych – wskazał swój zamiar współpracy z organami ochrony danych w dochodzeniach i rozstrzyganiu skarg wniesionych na podstawie zasad Tarczy Prywatności, w szczególności zamiar odpowiadania na ich zapytania, w przypadku gdy osoby, których dane dotyczą, pochodzące z UE wniosły skargę bezpośrednio do swojego krajowego organu ochrony danych,

  — wskazał wszelkie programy ochrony prywatności, których jest członkiem,

  — wskazał metodę kontroli zapewniającą przestrzeganie zasad (np. wewnętrzną, prowadzoną przez osobę trzecią),

  — wskazał – zarówno w zgłoszeniu samocertyfikacji, jak i w polityce ochrony prywatności – niezależny mechanizm ochrony prawnej, który umożliwia badanie i rozstrzyganie skarg,

  — zawarł w swojej odpowiedniej polityce ochrony prywatności, jeżeli jest ona dostępna na stronie internetowej, link do tej strony internetowej lub do formularza skargi, którą można złożyć w ramach niezależnego mechanizmu ochrony prawnej umożliwiającego zbadanie nierozstrzygniętych skarg, oraz

  — jeżeli podmiot wskazał, że zamierza uzyskiwać dane o zasobach ludzkich przekazywane z UE w związku ze stosunkiem pracy – zadeklarował swoje zobowiązanie do współpracy z organami ochrony danych i przestrzegania ich procedur w celu rozstrzygania skarg dotyczących jego działalności związanej z takimi danymi, przedłożył w Departamencie kopię swojej polityki ochrony prywatności w zakresie zasobów ludzkich i udzielił informacji, gdzie polityka ta jest dostępna do wglądu dla objętych nią pracowników,

— będzie współpracował z niezależnym mechanizmem ochrony prawnej w celu zweryfikowania, czy podmioty faktycznie zarejestrowały odpowiednie mechanizmy wskazane w zgłoszeniach samocertyfikacji, jeżeli taka rejestracja jest wymagana.

Zintensyfikowanie starań i podjęcie działań następczych w odniesieniu do podmiotów, które usunięto z wykazu podmiotów uczestniczących w programie Tarczy Prywatności:

— powiadomi podmioty, które usunięto z wykazu podmiotów uczestniczących w programie Tarczy Prywatności za „uporczywe nieprzestrzeganie zasad", że nie mają one prawa do zatrzymania danych zgromadzonych na podstawie zasad Tarczy Prywatności, oraz

— wyśle kwestionariusze do podmiotów, których samocertyfikacje wygasły lub które dobrowolnie wycofały się z programu Tarczy Prywatności, aby zweryfikować, czy dany podmiot ponownie zacznie stosować jej zasady, zaprzestanie ich stosowania lub nadal będzie je stosować do danych osobowych, które otrzymał w czasie, gdy uczestniczył w programie Tarczy Prywatności, a jeżeli dane osobowe zostaną zatrzymane, zweryfikuje, kto w ramach podmiotu będzie pełnił funkcję osoby odpowiedzialnej za bieżące kontakty w przypadku zapytań związanych z Tarczą Prywatności.

Wyszukiwanie fałszywych oświadczeń dotyczących uczestnictwa w programie i przeciwdziałanie im:

— będzie dokonywał przeglądu polityk ochrony prywatności podmiotów, które wcześniej uczestniczyły w programie Tarczy Prywatności, ale które usunięto z wykazu podmiotów uczestniczących w programie Tarczy Prywatności, aby zidentyfikować wszelkie fałszywe oświadczenia dotyczące uczestnictwa w programie Tarczy Prywatności,

— w przypadku gdy podmiot: a) wycofa się z programu Tarczy Prywatności, b) nie dokona ponownej certyfikacji potwierdzającej jej zobowiązanie do przestrzegania zasad lub c) zostanie usunięty z wykazu uczestników programu Tarczy Prywatności, w szczególności za „uporczywe nieprzestrzeganie zasad" – zobowiąże się do tego, aby na bieżąco i z urzędu weryfikować, czy podmiot usunął – z każdej odpowiedniej opublikowanej polityki ochrony prywatności – wszelkie odniesienia do Tarczy Prywatności sugerujące, że dalej jest ona aktywnym uczestnikiem programu Tarczy Prywatności i ma prawo do korzystania z przywilejów przysługujących w ramach Tarczy. Jeżeli Departament ustali, że takich odniesień nie usunięto, przekaże podmiotowi ostrzeżenie, że – w stosownych przypadkach – skieruje sprawę do odpowiedniego organu, zwracając się o ewentualne wszczęcie odpowiedniego postępowania, jeżeli podmiot ten nadal będzie twierdził, że posiada certyfikację Tarczy Prywatności. Jeżeli podmiot nie usunie odniesień ani nie dokona samocertyfikacji zobowiązującej go do przestrzegania zasad Tarczy Prywatności, Departament z urzędu skieruje sprawę do FTC, Departamentu Transportu lub innego odpowiedniego organu egzekwowania prawa lub też – w stosownych przypadkach – podejmie działanie służące wyegzekwowaniu znaku certyfikacyjnego Tarczy Prywatności,

— będzie podejmował inne działania służące zidentyfikowaniu fałszywych oświadczeń dotyczących uczestnictwa w programie Tarczy Prywatności i przypadków niewłaściwego wykorzystywania znaku certyfikacyjnego Tarczy Prywatności, w tym poprzez wyszukiwanie w internecie, gdzie umieszczono obrazy znaku certyfikacyjnego Tarczy Prywatności i odniesienia do Tarczy Prywatności w politykach ochrony prywatności podmiotu,

— bezzwłocznie rozwiąże wszelkie problemy, które zidentyfikujemy w trakcie monitorowania z urzędu fałszywych oświadczeń dotyczących uczestnictwa w programie i przypadków niewłaściwego wykorzystywania znaku certyfikacyjnego, w tym poprzez przekazanie ostrzeżenia podmiotom, które podają fałszywe informacje na temat ich uczestnictwa w programie Tarczy Prywatności, jak opisano powyżej,

— podejmie inne właściwe działania naprawcze; obejmują one wszelkie środki ochrony prawnej, które Departament ma prawo wdrożyć, i dokonanie zgłoszenia do FTC, Departamentu Transportu lub innego odpowiedniego organu egzekwowania prawa, oraz

— bezzwłocznie rozpatrzy i rozstrzygnie skargi dotyczące fałszywych oświadczeń dotyczących uczestnictwa w programie, jakie otrzymamy.

Departament dokona przeglądu polityk ochrony prywatności podmiotów, aby móc skuteczniej identyfikować fałszywe oświadczenia dotyczące uczestnictwa w programie Tarczy Prywatności i im przeciwdziałać. Konkretnie Departament dokona przeglądu polityk ochrony prywatności podmiotów, których samocertyfikacja wygasła ze względu na brak ponownej certyfikacji potwierdzającej ich zobowiązanie do przestrzegania zasad. Departament przeprowadzi ten rodzaj przeglądu, aby zweryfikować, czy takie podmioty usunęły – z każdej odpowiedniej opublikowanej polityki ochrony prywatności – wszelkie odniesienia, które sugerują, że podmiot nadal jest aktywnym uczestnikiem programu Tarczy Prywatności. W wyniku przeglądów tego rodzaju zidentyfikujemy podmioty, które nie usunęły takich odniesień, a Biuro Radcy Generalnego Departamentu wystosuje do tych podmiotów pismo z ostrzeżeniem o możliwości wszczęcia odpowiedniego postępowania, jeżeli odniesienia nie zostaną usunięte. Departament podejmie działania następcze w celu zapewnienia, aby podmioty usunęły niewłaściwe odniesienia albo dokonały ponownej certyfikacji potwierdzającej ich zobowiązanie do przestrzegania zasad. Ponadto Departament podejmie starania, aby zidentyfikować fałszywe oświadczenia dotyczące uczestnictwa w programie Tarczy Prywatności składane przez podmioty, które nigdy w tym programie nie uczestniczyły, i podejmie podobne działanie naprawcze w stosunku do takich podmiotów.

Dokonywanie z urzędu przeglądów i oceny przestrzegania zasad w ramach programu:

— będzie na bieżąco i efektywnie monitorował przestrzeganie zasad, w tym poprzez wysyłanie szczegółowych kwestionariuszy podmiotom uczestniczącym, aby wskazać problemy, które mogą wymagać podjęcia dalszych działań następczych. W szczególności takie przeglądy przestrzegania zasad odbywają się, w przypadku gdy: a) Departament otrzymał konkretne poważne skargi dotyczące nieprzestrzegania zasad przez podmiot, b) podmiot nie reaguje w zadowalający sposób na zapytania z Departamentu dotyczące informacji związanych z Tarczą Prywatności lub c) istnieją przekonujące dowody na to, że podmiot nie dochowuje swoich zobowiązań w ramach Tarczy Prywatności. Departament skonsultuje się – w stosownych przypadkach – z właściwymi organami ochrony danych w związku z takimi przeglądami przestrzegania zasad, oraz

— będzie przeprowadzał okresową ocenę zarządzania i nadzoru nad programem Tarczy Prywatności w celu zapewnienia, aby działania podejmowane w związku z monitorowaniem były adekwatne pod kątem rozwiązania nowych problemów, gdy te się pojawią.

Departament zwiększył zasoby, które zostaną przeznaczone na zarządzanie i nadzór nad programem Tarczy Prywatności, w tym podwoił liczbę pracowników odpowiedzialnych za zarządzanie i nadzór nad programem. Nadal będziemy przeznaczać odpowiednie zasoby na takie działania, aby zapewnić efektywne monitorowanie programu i zarządzanie nim.

Dostosowanie strony internetowej Tarczy Prywatności do indywidualnych potrzeb docelowych odbiorców

Departament, dostosowując stronę internetową Tarczy Prywatności, uwzględni przede wszystkim trzy grupy docelowych odbiorców: osoby fizyczne z UE, przedsiębiorstwa z UE i przedsiębiorstwa z USA. 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 zapewnią one jasne wyjaśnienie: 1) praw, jakie przysługują osobom fizycznym z UE w ramach Tarczy Prywatności; 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 ramach Tarczy Prywatności. W odniesieniu do przedsiębiorstw z UE ułatwią one kontrolę: 1) tego, czy podmiot może korzystać z przywilejów przysługujących w ramach Tarczy Prywatności; 2) rodzaju danych objętych samocertyfikacją podmiotu w ramach Tarczy Prywatności; 3) polityki ochrony prywatności mającej zastosowanie do danych objętych samocertyfikacją; oraz 4) metody, jaką wykorzystuje podmiot do kontroli przestrzegania przez nią zasad.

Pogłębiona współpraca z organami ochrony danych

Aby zwiększyć możliwości współpracy z organami ochrony danych, Departament ustanowi specjalny punkt kontaktowy w Departamencie, który będzie pełnił funkcję łącznika z organami ochrony danych. W przypadkach, w których organ ochrony danych uzna, że podmiot nie przestrzega zasad, w tym w następstwie skargi złożonej przez osobę fizyczną z UE, organ ochrony danych może skontaktować się ze specjalnym punktem w Departamencie w celu skierowania sprawy tego podmiotu do dalszego rozpoznania. Punkt kontaktowy będzie również otrzymywał zgłoszenia dotyczące podmiotów, które nieprawdziwie twierdzą, że uczestniczą w programie Tarczy Prywatności, chociaż nigdy nie dokonały samocertyfikacji zobowiązującej je do przestrzegania zasad. Punkt kontaktowy będzie wspierał organy ochrony danych w poszukiwaniu informacji dotyczących konkretnej samocertyfikacji podmiotu lub jego wcześniejszego uczestnictwa w programie i będzie odpowiadał na zapytania organu ochrony danych dotyczące realizacji określonych wymogów Tarczy Prywatności. Po drugie, Departament przekaże organom ochrony danych materiały dotyczące Tarczy Prywatności, 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 Tarczy Prywatności 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.

Ułatwienie rozstrzygania skarg na nieprzestrzeganie zasad

Departament, za pośrednictwem specjalnego punktu kontaktowego, będzie otrzymywał skargi przekazane mu przez organ ochrony danych dotyczące nieprzestrzegania zasad przez podmiot uczestniczący w programie Tarczy Prywatności. Departament dołoży wszelkich starań, aby ułatwić rozstrzygnięcie skargi na podmiot uczestniczący w programie Tarczy Prywatności. W terminie 90 dni od otrzymania skargi Departament przekaże organowi ochrony danych aktualne informacje. Aby ułatwić składanie takich skarg, Departament opracuje standardowy formularz, który organ ochrony danych będzie mógł złożyć w specjalnym punkcie kontaktowym Departamentu. Specjalny punkt kontaktowy będzie monitorował wszystkie zgłoszenia, jakie Departament otrzymuje od organów ochrony danych; ponadto Departament przedstawi sprawozdanie – w rocznym przeglądzie opisanym poniżej – zawierające łączną analizę otrzymanych w danym roku skarg.

Przyjęcie procedur arbitrażowych i wybór arbitrów w porozumieniu z Komisją

Departament dochowa swoich zobowiązań określonych w załączniku I i opublikuje procedury po osiągnięciu porozumienia.

Wspólny mechanizm przeglądu funkcjonowania Tarczy Prywatności

Departament Handlu, FTC i inne organy – w stosownych przypadkach – będą organizowały coroczne spotkania z Komisją, zainteresowanymi organami ochrony danych i odpowiednimi przedstawicielami Grupy Roboczej Art. 29, podczas których Departament przekaże aktualne informacje na temat programu Tarczy Prywatności. Coroczne spotkania będą obejmowały omówienie bieżących problemów dotyczących funkcjonowania, wdrażania i egzekwowania postanowień Tarczy Prywatności oraz nadzoru nad Tarczą Prywatności, w tym zgłoszeń skierowanych do Departamentu przez organy ochrony danych, wyników przeglądów przestrzegania zasad przeprowadzanych z urzędu; Pierwszy roczny przegląd i kolejne przeglądy będą obejmować w stosownych przypadkach dialog na inne tematy, m.in. w dziedzinie zautomatyzowanego podejmowania decyzji, włącznie z aspektami dotyczącymi podobieństw i różnic w podejściu stosowanym w Unii Europejskiej i Stanach Zjednoczonych.

Zmiany ustaw

Departament dołoży starań, aby poinformować Komisję o istotnych zmianach w amerykańskim prawie, o ile zmiany odnoszą się do Tarczy Prywatności w dziedzinie ochrony danych oraz ograniczeń i gwarancji mających zastosowanie do dostępu do danych osobowych przez amerykańskie organy i późniejszego wykorzystania danach.

spotkania mogą również wiązać się z omówieniem stosownych zmian prawnych.

W odniesieniu do ograniczeń przestrzegania zasad Tarczy Prywatności do celów bezpieczeństwa narodowego główny radca Urzędu Dyrektora Krajowych Służb Wywiadowczych, Robert Litt, również wystosował dwa pisma do Justina Antonipillai i Teda Deana z Departamentu Handlu, które zostały Państwu przekazane. Pisma te szczegółowo omawiają m.in. politykę, gwarancje i ograniczenia mające zastosowanie do działań rozpoznania radioelektronicznego prowadzonych przez Stany Zjednoczone. Ponadto pisma te opisują przejrzystość zapewnianą przez Wspólnotę Wywiadowczą w odniesieniu do tych kwestii. Ponieważ Komisja dokonuje oceny ram Tarczy Prywatności, informacje zawarte w tych pismach stanowią zapewnienie właściwego funkcjonowania Tarczy Prywatności zgodnie z jej zasadami. Rozumiemy, że mogą Państwo w przyszłości wykorzystywać informacje, które Wspólnota Wywiadowcza podała do wiadomości publicznej, a także inne informacje, do celów przeprowadzania corocznych przeglądów ram Tarczy Prywatności.

Mając na uwadze zasady Tarczy Prywatności oraz towarzyszące im pisma i materiały, w tym zobowiązania Departamentu dotyczące zarządzania i nadzoru nad ramami Tarczy Prywatności, oczekujemy, że Komisja uzna, iż ramy Tarczy Prywatności UE-USA zapewniają odpowiednią ochronę do celów prawa Unii i że dane z Unii Europejskiej nadal będą przekazywane podmiotom uczestniczącym w programie Tarczy Prywatności.

Z poważaniem

Ken Hyatt

Załącznik 2

Model arbitrażowy

ZAŁĄCZNIK I

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

A. **Zakres**

Osoba fizyczna może skorzystać z arbitrażu, aby ustalić – w odniesieniu do pozostałych roszczeń – czy podmiot uczestniczący w programie Tarczy Prywatności 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 Tarczy Prywatności.

B. **Dostępne środki ochrony prawnej**

W przypadku wszczęcia postępowania arbitrażowego panel ds. Tarczy Prywatności (w którego skład wchodzi jeden arbiter lub trzech arbitrów, zgodnie z ustaleniami stron) jest uprawniony do zasądzenia 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 jedyne uprawnienia przysługujące panelowi arbitrażowemu w odniesieniu do środków ochrony prawnej. W czasie obrad nad tym, jakie środki ochrony prawnej należy zastosować w danym przypadku, panel arbitrażowy musi wziąć pod uwagę inne środki ochrony prawnej, które zostały już zastosowane w ramach innych mechanizmów Tarczy Prywatności. 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 sekcji III podsekcja 11 lit. d) ppkt (i) zasad; 2) skorzystać z bezpłatnego niezależnego mechanizmu ochrony prawnej przewidzianego w zasadach; 3) przekazać stosowne informacje Departamentowi Handlu za pośrednictwem odpowiedniego organu ochrony danych i zapewnić Departamentowi Handlu możliwość podjęcia działań w celu rozwiązania danego problemu w terminach określonych w piśmie Urzędu ds. Handlu Międzynarodowego w Departamencie Handlu – 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 postępowania arbitrażowego nie można przeprowadzić, jeżeli unijny organ ochrony danych: 1) jest organem właściwym zgodnie z sekcją III.5 lub III.9 zasad; 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 odszkodowania za ten sam rodzaj naruszenia przed innym organem lub sądem, przy czym jeżeli godziwe odszkodowanie w formie niepieniężnej nie rekompensuje w pełni domniemanego naruszenia, wystąpienie osoby fizycznej o arbitraż nie wyklucza wniesienia powództwa o odszkodowanie do sądu.

([1]) Sekcja I.5 zasad.

E. **Kontrola i wykonanie**

Osoby fizyczne i podmioty uczestniczące w programie Tarczy Prywatności będą mogły wystąpić o przeprowadzenie kontroli sądowej i wykonanie orzeczeń arbitrażowych zgodnie z prawem amerykańskim, tj. federalną ustawą o arbitrażu ([1]). Wszelkie tego typu sprawy muszą być wnoszone przed federalny sąd pierwszej instancji, którego właściwość miejscowa obejmuje główne miejsce prowadzenia działalności podmiotu uczestniczącego w programie Tarczy Prywatności.

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

F. **Skład arbitrażowy**

Strony wybiorą arbitrów z wykazu arbitrów omówionego poniżej.

Zgodnie z obowiązującym prawem Departament Handlu Stanów Zjednoczonych i Komisja Europejska opracują wykaz co najmniej 20 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 wystąpi uzasadniona przyczyna skreślenia z wykazu, z możliwością przedłużenia na kolejny okres obejmujący trzy lata;

2) nie podlegają żadnym instrukcjom wydanym przez stronę, dowolny podmiot uczestniczący w programie Tarczy Prywatności, Stany Zjednoczone, 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 w zakresie unijnego prawa ochrony danych.

G. **Procedury arbitrażowe**

Zgodnie z obowiązującym prawem, w terminie 6 miesięcy od przyjęcia decyzji w sprawie adekwatności ochrony, Departament Handlu i Komisja Europejska uzgodnią przyjęcie istniejącego, ugruntowanego zbioru amerykańskich procedur arbitrażowych (takich jak AAA lub JAMS) na potrzeby uregulowania postępowań przed panelem ds. Tarczy Prywatności, 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;

([1]) 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 nieruchomości położonej 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 innej strony 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.

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 Stanów Zjednoczonych, 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 Unii Europejskiej organy ochrony danych UE 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 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 konieczności dozwolone może być przeprowadzenie szczegółowego postępowania dowodowego (and. 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.

H. **Koszty**

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

Zgodnie z obowiązującym prawem Departament Handlu ułatwi utworzenie funduszu, na który podmioty uczestniczące w programie Tarczy Prywatności będą zobowiązane wpłacać roczną składkę proporcjonalną do ich wielkości, która to składka pokryje koszty arbitrażu, w tym honorarium arbitra, do maksymalnej kwoty („górnej granicy"), po konsultacji z Komisją Europejską. Funduszem będzie zarządzać osoba trzecia, która będzie regularnie przedstawiać sprawozdania z działalności funduszu. Podczas corocznego przeglądu Departament Handlu i Komisja Europejska dokonają przeglądu funkcjonowania funduszu, w tym konieczności dostosowania kwoty składek lub maksymalnych kwot, oraz przeanalizują między innymi liczbę postępowań arbitrażowych oraz ich koszty i czas trwania, przy czym obie strony zgadzają się, że nie zostaną nałożone żadne nadmierne obciążenia finansowe na podmioty uczestniczące w programie Tarczy Prywatności. Honoraria pełnomocnika nie są objęte niniejszym przepisem ani żadnym funduszem ustanowionym na jego mocy.

ZAŁĄCZNIK II

RAMOWE ZASADY TARCZY PRYWATNOŚCI UE-USA WYDANE PRZEZ DEPARTAMENT HANDLU STANÓW ZJEDNOCZONYCH

I. OGÓLNY ZARYS

1. Chociaż Stany Zjednoczone i Unia Europejska dążą do tego samego celu, jakim jest podniesienie poziomu ochrony prywatności, to Stany Zjednoczone mają inne podejście do prywatności niż Unia Europejska. Stany Zjednoczone stosują podejście sektorowe, które polega na połączeniu ustawodawstwa, regulacji i samoregulacji. Mając na uwadze te różnice i aby zapewnić podmiotom w Stanach Zjednoczonych niezawodny mechanizm przekazywania danych osobowych z Unii Europejskiej 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, Departament Handlu wydaje niniejsze zasady Tarczy Prywatności, w tym zasady uzupełniające ((razem zwane dalej „zasadami") na mocy swych ustawowych uprawnień do ułatwiania, wspierania i rozwijania handlu międzynarodowego (tytuł 15 § 1512 kodeksu Stanów Zjednoczonych „U.S.C."). Zasady zostały opracowane w porozumieniu z Komisją Europejską, przedstawicielami przemysłu i innymi zainteresowanymi stronami w celu ułatwienia handlu między Stanami Zjednoczonymi a Unią Europejską. Są one przeznaczone do wyłącznego użytku amerykańskich podmiotów otrzymujących dane osobowe z Unii Europejskiej w celu zakwalifikowania ich do programu Tarczy Prywatności, a zatem przyznania im przywilejów przysługujących na mocy decyzji Komisji Europejskiej w sprawie adekwatności ochrony ([1]). Zasady pozostają bez wpływu na stosowanie krajowych przepisów wprowadzających w życie dyrektywę 95/46/WE („dyrektywa"), które stosuje się do przetwarzania danych osobowych w państwach członkowskich. Zasady nie ograniczają również obowiązków związanych z ochroną prywatności, które w innym wypadku mają zastosowanie w prawie amerykańskim.

2. Aby móc skorzystać z Tarczy Prywatności w celu uzyskania danych z UE, podmiot musi dokonać samocertyfikacji zobowiązującej go do przestrzegania zasad w Departamencie Handlu (lub wobec przez niego wyznaczonej jednostki) („Departament"). Chociaż decyzja podmiotu o dołączeniu do Tarczy Prywatności 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 Tarczy Prywatności, podmiot musi a) podlegać uprawnieniom dochodzeniowym i wykonawczym Federalnej Komisji Handlu („FTC"), Departamentowi Transportu lub innemu organowy ustawowemu, 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. W razie nieprzestrzegania zasad przez podmiot można dochodzić wykonania obowiązku na mocy sekcji 5 ustawy o Federalnej Komisji Handlu, w której zakazano nieuczciwych i wprowadzających w błąd działań w ramach wymiany handlowej lub mających wpływ na wymianę handlową (tytuł 15 § 45 lit. a) U.S.C.) lub na mocy innych przepisów ustawowych lub wykonawczych, w których zakazano takich działań.

3. Departament Handlu będzie prowadził i publicznie udostępniał oficjalny wykaz amerykańskich podmiotów, które dokonały samocertyfikacji w Departamencie i zadeklarowały swoje zobowiązanie do przestrzegania zasad („wykaz podmiotów uczestniczących w programie Tarczy Prywatności"). Przywileje wynikające z Tarczy Prywatności przysługują od dnia, w którym Departament umieści podmiot w wykazie podmiotów uczestniczących w programie Tarczy Prywatności. Departament usunie podmiot z wykazu podmiotów uczestniczących w programie Tarczy Prywatności, jeżeli podmiot dobrowolnie wycofa się z programu Tarczy Prywatności lub jeżeli nie dokona corocznej ponownej certyfikacji w Departamencie. Usunięcie podmiotu z wykazu podmiotów uczestniczących w programie Tarczy Prywatności oznacza, że nie może ona już korzystać z przywilejów przysługujących na mocy decyzji Komisji Europejskiej w sprawie adekwatności ochrony, aby uzyskiwać dane osobowe z UE. Podmiot ten musi nadal stosować zasady do danych osobowych, które otrzymał w czasie, gdy uczestniczył w Tarczy Prywatności, i musi potwierdzać co roku to zobowiązanie w Departamencie dopóty, dopóki przechowuje takie dane; w innym razie podmiot musi zwrócić lub usunąć dane lub też zapewnić „odpowiednią" ochronę danych za pomocą innych dozwolonych środków. Departament usunie również z wykazu podmiotów uczestniczących w programie Tarczy Prywatności te podmioty, które uporczywie nie przestrzegały zasad; podmioty te nie kwalifikują się do tego, by korzystać z przywilejów przysługujących w ramach Tarczy Prywatności i muszą zwrócić lub usunąć dane osobowe, które otrzymały w ramach Tarczy Prywatności.

4. Departament będzie również prowadził i publicznie udostępniał oficjalny rejestr amerykańskich podmiotów, które wcześniej dokonały samocertyfikacji w Departamencie, ale które usunięto z wykazu podmiotów uczestniczących w programie Tarczy Prywatności. Departament wystosuje jasne ostrzeżenie, w którym poda, że te podmioty nie są

([1]) Pod warunkiem że decyzja Komisji w sprawie adekwatności ochrony przewidzianej przez Tarczę Prywatności UE-USA ma zastosowanie do Islandii, Liechtensteinu i Norwegii, zasady Tarczę Prywatności UE-USA obejmą zarówno Unię Europejską, jak i te trzy kraje. Z tego względu odniesienia do Unii Europejskiej i jej państw członkowskich będą rozumiane jako obejmujące Islandię, Liechtenstein i Norwegię.

uczestnikami Tarczy Prywatności; że usunięcie z wykazu podmiotów uczestniczących Tarczy Prywatności oznacza, iż nie mogą się one prezentować jako podmioty przestrzegające zasad Tarczy Prywatności ani nie mogą wygłaszać jakichkolwiek oświadczeń czy też stosować wprowadzających w błąd praktyk, które sugerowałyby ich uczestnictwo w programie Tarczy Prywatności; oraz że takie podmioty nie mogą już korzystać zprzywilejów przysługujących na mocy decyzji Komisji Europejskiej w sprawie adekwatności ochrony,które umożliwiłyby tym podmiotom uzyskanie danych osobowych z UE. Wobec podmiotu, która twierdzi, że nadal uczestniczy w programie Tarczy Prywatności, lub który podaje inne fałszywe informacje na temat swojego uczestnictwa w programie Tarczy Prywatności po jego usunięciu z wykazu podmiotów uczestniczących w programie Tarczy Prywatności, FTC, Departament Transportu lub inne organy egzekwowania prawa mogą wszcząć odpowiednie postępowanie.

5. Przestrzeganie tych zasad może być ograniczone: a) w zakresie niezbędnym do spełnienia wymogów bezpieczeństwa narodowego, interesu publicznego lub egzekwowania prawa; b) ustawą, rozporządzeniem rządu lub orzecznictwem, którymi nałożono sprzeczne obowiązki lub 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 dyrektywy lub przepisów prawa państwa członkowskiego dopuszcza się wyjątki lub odstępstwa, pod warunkiem że takie wyjątki lub odstępstwa stosuje się w porównywalnych okolicznościach. Zgodnie z celem zwiększenia ochrony prywatności podmioty powinny dążyć do pełnego wdrożenia tych zasad w sposób przejrzysty, w tym wskazując w swoich politykach ochrony prywatności przypadki, w których wyjątki od zasad wskazane w lit. b) powyżej będą regularnie stosowane. Z tego samego powodu – w przypadku gdy zasady lub prawo amerykańskie dopuszcza taką możliwość – oczekuje się, że w miarę możliwości podmioty będą decydować się na wyższy poziom ochrony.

6. Po przystąpieniu do programu Tarczy Prywatności podmioty mają obowiązek stosować zasady zawsze, gdy przekazują dane osobowe w ramach programu Tarczy Prywatności. Podmiot, który chce rozszerzyć przywileje wynikające z Tarczy Prywatności 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 zasadach uzupełniających dotyczących samocertyfikacji.

7. Prawo amerykańskie będzie miało zastosowanie do wykładni i zagadnień związanych z przestrzeganiem zasad oraz odpowiednimi politykami ochrony prywatności podmiotów uczestniczących w programie Tarczy Prywatności z wyjątkiem przypadków, gdy takie podmioty zobowiązały się współpracować z europejskimi organami ochrony danych. 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 dyrektywy, otrzymane z Unii Europejskiej 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 jest data ostatecznego zatwierdzenia postanowienia dotyczącego odpowiedniego poziomu ochrony przez Komisję Europejską.

II. ZASADY

1. **Powiadomienie**

   a. Podmiot musi poinformować osoby fizyczne o:

      i. swoim uczestnictwie w programie Tarczy Prywatności i podać link do strony internetowej zawierającej wykaz podmiotów uczestniczących w programie Tarczy Prywatności lub adres tej strony,

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

iii. swoim zobowiązaniu do stosowania zasad do wszystkich danych osobowych otrzymanych z UE w ramach Tarczy Prywatności,

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 mogę odpowiadać na takie zapytania lub skargi,

vi. rodzaju lub tożsamości osób 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 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, Departamentu Transportu lub jakiegokolwiek innego amerykańskiego uprawnionego organu ustawowego,

xi. możliwości wystąpienia przez osobę fizyczną – pod pewnymi warunkami – o arbitraż,

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 wtórnego przekazywania danych osobom trzecim.

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 osobie trzeciej.

2. **Wybór**

a. Podmiot musi dać osobom fizycznym możliwość wyboru (klauzula *opt-out*), czy dane osobowe ich dotyczące mają: (i) zostać ujawnione osobie 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. W drodze odstępstwa od poprzedniego ustępu zagwarantowanie wyboru nie jest konieczne, jeżeli dane ujawnia się osobie trzeciej, która działa jako przedstawiciel upoważniony do wykonywania czynności w imieniu i na polecenie podmiotu. Podmiot powinien jednak zawsze zawrzeć umowę z przedstawicielem.

c. W przypadku danych wrażliwych (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 (zezwolenie) osób fizycznych, jeżeli takie dane mają zostać (i) ujawnione osobie 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 osobę trzecią jako dane wrażliwe, w przypadku gdy osoba trzecia określa i traktuje je jako wrażliwe.

3. **Odpowiedzialność za wtórne przekazywanie**

a. Przekazując dane osobowe osobie trzeciej działającej jako administrator, podmioty muszą stosować zasady powiadomienia i wyboru. Podmioty muszą również zawrzeć z administratorem będącym osobą 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, osoba trzecia będąca administratorem zaprzestaje przetwarzania lub podejmuje inne właściwe uzasadnione środki w celu zaradzenia tej sytuacji.

b. Przekazując dane osobowe osobie trzeciej działającej jako administrator, podmioty muszą: (i) przekazywać takie dane wyłącznie do ograniczonych i określonych celów; (ii) upewnić się, że podmiot przetwarzający ma obowiązek zapewnienia przynajmniej takiego samego poziomu ochrony prywatności co poziom wymagany w zasadach; (iii) podjąć zasadne i odpowiednie kroki w celu zagwarantowania, że podmiot przetwarzający będzie efektywnie przetwarzać dane osobowe przekazane mu w sposób zgodny z zobowiązaniami podmiotu wynikającymi z zasad; (iv) nałożyć na podmiot przetwarzający 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 podmiotem przetwarzającym.

4. **Bezpieczeństwo**

a. Podmioty tworzące, przechowujące, wykorzystujące lub rozpowszechniające dane osobowe muszą podejmować 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 celowe**

a. Zgodnie z zasadami dane osobowe muszą ograniczać się do danych, które są istotne do celów przetwarzania ([1]). 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, dokładne, kompletne i aktualne. Podmiot musi przestrzegać zasad dopóty, dopóki przechowuje takie dane.

b. Informacje mogą być zatrzymane w formie identyfikującej osobę fizyczną lub umożliwiającej jej identyfikację ([2]) jedynie tak długo, jak długo służy to celowi przetwarzania w rozumieniu 5a. 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 innym zasadom i przepisom ramowym. 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.

([1]) 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.

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

7. **Ochrona prawna, egzekwowanie prawa i 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 muszę 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 i poprzez odniesienie do zasad, a także przyznaje odszkodowanie, w przypadku gdy przewidziano to w prawie właściwym lub w ramach inicjatywy sektora prywatnego;

ii. dalsze postępowanie 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 Tarczy Prywatności. 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.

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 wtórnego przekazywania podmiot uczestniczący w programie Tarczy Prywatności jest odpowiedzialny za przetwarzanie danych osobowych, które otrzymuje w ramach Tarczy Prywatności, a następnie przekazuje je osobie trzeciej działającej jako podmiot przetwarzający w jej imieniu. Podmiot objęty Tarczą Prywatności ponosi odpowiedzialność zgodnie z zasadami, jeżeli jego podmiot przetwarzający 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 decyzji FTC lub orzeczenia sądu w związku z nieprzestrzeganiem zasad, upublicznia on wszelkie istotne części sprawozdań dotyczących przestrzegania zasad lub oceny związane z Tarczą Prywatności, które przedłożył FTC, w zakresie zgodnym z wymogami poufności. Departament utworzył specjalne stanowisko ds. kontaktów z organami ochrony danych na wypadek jakichkolwiek problemów z przestrzeganiem zasad przez podmioty uczestniczące w programie Tarczy Prywatności. FTC będzie priorytetowo traktował 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 (pozwolenia) 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 jej celów jej działalności, a dane nie są ujawnione osobom 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 i wyłączenie z zakresu dyrektywy materiałów dziennikarskich, 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 Tarczy Prywatności.

3. **Odpowiedzialność pośrednia**

a. Dostawcy usług internetowych, operatorzy telekomunikacyjni i inne podmioty nie podlegają odpowiedzialności w ramach zasad Tarczy Prywatności, gdy w imieniu innej podmiotu jedynie przekazują, kierują, przełączają lub przechowują informacje. Podobnie jak w przypadku samej dyrektywy Tarcza Prywatności nie powoduje odpowiedzialności pośredniej. W zakresie, w jakim podmiot działa jedynie jako kanał dla danych przekazywanych przez osoby 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 podmioty uczestniczące w programie Tarczy Prywatności, są regularnie poddawane audytom. Skuteczność tego rodzaju audytów, szczególnie tych dotyczących potencjalnych naruszeń, może być zagrożona w razie przedwczesnego ujawnienia. Podobnie podmiot uczestniczący w programie Tarczy Prywatności, 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 unijnymi organami ochrony danych w sposób opisany poniżej. W ramach programu Tarczy Prywatności podmioty amerykańskie otrzymujące dane osobowe z UE muszą zobowiązać się do stosowania skutecznych mechanizmów w celu zapewnienia przestrzegania zasad Tarczy Prywatności. 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)(i) i (a)(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 Tarczy Prywatności złożonym w Departamencie Handlu (zob. zasada uzupełniająca dotycząca samocertyfikacji), że podmiot:

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

ii. będzie współpracował z organami ochrony danych przy badaniu i rozstrzyganiu skarg wniesionych w ramach Tarczy Prywatności; 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 Tarczy Prywatności, 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 Unii Europejskiej, 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 w ramach Tarczy Prywatności. Wskazówki te będą miały na celu zapewnienie prawidłowego stosowania zasad Tarczy Prywatności 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 Tarczy Prywatności, 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 Federalnej Komisji Handlu, Departamentowi Transportu albo innemu federalnemu lub stanowemu organowi Stanów Zjednoczonych posiadającemu ustawowe uprawnienia do wszczęcia postępowania w przypadku wprowadzenia w błąd albo podania fałszywych informacji albo stwierdzenia, że porozumienie o współpracy zostało poważnie naruszone i musi tym samym zostać uznane za nieważne. W tym ostatnim przypadku grupa poinformuje Departament Handlu, tak aby wykaz podmiotów uczestniczących w programie Tarczy Prywatności mógł zostać odpowiednio zmieniony. Każdy przypadek niewypełnienia zobowiązania do współpracy z organami ochrony danych, a także przypadki nieprzestrzegania zasad Tarczy Prywatności będą podlegały zaskarżeniu jako praktyka wprowadzająca w błąd na mocy sekcji 5 ustawy o Federalnej Komisji Handlu albo innej podobnej ustawy.

d. Podmiot, który chce, aby przywileje wynikające z Tarczy Prywatności 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 i mogą również zostać poproszone o pokrycie koniecznych wydatków związanych z tłumaczeniami wynikających z rozpatrywania przez grupę zgłoszeń lub skarg złożonych przeciwko nim. Roczna składka nie przekroczy 500 USD, a w przypadku mniejszych przedsiębiorstw będzie niższa.

6. **Samocertyfikacja**

a. Przywileje wynikające z Tarczy Prywatności przysługują od dnia, w którym Departament umieści zgłoszenie samocertyfikacji złożone przez podmiot w wykazie podmiotów uczestniczących w programie Tarczy Prywatności po wcześniejszym ustaleniu, czy zgłoszenie jest kompletne.

b. W celu dokonania samocertyfikacji do celów Tarczy Prywatności podmiot musi złożyć w Departamencie zgłoszenie samocertyfikacji podpisane przez członka zarządu w imieniu podmiotu, który przystępuje do programu Tarczy Prywatności, zawierające przynajmniej następujące dane:

i. nazwę podmiotu, adres pocztowy, adres e-mail, numery telefonu i faksu;

ii. opis działalności podmiotu w odniesieniu do danych osobowych otrzymywanych z UE; oraz

iii. opis obowiązującej w podmiocie polityki 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;

2. datę jej wdrożenia;

3. biuro kontaktowe dla rozpatrywania skarg, wniosków o udostępnienie danych oraz wszelkich innych kwestii wynikających z uczestnictwa w programie Tarczy Prywatności;

4. 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);

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

6. metodę kontroli, np. wewnętrzną lub przez osoby trzecie (zob. zasada uzupełniająca dotycząca kontroli); oraz

7. niezależny mechanizm ochrony prawnej, który umożliwia badanie nierozstrzygniętych skarg.

c. W przypadku gdy podmiot chce, aby jego przywileje wynikające z Tarczy Prywatności 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 w zgłoszeniu samocertyfikacji i zobowiązać się do współpracy z zainteresowanym organem lub zainteresowanymi organami UE zgodnie z obowiązującymi zasadami uzupełniającymi dotyczącymi danych o zasobach ludzkich i dotyczącymi 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.

d. Departament będzie prowadzić wykaz podmiotów uczestniczących w programie Tarczy Prywatności, które złożyły wypełnione zgłoszenie samocertyfikacji, zapewniając sobie w ten sposób przywileje wynikające z Tarczy Prywatności, i będzie również aktualizować ten wykaz na podstawie corocznych zgłoszeń samocertyfikacji i zawiadomień otrzymanych na podstawie zasady uzupełniającej dotyczącej rozstrzygania sporów i egzekwowania przepisów prawa. Tego rodzaju zgłoszenia samocertyfikacji muszą być składane co najmniej raz w roku; w przeciwnym razie podmiot zostanie wykreślony z wykazu podmiotów uczestniczących w programie Tarczy Prywatności i pozbawiony przywilejów. Zarówno wykaz podmiotów uczestniczących w programie Tarczy Prywatności, jak i zgłoszenia samocertyfikacji przez podmioty będą podawane do wiadomości publicznej. Wszystkie podmioty, które Departament umieścił w wykazie podmiotów uczestniczących w programie Tarczy Prywatności, muszą także podać w opublikowanych przez siebie odpowiednich oświadczeniach dotyczących polityki ochrony prywatności informację o tym, że przestrzegają zasady Tarczy

Prywatności. Jeśli polityka ochrony prywatności jest dostępna na stronie internetowej podmiotu, musi znaleźć się w niej link do strony internetowej Departamentu poświęconej Tarczy Prywatności oraz link do strony internetowej lub formularza skargi w ramach niezależnego mechanizmu ochrony prawnej, który umożliwia rozpoznanie nierozstrzygniętych skarg.

e. Zasady ochrony prywatności mają zastosowanie niezwłocznie po certyfikacji. Uznając, że zasady wpłyną na stosunki handlowe z osobami trzecimi, podmioty, które dokonają certyfikacji do celów ram Tarczy Prywatności w ciągu dwóch pierwszych miesięcy od momentu, w którym ramy te staną się skuteczne, zapewnią zgodność istniejących stosunków handlowych z osobami trzecimi z zasadami odpowiedzialności za wtórne przekazywanie danych jak najszybciej, a w żadnym razie nie później niż dziewięć miesięcy od daty certyfikacji do celów Tarczy Prywatności. W czasie tego okresu przejściowego, w którym podmioty przekazują dane osobom trzecim, (i) stosują one zasady ogłoszenia i wyboru oraz (ii) w przypadku danych osobowych przekazywanych osobie trzeciej działającej w charakterze przedstawiciela upewniają się, że przedstawiciel jest zobowiązany do zapewnienia przynajmniej takiego samego poziomu ochrony, jaki jest wymagany w zasadach.

f. Podmiot musi podporządkować zasadom Tarczy Prywatności wszystkie dane osobowe otrzymane z UE w oparciu o Tarczę Prywatności. Zobowiązanie do przestrzegania zasad Tarczy Prywatności nie jest ograniczone czasowo w odniesieniu do danych osobowych otrzymanych w okresie, w którym podmiot korzysta z przywilejów wynikających z Tarczy Prywatności. 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 programie Tarczy Prywatności. Podmiot, który wycofuje się z programu Tarczy Prywatności, lecz chce zatrzymać tego rodzaju dane, musi corocznie potwierdzać Departamentowi swoje zobowiązanie do stosowania zasad lub zapewniania „odpowiedniej" ochrony danych za pomocą innych zatwierdzonych środków (na przykład stosując umowę w pełni odzwierciedlającą wymogi odpowiednich standardowych klauzul umownych przyjętych przez Komisję Europejską); w przeciwnym razie podmiot musi zwrócić lub usunąć dane. Podmiot, który wycofuje się z programu Tarczy Prywatności musi usunąć z każdej odpowiedniej polityki ochrony prywatności wszelkie odniesienia do Tarczy Prywatności, które sugerują, że podmiot wciąż aktywnie uczestniczy w programie Tarczy Prywatności i jest uprawniony do wynikających z niego przywilejów.

g. Podmiot, który przestanie istnieć jako odrębny podmiot prawny w wyniku połączenia lub przejęcia, musi zawiadomić o tym Departament z wyprzedzeniem. Zawiadomienie powinno także zawierać informację o tym, czy podmiot przejmujący albo podmiot powstały w wyniku połączenia się przedsiębiorstw (i) będzie w dalszym ciągu związany zasadami Tarczy Prywatności na skutek działania prawa regulującego przejęcie bądź połączenie czy też (ii) zamierza dokonać samocertyfikacji potwierdzającej przestrzeganie zasad Tarczy Prywatności bądź zastosować inne gwarancje, takie jak umowa pisemna, które zapewnią przestrzeganie zasad Tarczy Prywatności. W przypadku gdy ani ppkt (i) ani (ii) nie ma zastosowania, wszelkie dane osobowe uzyskane w ramach Tarczy Prywatności muszą zostać bezzwłocznie usunięte.

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

7. **Kontrola**

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

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 z wymogami.

c. W ramach samooceny kontrola taka musi wykazać, że opublikowana polityka ochrony prywatności danego podmiotu dotycząca danych osobowych otrzymanych z UE jest właściwa, kompleksowa, umieszczona w wyraźnym miejscu, w pełni wprowadzona w życie oraz dostępna. Podmiot musi także wykazać, że jego polityka ochrony prywatności jest zgodna z zasadami Tarczy Prywatności; że osoby fizyczne są informowane o wszelkich wewnętrznych niezależnych mechanizmach rozpatrywania skarg oraz niezależnych mechanizmach składania skarg; że stosuje ona odpowiednie procedury szkoleń pracowników we wprowadzaniu w życie polityki ochrony prywatności i karania pracowników w przypadku jej nieprzestrzegania; oraz że stosuje ona wewnętrzne

procedury okresowego przeprowadzania przedmiotowych przeglądów zgodności z powyższym. Oświadczenie potwierdzające samoocenę musi zostać podpisane przez członka podmiotu zajmującego wysokie stanowisko 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, przegląd taki musi wykazać, że polityka podmiotu w zakresie ochrony prywatności dotycząca danych osobowych otrzymanych z UE jest zgodna z zasadami Tarczy Prywatności oraz że zasady te są przestrzegane, a osoby fizyczne informowane o procedurach wnoszenia 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 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.

e. Podmioty muszą zachowywać dokumenty dotyczące wdrażania praktyk ochrony prywatności w ramach Tarczy Prywatności oraz udostępniać je na żądanie, w toku dochodzenia bądź badania skargi dotyczącej nieprzestrzegania zasad, niezależnemu organowi 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 Tarczy Prywatności 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 ([1]);

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, 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 przeorganizować 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.

([1]) 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. 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.

ii. Jeżeli poufne informacje handlowe można łatwo oddzielić od innych danych osobowych będących przedmiotem wniosku o udostępnienie danych, podmiot powinien przeorganizować 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 dyrektywy 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

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

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

i. Termin na odpowiedź

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 Tarczy Prywatności

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 Tarczą Prywatności, przekazanie takich danych jest objęte ochroną zapewnioną w ramach Tarczy Prywatności. W takich przypadkach kwestie związane z gromadzeniem informacji i ich przetwarzaniem przed przekazaniem będą regulowały przepisy prawa krajowego państwa 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 Tarczy Prywatności mają zastosowanie wyłącznie w przypadku przekazywania indywidualnie zidentyfikowanych 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 ogłoszenia i wyboru

i. Amerykański podmiot, który otrzymał informacje na temat pracownika z UE zgodnie z Tarczą Prywatności, może ujawnić takie informacje osobom trzecim lub korzystać z nich w innych celach wyłącznie zgodnie z zasadami ogłoszenia 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

Zasada uzupełniająca 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 Unii Europejskiej muszą oczywiście przestrzegać przepisów krajowych w tym obszarze i zapewnić pracownikom z Unii Europejskiej 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 Tarczą Prywatności 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 Tarczy Prywatności. 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 Tarczą Prywatności, który korzysta z danych o unijnych zasobach ludzkich przekazanych przez Unię Europejską w kontekście stosunku pracy i który zamierza objąć transfery takich danych Tarczą Prywatności, musi zobowiązać się do współpracy w stosownych dochodzeniach oraz do przestrzegania wskazówek organów UE w tym zakresie.

e. Stosowanie zasady odpowiedzialności za wtórne przekazywanie

W przypadku wystąpienia sporadycznych, związanych z zatrudnieniem potrzeb operacyjnych podmiotu uczestniczącego w programie Tarczy Prywatności dotyczących danych osobowych przekazywanych zgodnie z Tarczą Prywatności, 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 osobą trzecią, pomimo że w normalnych warunkach byłoby to wymagane zgodnie z zasadą odpowiedzialności za wtórne przekazywanie, pod warunkiem że podmiot uczestniczący w programie Tarczy Prywatności zapewnił zgodność z zasadami ogłoszenia i wyboru.

10. **Obowiązkowe umowy dotyczące wtórnego 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 Tarczą Prywatności.

ii. Administratorzy danych w Unii Europejskiej 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 Tarczą Prywatności, czy też nie. Celem umowy jest zagwarantowanie, by podmiot przetwarzający:

1. podejmował działania wyłącznie na polecenie 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 wtórnego 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 podmioty objęte Tarczą Prywatności zapewniają odpowiedni poziom ochrony, zawierane z takimi podmiotami umowy dotyczące zwykłego przetwarzania danych nie wymagają wcześniejszego zatwierdzenia (lub są automatycznie zatwierdzane przez państwa członkowskie UE), w odróżnieniu od umów z odbiorcami, którzy nie są objęci Tarczą Prywatności lub którzy z innych względów nie zapewniają odpowiedniego poziomu ochrony.

b. Przekazywanie danych w ramach kontrolowanej grupy korporacji lub jednostek

Jeżeli chodzi o przekazywanie danych osobowych między dwoma administratorami danych w ramach kontrolowanej grupy korporacji lub jednostek, zgodnie z zasadą odpowiedzialności za wtórne 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 podmiot uczestniczący w programie Tarczy Prywatności pozostaje odpowiedzialny za zapewnienie zgodności z zasadami.

c. Transfery między administratorami danych

Jeżeli chodzi o transfery między administratorami danych, administrator danych będący odbiorcą nie musi być podmiotem uczestniczącym w programie Tarczy Prywatności ani nie musi zapewniać możliwości skorzystania z niezależnego mechanizmu ochrony prawnej. Podmiot uczestniczący w programie Tarczy Prywatności musi podpisać umowę z będącym osobą trzecią odbiorcą – administratorem danych – który zapewnia poziom ochrony równoważny poziomowi zapewnianemu zgodnie z Tarczą Prywatności, przy czym administrator będący osobą trzecią nie musi być podmiotem uczestniczącym w programie Tarczy Prywatności ani nie musi zapewniać możliwości skorzystania z niezależnego mechanizmu ochrony prawnej, o ile zapewni możliwość skorzystania z równoważnego mechanizmu.

11. **Rozstrzyganie sporów i egzekwowanie**

a. W zasadzie dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności ustanowiono wymogi w zakresie egzekwowania zasad Tarczy Prywatności. 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 Tarczy Prywatności 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 wykonawczymi dotyczącymi nadzoru stanowiącymi podstawę prawną rozpatrywania skarg wnoszonych przez osoby fizyczne i rozstrzygania sporów; oraz (iii) podjęcie zobowiązania do współpracy z organami ochrony danych mającymi swoją siedzibę w Unii Europejskiej 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 zwrócić uwagę na fakt, że wymogi określone w zasadzie dotyczącej ochrony prawnej, egzekwowania prawa oraz odpowiedzialności są uzupełniające względem wymogu, zgodnie z którym działania wynikające z samoregulacji muszą być wykonalne na podstawie sekcji 5 ustawy o Federalnej Komisji Handlu,

w której to sekcji wprowadza się zakaz podejmowania nieuczciwych lub wprowadzających w błąd działań, lub innych ustaw lub przepisów wykonawczych zakazujących podejmowania takich działań.

c. Aby ułatwić zapewnienie zgodności z zobowiązaniami Tarczy Prywatności i aby wesprzeć stosowne podmioty w zarządzaniu programem, podmioty – a także stosowane przez nie niezależne mechanizmy ochrony prawnej – muszą przekazywać informacje dotyczące Tarczy Prywatności 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. Konsumentów 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 konsumenta 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. Organy ds. rozstrzygania sporów powinny rozpatrzeć każdą skargę przekazaną przez osoby fizyczne, chyba że taka skarga będzie w oczywisty sposób bezpodstawna lub niepoważna. Podmiot 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 Tarczy Prywatności. 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 Tarczy Prywatności oraz na temat usług świadczonych przez siebie w ramach Tarczy Prywatności. Takie informacje muszą obejmować: 1) informacje na temat wymogów dotyczących niezależnych mechanizmów ochrony prawnej ustanowionych w zasadach Tarczy Prywatności lub łącze do takich informacji; 2) łącze do strony internetowej Departamentu poświęconej Tarczy Prywatności; 3) wyjaśnienie, że usługi rozwiązywania sporów w ramach Tarczy Prywatności są świadczone na rzecz osób fizycznych nieodpłatnie; 4) opis procedury składania skargi dotyczącej kwestii związanych z Tarczą Prywatności; 5) wyznaczenie terminu na rozpoznanie skarg dotyczących Tarczy Prywatności; 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. W sprawozdaniu rocznym należy zawrzeć: 1) informacje o łącznej liczbie skarg powiązanych z Tarczą Prywatności otrzymanych w roku sprawozdawczym; 2) informacje o charakterze otrzymanych skarg; 3) informacje o jakości mechanizmu rozstrzygania sporów, np. informacje o czasie niezbędnym do rozpatrzenia skarg; oraz 4) informacje o działaniach podjętych w rezultacie otrzymania skarg, w szczególności o liczbie i rodzaju 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 podmiot uczestniczący w programie Tarczy Prywatności 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 ([1]), lub w przypadku zarzutu dotyczącego adekwatności Tarczy Prywatności. W przypadku wszczęcia postępowania arbitrażowego panel ds. Tarczy Prywatności (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. Osoba fizyczna i podmioty uczestniczące w programie Tarczy Prywatności będą mogły wystąpić o przeprowadzenie kontroli sądowej i wykonanie orzeczeń arbitrażowych zgodnie z prawem amerykańskim, tj. federalną ustawą o arbitrażu.

([1]) Sekcja I.5 zasad.

e. Środki ochrony prawnej i sankcje

Zastosowanie jakichkolwiek środków ochrony prawnej zapewnianych przez 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 nieprzestrzegania zasad do wiadomości publicznej oraz nakazanie usunięcia danych w określonych przypadkach ([1]). Inne sankcje mogą obejmować zawieszenie lub cofnięcie zezwolenia na prowadzenie działalności, przyznanie osobom fizycznym odszkodowania z tytułu szkody poniesionej wskutek nieprzestrzegania zasad oraz zabezpieczenie roszczenia. 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 podmioty uczestniczące w programie Tarczy Prywatności z obowiązku zastosowania się do wydanych przez nie orzeczeń i decyzji oraz powiadomić o tym fakcie Departament.

f. Działania FTC

FTC zobowiązał się do priorytetowego rozpatrywania zgłoszeń dotyczących domniemanego nieprzestrzegania zasad przekazywanych przez: (i) organy samoregulacyjne ds. prywatności i inne niezależne organy ds. rozpatrywania 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 niezgodnych z prawdą deklaracji o przestrzeganiu zasad Tarczy Prywatności lub o przynależności do Tarczy Prywatności składanych przez podmioty, które nie figurują już w wykazie podmiotów uczestniczących w programie Tarczy Prywatności 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 przynależności do Tarczy Prywatności.

g. Uporczywe nieprzestrzeganie zasad

i. Jeżeli dany podmiot będzie uporczywie nie przestrzegać zasad, straci możliwość dalszego korzystania z Tarczy Prywatności. Podmioty, które uporczywie nie przestrzegały zasad, zostaną usunięte przez Departament z wykazu podmiotów uczestniczących w programie Tarczy Prywatności i będą zobowiązane do zwrócenia lub usunięcia danych osobowych, które otrzymały w ramach Tarczy Prywatności.

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 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 takich przypadkach 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 podmiotów uczestniczących w programie Tarczy Prywatności w odpowiedzi na dowolne otrzymane powiadomienie o uporczywym nieprzestrzeganiu zasad, niezależnie

([1]) 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 Tarczy Prywatności.

od tego, czy powiadomienie to zostanie przekazane przez sam podmiot, samoregulacyjny organ ds. prywatności lub inny niezależny organ ds. rozstrzygania sporów lub organ rządowy, po uprzednim zapewnieniu podmiotowi, który nie wywiązał się z obowiązku przestrzegania zasad, możliwości ustosunkowania się do tych zarzutów w terminie 30 dni. Dlatego też prowadzony przez Departament wykaz podmiotów uczestniczących w programie Tarczy Prywatności będzie zawierał przejrzyste informacje na temat tego, które podmioty mogą nadal korzystać z przywilejów wynikających z Tarczy Prywatności.

iv. Podmiot ubiegający się o uczestnictwo w organie samoregulacyjnym w celu ponownego zakwalifikowania się do objęcia Tarczą Prywatności musi przedstawić temu organowi wyczerpujące informacje na temat swojego wcześniejszego udziału w Tarczy Prywatności.

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 rozsądnych 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* realizowanego na szczeblu centralnym, np. usługi preferencji pocztowych świadczonej przez Stowarzyszenie Marketingu Bezpośredniego (ang. Direct Marketing Association's Mail Preference Service). Podmioty korzystające z usługi preferencji pocztowych świadczonej przez Stowarzyszenie Marketingu Bezpośredniego powinny informować konsumentów, którzy nie chcą otrzymywać informacji handlowych, o dostępności tej usługi. 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. Na podstawie art. 26 dyrektywy dane osobowe mogą zostać przekazane „do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony w znaczeniu art. 25 ust. 2", o ile (i) jest to konieczne do świadczenia usług żądanych przez konsumenta lub do spełnienia warunków określonych w umowie, np. warunków umowy dotyczącej programu lojalnościowego „frequent flyer"; lub (ii) konsument jednoznacznie wyraził na to zgodę. Podmioty amerykańskie uczestniczące w programie Tarczy Prywatności zapewniają odpowiednią ochronę danych osobowych, dlatego też mogą przyjmować transfery danych z UE bez konieczności spełnienia tych lub innych warunków ustanowionych w art. 26 dyrektywy. Ponieważ w programie Tarczy Prywatności ustanowiono określone zasady postępowania z danymi wrażliwymi, takie informacje (które mogą być gromadzone np. w związku z koniecznością udzielenia klientom pomocy fizycznej) mogą zostać uwzględnione w transferach przekazywanych uczestnikom programu Tarczy Prywatności. 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 obowiązującego w państwie członkowskim UE lub zasad Tarczy Prywatności

Przepisy obowiązujące w państwie członkowskim mają zastosowanie przy gromadzeniu danych osobowych i przy wszelkim przetwarzaniu takich danych przed ich przekazaniem Stanom Zjednoczonym. Zasady Tarczy Prywatności 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 Tarczą Prywatności 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 badań klinicznych

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

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 stosowania i skuteczności produktów

Przedsiębiorstwo zajmujące się wytwarzaniem produktów farmaceutycznych i wyrobów medycznych nie ma obowiązku stosowania zasad Tarczy Prywatności w zakresie zasad powiadomienia, wyboru, odpowiedzialności za wtórne przekazywanie danych i dostępu przy podejmowaniu działań dotyczących monitorowania bezpieczeństwa stosowania 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 ustawowych. 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

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 nie stanowi przypadku przekazania danych osobowych, który podlegałby zasadom Tarczy Prywatności.

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

a. Podmiot musi stosować przyjęte w ramach Tarczy Prywatności zasady bezpieczeństwa, integralności danych i ograniczenia celowego oraz zasadę dotyczącą ochrony prawnej, egzekwowania prawa oraz odpowiedzialności w odniesieniu do danych osobowych pochodzących z ogólnodostępnych źródeł. Zasady te mają 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 wtórne 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 wtórne przekazywanie w odniesieniu do ogólnodostępnych informacji nie jest co do zasady konieczne, chyba że osoba dokonująca przeniesienia 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 Tarczy Prywatności.

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 w programie Tarczy Prywatności 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 w programie Tarczy Prywatności, informacje, które zostały ujawnione przez Wspólnotę Wywiadowczą, oraz inne informacje mogą być wykorzystywane przy przeprowadzaniu corocznego wspólnego przeglądu funkcjonowania Tarczy Prywatności 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 programie Tarczy Prywatności zgodnie z zasadą dotyczącą ochrony prawnej, egzekwowania prawa oraz odpowiedzialności. Opisana poniżej możliwość przeprowadzenia arbitrażu ma zastosowanie do niektórych „pozostałych" roszczeń dotyczących danych objętych Tarczą Prywatności UE-USA. Celem tego rozwiązania jest zapewnienie możliwości skorzystania przez osoby fizyczne na zasadzie dobrowolności z szybkiego, niezależnego i sprawiedliwego mechanizmu rozstrzygania przypadków domniemanych naruszeń zasad, które nie zostały rozstrzygnięte w ramach żadnego z pozostałych mechanizmów Tarczy Prywatności, o ile ustanowiono takie mechanizmy.

A. **Zakres**

Osoba fizyczna może skorzystać z arbitrażu, aby ustalić – w odniesieniu do pozostałych roszczeń – czy podmiot uczestniczący w programie Tarczy Prywatności 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 Tarczy Prywatności.

B. **Dostępne środki ochrony prawnej**

W przypadku wszczęcia postępowania arbitrażowego panel ds. Tarczy Prywatności (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 jedyne uprawnienia przysługujące panelowi arbitrażowemu w odniesieniu do środków ochrony prawnej. W czasie obrad nad tym, jakie środki ochrony prawnej należy zastosować w danym przypadku, panel arbitrażowy musi wziąć pod uwagę inne środki ochrony prawnej, które zostały już zastosowane w ramach innych mechanizmów Tarczy Prywatności. 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 sekcji III podsekcja 11 lit. d) ppkt (i) zasad; 2) skorzystać z bezpłatnego niezależnego mechanizmu ochrony prawnej przewidzianego w zasadach; 3) przekazać stosowne informacje Departamentowi Handlu za pośrednictwem odpowiedniego organu ochrony danych i zapewnić Departamentowi Handlu możliwość podjęcia działań w celu rozwiązania danego problemu w terminach określonych w piśmie Urzędu ds. Handlu Międzynarodowego w Departamencie Handlu – 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 postępowania arbitrażowego nie można przeprowadzić, jeżeli unijny organ ochrony danych: 1) jest organem właściwym zgodnie z sekcją III.5 lub III.9 zasad; 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]) Sekcja I.5 zasad.

E. **Kontrola i wykonanie**

Osoby fizyczne i podmioty uczestniczące w programie Tarczy Prywatności będą mogły wystąpić o przeprowadzenie kontroli sądowej i wykonanie orzeczeń arbitrażowych zgodnie z prawem amerykańskim, tj. federalną ustawą o arbitrażu ([1]). Wszelkie tego typu sprawy muszą być wnoszone przed federalny sąd pierwszej instancji, którego właściwość miejscowa obejmuje główne miejsce prowadzenia działalności podmiotu uczestniczącego w programie Tarczy Prywatności.

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

F. **Skład arbitrażowy**

Strony wybiorą arbitrów z wykazu arbitrów omówionego poniżej.

Zgodnie z obowiązującym prawem Departament Handlu Stanów Zjednoczonych i Komisja Europejska opracują wykaz co najmniej 20 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 wystąpi uzasadniona przyczyna skreślenia z wykazu, z możliwością przedłużenia na kolejny okres obejmujący trzy lata;

2) nie podlegają żadnym instrukcjom wydanym przez stronę, dowolny podmiot uczestniczący w programie Tarczy Prywatności, Stany Zjednoczone, 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 w zakresie unijnego prawa ochrony danych.

G. **Procedury arbitrażowe**

Zgodnie z obowiązującym prawem, w terminie sześciu miesięcy od przyjęcia decyzji w sprawie odpowiedniej ochrony danych osobowych, Departament Handlu i Komisja Europejska uzgodnią przyjęcie istniejącego, ugruntowanego zbioru amerykańskich procedur arbitrażowych (takich jak AAA lub JAMS) na potrzeby uregulowania postępowań przed panelem ds. Tarczy Prywatności, 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;

([1]) 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 nieruchomości położonej za granicą, przewiduje podjęcie działać lub wykonanie za granicą lub jest w inny zasadny sposób powiązany z jednym państwem obcym lub większą ich liczbą". 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 innej strony 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.

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 Stanów Zjednoczonych, 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 Unii Europejskiej organy ochrony danych UE 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 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 konieczności dozwolone może być przeprowadzenie szczegółowego postępowania dowodowego (and. 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.

H. **Koszty**

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

Zgodnie z mającym zastosowanie prawem Departament Handlu ułatwi utworzenie funduszu, na który podmioty uczestniczące w programie Tarczy Prywatności będą zobowiązane wpłacać roczną składkę proporcjonalną do ich wielkości, która to składka pokryje koszty arbitrażu, w tym honorarium arbitra, do maksymalnej kwoty („górnej granicy"), po konsultacji z Komisją Europejską. Funduszem będzie zarządzać osoba trzecia, która będzie regularnie przedstawiać sprawozdania z działalności funduszu. Podczas corocznego przeglądu Departament Handlu i Komisja Europejska dokonają przeglądu funkcjonowania funduszu, w tym konieczności dostosowania kwoty składek lub maksymalnych kwot, oraz przeanalizują między innymi liczbę postępowań arbitrażowych oraz ich koszty i czas trwania, przy czym obie strony zgadzają się, że nie zostaną nałożone żadne nadmierne obciążenia finansowe na podmioty uczestniczące w programie Tarczy Prywatności. Honoraria pełnomocnika nie są objęte niniejszym przepisem ani żadnym funduszem ustanowionym na jego mocy.

ZAŁĄCZNIK III

Pismo amerykańskiego sekretarza stanu Johna Kerry'ego

Dnia 7 lipca 2016 r.

Szanowna Pani Komisarz!

Z zadowoleniem stwierdzam, że udało się nam osiągnąć porozumienie w sprawie Tarczy Prywatności UE-USA, w której ramach zostanie powołany rzecznik, za pośrednictwem którego organy w Unii Europejskiej będą mogły składać w imieniu osób fizycznych z UE wnioski dotyczące praktyk Stanów Zjednoczonych w zakresie rozpoznania radioelektronicznego.

W dniu 17 stycznia 2014 r. prezydent Barack Obama zapowiedział ważne reformy dotyczące wywiadu zawarte w dyrektywie politycznej Prezydenta nr 28 (PPD-28). Na mocy tej dyrektywy wyznaczyłem podsekretarz stanu Catherine A. Novelli, która pełni również urząd starszego koordynatora ds. międzynarodowej dyplomacji w dziedzinie technologii informacyjnej, na osobę odpowiedzialną za kontakty z rządami zagranicznymi, które pragną zgłosić swoje obawy dotyczące działań z zakresu rozpoznania radioelektronicznego prowadzonych przez Stany Zjednoczone. Wzorując się na tych doświadczeniach, powołałem Urząd Rzecznika ds. Tarczy Prywatności zgodnie z warunkami określonymi w załączniku A, które zostały zaktualizowane od czasu mojego pisma z dnia 22 lutego 2016 r. Powierzyłem pełnienie tej funkcji podsekretarz Novelli. Podsekretarz Novelli działa niezależnie od Wspólnoty Wywiadowczej Stanów Zjednoczonych, a ja jestem jej bezpośrednim przełożonym.

Poleciłem moim pracownikom, aby przeznaczyli niezbędne środki na wdrożenie tego nowego mechanizmu, i jestem pewien, że będzie to skuteczny środek, który przyczyni się do rozwiania obaw osób fizycznych z Unii.

Z poważaniem

John F. Kerry

Załącznik A

Urząd Rzecznika ds. Tarczy Prywatności UE-USA w odniesieniu do rozpoznania radioelektronicznego

Uznając znaczenie ram Tarczy Prywatności UE-USA w niniejszym memorandum przedstawiono proces wdrażania nowego mechanizmu, zgodnie z dyrektywą polityczną Prezydenta nr 28 (PPD-28), w odniesieniu do rozpoznania radioelektronicznego ([1]).

W dniu 17 stycznia 2014 r. prezydent Obama wygłosił przemówienie, w którym zapowiedział ważne reformy dotyczące wywiadu. W przemówieniu tym prezydent zaznaczył, że „nasze wysiłki pomagają chronić nie tylko nasz naród, ale również naszych przyjaciół i sojuszników. Nasze działania będą skuteczne tylko wtedy, gdy zwykli obywatele w innych państwach będą mieli pewność, że Stany Zjednoczone szanują także ich prywatność". Prezydent Obama zapowiedział wydanie nowej dyrektywy prezydenckiej, PPD-28, w celu jasnego określenia, co robimy, a czego nie, jeżeli chodzi o obserwację prowadzoną za granicą.

Na podstawie sekcji 4 lit. d) dyrektywy politycznej Prezydenta nr 28 Sekretarz Stanu jest zobowiązany wyznaczyć „starszego koordynatora ds. międzynarodowej dyplomacji w dziedzinie technologii informacyjnej" („starszy koordynator"), który będzie pełnił funkcję „osoby odpowiedzialnej za kontakty z rządami zagranicznymi, które pragną zgłosić swoje obawy dotyczące działań z zakresu rozpoznania radioelektronicznego prowadzonych przez Stany Zjednoczone". Od stycznia 2015 r. podsekretarz C. Novelli pełni funkcję starszego koordynatora.

W niniejszym memorandum opisuje się nowy mechanizm, który będzie stosował starszy koordynator, aby ułatwić rozpatrywanie wniosków dotyczących dostępu ze względów bezpieczeństwa narodowego do danych przekazywanych Stanom Zjednoczonym przez Unię Europejską zgodnie z Tarczą Prywatności, standardowymi klauzulami umownymi, wiążącymi regułami korporacyjnymi, „odstępstwami" ([2]) lub „możliwymi przyszłymi odstępstwami" ([3]) za pomocą kanałów ustanowionych na mocy obowiązujących przepisów i polityki Stanów Zjednoczonych oraz aby ułatwić udzielanie odpowiedzi na te wnioski.

1. **Rzecznik ds. Tarczy Prywatności.** Starszy koordynator będzie pełnił rolę Rzecznika ds. Tarczy Prywatności i wyznaczy dodatkowych urzędników Departamentu Stanu, którzy będą pomagać mu w wykonywaniu obowiązków wyszczególnionych w niniejszym memorandum. (Koordynator i ewentualnie urzędnicy pełniący takie obowiązki będą zwani w dalszej części niniejszego dokumentu „Rzecznikiem ds. Tarczy Prywatności"). Rzecznik ds. Tarczy Prywatności będzie ściśle współpracował z odpowiednimi urzędnikami z innych departamentów i agencji, którzy są odpowiedzialni za rozpatrywanie wniosków zgodnie z obowiązującymi przepisami i polityką Stanów Zjednoczonych. Rzecznik działa niezależnie od Wspólnoty Wywiadowczej. Rzecznik podlega bezpośrednio Sekretarzowi Stanu, który zapewni, by wykonywał on zadania w sposób obiektywny i nie ulegał niepożądanym wpływom, który mogłyby wywrzeć skutek na odpowiedź, której należy udzielić.

2. **Skuteczna koordynacja.** Rzecznik ds. Tarczy Prywatności będzie mógł skutecznie korzystać z mechanizmów oraz koordynować działania organów nadzoru, co zostało opisane poniżej, na potrzeby zapewnienia, by odpowiedź na

([1]) Pod warunkiem że decyzja Komisji w sprawie adekwatności ochrony przewidzianej przez Tarczę Prywatności UE-USA ma zastosowanie do Islandii, Liechtensteinu i Norwegii, zasady Tarczę Prywatności UE-USA obejmują zarówno Unię Europejską, jak i te trzy kraje. Z tego względu odniesienia do Unii Europejskiej i jej państw członkowskich należy rozumieć jako obejmujące Islandię, Liechtenstein i Norwegię.

([2]) „Odstępstwa" w tym kontekście oznaczają przekazanie na zasadach handlowych, które ma miejsce pod warunkiem że: a) osoba, której dane dotyczą, udzieliła jednoznacznej zgody na proponowane przekazanie danych; lub b) przekazanie danych jest konieczne do wykonania umowy zawartej między osobą, której dane dotyczą, a administratorem danych lub do wdrożenia środków poprzedzających zawarcie umowy na wniosek osoby, której dane dotyczą; lub c) przekazanie danych jest konieczne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą, między administratorem danych a osobą trzecią; lub d) przekazanie danych jest konieczne lub wymagane prawnie z ważnych względów interesu publicznego lub w celu ustalenia, zgłoszenia lub obrony roszczeń prawnych; lub e) przekazanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą; lub f) przekazanie danych następuje z rejestru, który ma służyć, zgodnie z obowiązującymi przepisami ustawowymi lub wykonawczymi, jako źródło informacji dla ogółu społeczeństwa i do którego mają wgląd albo wszystkie jednostki, albo każda osoba, która wykaże uzasadniony interes, w zakresie, w jakim warunki określone przez prawo odnośnie do wglądu do takiego rejestru zostały w danym przypadku spełnione.

([3]) „Możliwe przyszłe odstępstwa" w tym kontekście oznaczają przekazanie na zasadach handlowych, które ma miejsce pod jednym z następujących warunków, o ile dany warunek stanowi podstawę prawną do przekazania danych osobowych między Unią Europejską a Stanami Zjednoczonymi: a) osoba, której dane dotyczą, udzieliła wyraźnej zgody na proponowane przekazanie danych, po tym jak została poinformowana o możliwych zagrożeniach związanych z takim przekazaniem danych z powodu braku decyzji w sprawie odpowiedniej ochrony danych osobowych i odpowiednich gwarancji; lub b) przekazanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innych osób, w przypadku gdy osoby, których dane dotyczą, są fizycznie lub prawnie niezdolne do udzielenia zgody; lub c) w przypadku przekazania danych państwu trzeciemu lub organizacji międzynarodowej – gdy nie mają zastosowania inne odstępstwa lub możliwe przyszłe odstępstwa – jedynie gdy przekazanie nie odbywa się wielokrotnie, dotyczy wyłącznie ograniczonej liczby osób, których dane dotyczą, jest niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, które nie są podrzędne wobec interesów lub praw i wolności osoby, której dane dotyczą, w przypadku gdy administrator ocenił wszystkie okoliczności związane z przekazaniem danych i na podstawie tej oceny przedstawił odpowiednie gwarancje w odniesieniu do ochrony danych osobowych.

wnioski przekazane przez unijny organ rozpatrujący skargi osób fizycznych była oparta na odpowiednich informacjach. Jeżeli wniosek dotyczy zgodności obserwacji z prawem Stanów Zjednoczonych, Rzecznik ds. Tarczy Prywatności będzie mógł współpracować z jednym z niezależnych organów nadzoru, którym przysługują uprawnienia dochodzeniowe.

a. Rzecznik ds. Tarczy Prywatności będzie ściśle współpracował z innymi urzędnikami rządu Stanów Zjednoczonych, w tym odpowiednimi niezależnymi organami nadzoru, w celu zapewnienia, aby wypełnione wnioski zostały rozpatrzone i rozstrzygnięte zgodnie z obowiązującym prawem i politykami. W szczególności Rzecznik ds. Tarczy Prywatności będzie mógł ściśle współpracować z Urzędem Dyrektora Krajowych Służb Wywiadowczych, Departamentem Sprawiedliwości oraz innymi departamentami i agencjami zaangażowanymi w razie potrzeby w ochronę bezpieczeństwa narodowego Stanów Zjednoczonych oraz Inspektorami Generalnymi, urzędnikami ds. ustawy o dostępie do informacji publicznej oraz urzędnikami Biura Wolności Obywatelskich i Ochrony Prywatności.

b. Rząd Stanów Zjednoczonych będzie opierał się na mechanizmach na rzecz koordynowania i nadzorowania kwestii związanych z bezpieczeństwem narodowym we wszystkich departamentach i agencjach w celu zapewnienia, by Rzecznik ds. Tarczy Prywatności mógł udzielać odpowiedzi w rozumieniu sekcji 4 lit. e) na wnioski złożone na podstawie sekcji 3 lit. b).

c. Rzecznik ds. Tarczy Prywatności może kierować sprawy związane ze składanymi wnioskami do Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi do rozpatrzenia.

3. **Składanie wniosków.**

a. Wniosek zostanie początkowo przekazany organom nadzoru w państwach członkowskich właściwym w zakresie nadzoru nad krajowymi służbami bezpieczeństwa lub przetwarzania danych osobowych przez organy publiczne. Wniosek zostanie przekazany Rzecznikowi przez scentralizowany organ unijny (zwany dalej łącznie: „unijnym organem rozpatrującym skargi osób fizycznych").

b. Unijny organ rozpatrujący skargi osób fizycznych zapewni kompletność wniosku poprzez poniższe działania:

(i) sprawdzenie tożsamości osoby fizycznej oraz czy dana osoba działa we własnym imieniu czy jako przedstawiciel organizacji rządowej lub międzyrządowej;

(ii) upewnienie się, że wniosek złożono w formie pisemnej i zawiera on następujące informacje podstawowe:

— wszelkie informacje, które stanowią podstawę wniosku,

— charakter informacji lub opis żądania,

— ewentualnie jednostki rządu Stanów Zjednoczonych, które uznaje się za zaangażowane, oraz

— pozostałe środki podjęte w celu uzyskania informacji lub opis żądanie oraz odpowiedź otrzymana w następstwie zastosowania tych środków;

(iii) sprawdzenie, czy wniosek dotyczy danych, w przypadku których można racjonalnie założyć, że zostały przekazane Stanom Zjednoczonym przez UE zgodnie z Tarczą Prywatności, standardowymi klauzulami umownymi, wiążącymi regułami korporacyjnymi, odstępstwami lub możliwymi przyszłymi odstępstwami.

(iv) wstępne określenie, czy wniosek nie jest niepoważny, złożony w celu nękania lub w złej wierze.

c. Wniosek, złożony w celu dalszego rozpatrzenia przez rzecznika ds. Tarczy Prywatności na podstawie niniejszego memorandum, nie musi zawierać informacji, że rząd Stanów Zjednoczonych miał w istocie dostęp do danych wnioskodawcy w ramach działań z zakresu rozpoznania radioelektronicznego.

4. **Zobowiązanie do skontaktowania się z unijnym organem rozpatrującym skargi osób fizycznych, który wniósł wniosek**

a. Rzecznik ds. Tarczy Prywatności poinformuje o otrzymaniu wniosku unijny organ rozpatrujący skargi osób fizycznych, który wniósł wniosek.

b. Rzecznik ds. Tarczy Prywatności przeprowadzi wstępną analizę celem sprawdzenia, czy wniosek został wypełniony zgodnie z sekcją 3 lit. b). Jeżeli rzecznik ds. Tarczy Prywatności zauważy jakiekolwiek uchybienia lub będzie miał jakiekolwiek pytania dotyczące wypełnienia wniosku, będzie dążył do rozstrzygnięcia tych kwestii wspólnie z unijnym organem rozpatrującym skargi osób fizycznych.

c. Jeżeli, aby ułatwić właściwe rozpatrzenie wniosku, Rzecznik ds. Tarczy Prywatności potrzebuje więcej informacji na temat wniosku, lub jeżeli konieczne jest, aby osoba fizyczna, która złożyła wniosek, podjęła określone działania, Rzecznik ds. Tarczy Prywatności poinformuje o tym unijny organ rozpatrujący skargi osób fizycznych.

d. Rzecznik ds. Tarczy Prywatności będzie monitorował status wniosków i w stosownych przypadkach będzie przekazywał aktualne informacje unijnemu organowi rozpatrującemu skargi osób fizycznych.

e. Po złożeniu wniosku zgodnie z procedurą opisaną w sekcji 3 niniejszego memorandum Rzecznik ds. Tarczy Prywatności przekaże w terminie odpowiednią odpowiedź unijnemu organowi rozpatrującemu skargi osób fizycznych, z zastrzeżeniem ciągłego zobowiązania do ochrony informacji zgodnie z obowiązującym prawem i politykami. Rzecznik ds. Tarczy Prywatności przekaże odpowiedź unijnemu organowi rozpatrującemu skargi osób fizycznych, w którym potwierdza, że (i) skarga została właściwie zbadana oraz że (ii) działano zgodnie z przepisami, ustawami, rozporządzeniami wykonawczymi, dyrektywami prezydenckimi i strategiami politycznymi agencji zawierającymi ograniczenia i gwarancje opisane w piśmie Urzędu Dyrektora Krajowych Służb Wywiadowczych, a w przypadku nieprzestrzegania tych regulacji problem ten został rozwiązany. Rzecznik ds. Tarczy Prywatności nie potwierdzi, ani nie zaprzeczy, że dana osoba jest objęta obserwacją, ani nie potwierdzi, że zastosowano specjalne środki zaradcze. Jak wyjaśniono w sekcji 5 wnioski dotyczące ustawy o dostępie do informacji publicznej będą rozpatrywane zgodnie z ustawą i obowiązującymi przepisami.

f. Rzecznik ds. Tarczy Prywatności będzie kontaktował się bezpośrednio z unijnym organem rozpatrującym skargi osób fizycznych, który z kolei będzie odpowiedzialny za kontakty z osobą fizyczną składającą wniosek. Jeżeli bezpośrednia komunikacja jest częścią jednego z podstawowych procesów opisanych poniżej, wówczas taka komunikacja będzie odbywała się zgodnie z obowiązującymi procedurami.

g. Zobowiązania określone w niniejszym memorandum nie będą miały zastosowania do ogólnych twierdzeń, że Tarcza Prywatności UE-USA jest niezgodna z wymogami Unii Europejskiej dotyczącymi ochrony danych. Zobowiązania określone w niniejszym memorandum są realizowane w oparciu o wspólne porozumienie między Komisją Europejską a rządem Stanów Zjednoczonych, zgodnie z którym przyjmuje się, że z uwagi na zakres zobowiązań w ramach tego mechanizmu mogą istnieć ograniczenia co do zasobów, które pojawiają się m.in. w odniesieniu do wniosków opartych na ustawie o dostępie do informacji publicznej. Jeżeli funkcjonowanie Urzędu Rzecznika ds. Tarczy Prywatności wykracza poza rozsądne ograniczenia w zakresie zasobów i uniemożliwia wywiązanie się ze wspomnianych zobowiązań, rząd Stanów Zjednoczonych omówi z Komisją Europejską ewentualne zmiany, które mogą być odpowiednie do sprostania danej sytuacji.

5. **Wnioski o udzielenie informacji.** Wnioski o udostępnienie rejestrów rządu Stanów Zjednoczonych mogą być sporządzane i rozpatrywane zgodnie z ustawą o dostępie do informacji publicznej.

a. Ustawa o dostępie do informacji publicznej zapewnia każdej osobie środki umożliwiające uzyskanie dostępu do istniejących rejestrów agencji federalnych, niezależnie od narodowości wnioskodawcy. Ustawa ta jest skodyfikowana w Kodeksie Stanów Zjednoczonych, tytuł 5 § 552 U.S.C. Ustawa, wraz z dodatkowymi informacjami na temat ustawy o dostępie do informacji publicznej, jest dostępna pod adresem www.FOIA.gov i http://www.justice.gov/oip/foia-resources. Każda agencja zatrudnia głównego urzędnika ds. ustawy o dostępie do informacji publicznej i na swojej ogólnodostępnej stronie internetowej publikuje informacje dotyczące sposobu zwrócenia się z wnioskiem w sprawie tej ustawy do agencji. Agencje prowadzą między sobą konsultacje dotyczące wniosków na podstawie ustawy o dostępie do informacji publicznej dotyczących rejestrów prowadzonych przez inną agencję.

b. Przykładowo:

(i) Urząd Dyrektora Krajowych Służb Wywiadowczych utworzył portal poświęcony ustawie o dostępie do informacji publicznej: http://www.dni.gov/index.php/about-this-site/foia. Portal ten zawiera informacje na temat składania wniosków, sprawdzania statusu złożonego wniosku i dostępu do informacji, które zostały ujawnione i opublikowane przez Urząd Dyrektora Krajowych Służb Wywiadowczych na mocy ustawy o dostępie do informacji publicznej. Portal Urzędu Dyrektora Krajowych Służb Wywiadowczych poświęcony ustawie o dostępie do informacji publicznej zawiera linki do innych stron internetowych dotyczących tej ustawy prowadzonych przez agencje Wspólnoty Wywiadowczej: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

(ii) Urząd ds. Polityki Informacyjnej przy Departamencie Sprawiedliwości zapewnia wyczerpujące informacje na temat ustawy o dostępie do informacji publicznej: http://www.justice.gov/oip. Obejmuje to nie tylko informacje na temat zwracania się do Departamentu Sprawiedliwości z wnioskiem dotyczącym ustawy o dostępie do informacji publicznej, ale także wytyczne dla rządu Stanów Zjednoczonych dotyczące interpretowania i stosowania wymogów w zakresie ustawy o dostępie do informacji publicznej.

c. Na mocy ustawy o dostępie do informacji publicznej dostęp do rządowych rejestrów zależy od pewnych wymienionych wyłączeń. Obejmują one ograniczenia dostępu do niejawnych informacji na temat bezpieczeństwa narodowego, danych osobowych osób trzecich oraz informacji na temat dochodzeń prowadzonych przez organy egzekwowania prawa oraz są porównywalne do ograniczeń nałożonych przez każde państwo członkowskie UE na podstawie własnego prawa dostępu do informacji. Ograniczenia te odnoszą się zarówno do Amerykanów, jak i osób innej narodowości.

d. Sporne decyzje dotyczące udostępniania rejestrów będących przedmiotem wniosku zgodnie z ustawą o dostępie do informacji publicznej można zaskarżyć administracyjnie, a następnie w sądzie federalnym. Sąd jest zobowiązany na nowo ustalić, czy udostępnienie rejestrów zostały wstrzymane zasadnie, tytuł 5 § 552(a)(4)(B) U. S.C., oraz może nakazać rządowi zapewnienie dostępu do rejestrów. W niektórych sprawach sąd obalił stanowisko rządu, zgodnie z którym nie należało dopuścić do ujawnienia informacji z uwagi na ich niejawny charakter. Mimo że nie ma możliwości zasądzenia odszkodowania pieniężnego, sąd może zarządzić wypłatę honorariów pełnomocnikom procesowym.

6. **Wnioski dotyczące dalszych działań.** Wniosek dotyczący naruszenia prawa lub innego wykroczenia zostanie przekazany odpowiedniemu organowi rządowemu Stanów Zjednoczonych, m.in. niezależnym organom nadzoru, które mają uprawnienia do badania danego wniosku i zdolność do rozwiązywania problemów związanych z nieprzestrzeganiem zasad opisanych poniżej.

a. Inspektorzy Generalni są ustawowo niezależni; mają szerokie uprawnienia w zakresie prowadzenia dochodzeń, audytów oraz kontroli programów, w tym dotyczących oszustw i nadużyć lub naruszeń prawa; mogą również zalecić działania naprawcze.

(i) W ustawie o Inspektorze Generalnym z 1978 r., z późniejszymi zmianami, ustawowo ustanowiono urząd Federalnego Inspektora Generalnego jako niezależną i obiektywną jednostkę w obrębie większości agencji, do którego obowiązków należy zwalczanie marnotrawienia zasobów, oszustw i nadużyć w ramach programów i działań prowadzonych przez poszczególne agencje. W tym celu każdy Inspektor Generalny jest odpowiedzialny za przeprowadzanie audytów i dochodzeń dotyczących programów i operacji prowadzonych przez jego agencję. Ponadto Inspektorzy Generalni zapewniają kierownictwo i koordynację oraz zalecają działania mające na celu promowanie gospodarności, efektywności i skuteczności, a także zapobiegają oszustwom i nadużyciom w ramach programów i działań prowadzonych przez agencje oraz wykrywają te oszustwa i nadużycia.

(ii) Każda z agencji Wspólnoty Wywiadowczej ma swoje własne Biuro Inspektora Generalnego odpowiedzialne, między innymi, za nadzór nad działaniami służb wywiadowczych. Szereg sprawozdań Inspektora Generalnego w sprawie programów służb wywiadowczych został udostępniony do wglądu publicznego.

(iii) Przykładowo:

— Biuro Inspektora Generalnego Wspólnoty Wywiadowczej utworzono zgodnie z sekcją 405 ustawy o zatwierdzeniu działań wywiadowczych na rok budżetowy 2010 – http://www.gpo.gov/fdsys/pkg/PLAW-111publ259/pdf/PLAW-111publ259.pdf. Inspektor Generalny Wspólnoty Wywiadowczej jest odpowiedzialny za prowadzenie w całej Wspólnocie audytów, dochodzeń, kontroli i przeglądów, w ramach których rozpoznaje i likwiduje zagrożenia systemowe, luki w zabezpieczeniach i niedociągnięcia zakłócające misje agencji Wspólnoty Wywiadowczej w celu pozytywnego oddziaływania na gospodarność i efektywność całej Wspólnoty. Inspektor Generalny Wspólnoty Wywiadowczej jest uprawniony do badania skarg lub informacji na temat zarzutów dotyczących naruszenia prawa, zasad, regulacji, marnotrawstwa, oszustw, nadużyć władzy lub znacznego lub szczególnego zagrożenia dla zdrowia i bezpieczeństwa publicznego w związku z Urzędem Dyrektora Krajowych Służb Wywiadowczych lub programami i działaniami wywiadowczymi Wspólnoty Wywiadowczej. Inspektor Generalny Wspólnoty Wywiadowczej publikuje informacje, w jaki sposób można się zwrócić bezpośrednio do tej jednostki w celu złożenia zawiadomienia: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— Biuro Inspektora Generalnego w Departamencie Sprawiedliwości Stanów Zjednoczonych (DOJ) – https://www.justice.gov – zostało powołane ustawowo jako niezależny podmiot, którego misją jest wykrywanie marnotrawstwa, oszustw, nadużyć i wykroczeń w programach realizowanych przez Departament Sprawiedliwości i wykroczeń personelu oraz zapobieganie im oraz promowanie gospodarności i skuteczności w ramach tych programów. Biuro Inspektora Generalnego bada domniemane naruszenia przepisów prawa karnego i cywilnego przez pracowników Departamentu Sprawiedliwości, a także prowadzi audyty i kontrole programów realizowanych w ramach tego Departamentu. Biuro Inspektora Generalnego jest właściwe do rozpatrywania wszystkich skarg dotyczących wykroczeń przeciwko pracownikom Departamentu Sprawiedliwości, w tym Federalnego Biura Śledczego; Agencji ds. Egzekwowania Przepisów dotyczących Narkotyków, Federalnego Urzędu Więziennictwa; Amerykańskich Służb Porządkowych; Urzędu ds. Alkoholu, Tytoniu, Broni Palnej i Materiałów Wybuchowych; Biura Prokuratora Generalnego Stanów Zjednoczonych; oraz pracownikom, którzy pracują w innych wydziałach lub urzędach Departamentu Sprawiedliwości. (Zgodnie z jedynym

wyjątkiem zarzuty dotyczące wykroczenia popełnionego przez prokuratora Departamentu lub funkcjonariusza organu egzekwowania prawa, w ramach wykonywania obowiązków służbowych przez prokuratora Departamentu w zakresie prowadzenia dochodzeń, postępowania sądowego lub udzielania porad prawnych rozpatruje Urząd ds. Odpowiedzialności Zawodowej działający przy Departamencie). Ponadto na mocy sekcji 1001 amerykańskiej ustawy antyterrorystycznej („USA Patriot Act") podpisanej w dniu 26 października 2001 r. Inspektor Generalny jest zobowiązany do dokonywania przeglądu informacji i przyjmowania skarg dotyczących łamania praw i wolności obywatelskich przez pracowników Departamentu Sprawiedliwości. Biuro Inspektora Generalnego prowadzi ogólnodostępną stronę internetową – https://www.oig.justice.gov – która obejmuje „gorącą linię" do składania wniosków – https://www.oig.justice.gov/hotline/index.htm.

b. Urzędy i podmioty ds. prywatności i wolności obywatelskich w rządzie Stanów Zjednoczonych również mają określone obowiązki. Przykładowo:

(i) na mocy sekcji 803 zaleceń wykonawczych zawartych w ustawie z 2007 r. o Komisji utworzonej w wyniku zamachów z 11 września, skodyfikowanej w Kodeksie Stanów Zjednoczonych w tytule 42 § 2000-ee1, powołuje się urzędników ds. prywatności i wolności obywatelskich w określonych departamentach i agencjach (m.in. Departamencie Stanu, Departamencie Sprawiedliwości i Urzędzie Dyrektora Krajowych Służb Wywiadowczych). W sekcji 803 sprecyzowano, że urzędnicy ds. prywatności i wolności obywatelskich będą sprawowali rolę głównego doradcy odpowiedzialnego m.in. za zapewnienie, aby taki departament, agencja lub podmiot posiadały odpowiednie procedury rozpatrywania skarg od osób fizycznych, które twierdzą, że dany departament, agencja lub podmiot naruszyły ich prywatność lub wolności obywatelskie.

(ii) Na mocy ustawy o bezpieczeństwie narodowym z 1948, z późniejszymi zmianami utworzono funkcję urzędnika ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych, który kieruje Biurem Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych. Do obowiązków urzędnika ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych należy zapewnienie, aby strategie polityczne i procedury agencji Wspólnoty Wywiadowczej przewidywały odpowiednie gwarancje ochrony prywatności i wolności obywatelskich oraz badanie skarg dotyczących łamania lub naruszenia wolności obywatelskich i prywatności w ramach programów i działań prowadzonych przez Urząd Dyrektora Krajowych Służb Wywiadowczych oraz prowadzenie dochodzeń w takich sprawach. Urzędnik ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych umieszcza na swojej stronie internetowej informacje dostępne dla ogółu społeczeństwa, w tym instrukcje dotyczące sposobu składania skargi: www.dni.gov/clpo. Jeżeli urzędnik ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych otrzyma skargę dotyczącą naruszenia prywatności lub wolności obywatelskich w ramach programów i działań prowadzonych przez Wspólnotę Wywiadowczą, będzie współpracował z innymi agencjami Wspólnoty Wywiadowczej nad sposobem rozpatrzenia skargi w ramach Wspólnoty Wywiadowczej. Należy zauważyć, że Agencja Bezpieczeństwa Narodowego także posiada Biuro Wolności Obywatelskich i Ochrony Prywatności, które na swojej stronie internetowej przedstawia informacje na temat swoich obowiązków – https://www.nsa.gov/civil_liberties/. Jeżeli z informacji wynika, że agencja nie przestrzega wymogów dotyczących prywatności (np. wymogu określonego w sekcji 4 dyrektywy politycznej Prezydenta nr 28), wówczas agencje korzystają z mechanizmów zgodności na potrzeby zbadania zdarzenia i naprawienia danej sytuacji. Agencje są zobowiązane zgodnie z dyrektywą polityczną Prezydenta nr 28 zgłaszać przypadki nieprzestrzegania wymogów Urzędowi Dyrektora Krajowych Służb Wywiadowczych.

(iii) Biuro Ochrony Prywatności i Wolności Obywatelskich przy Departamencie Sprawiedliwości wspiera głównego urzędnika ds. ochrony prywatności i wolności obywatelskich działającego w Departamencie w wykonywanych przez niego zadaniach i obowiązkach. Głównym zadaniem Biura Ochrony Prywatności i Wolności Obywatelskich jest ochrona prywatności i wolności obywatelskich Amerykanów poprzez prowadzenie przeglądu, nadzoru i koordynacji działań Departamentu w zakresie ochrony prywatności. Biuro Ochrony Prywatności i Wolności Obywatelskich udziela porad prawnych i zapewnia wytyczne agencjom Departamentu; zapewnia, aby Departament przestrzegał wymogów dotyczących prywatności, w tym ustawy o prywatności z 1974 r., przepisów dotyczących prywatności określonych w ustawie o administracji elektronicznej z 2002 r., w ustawie federalnej o zarządzaniu bezpieczeństwem informacji oraz w dyrektywach dotyczących polityki administracyjnej opublikowanych na potrzeby wykonania ustaw; opracowuje i zapewnia szkolenia z zakresu ochrony prywatności w Departamencie; pomaga głównemu urzędnikowi ds. ochrony prywatności i wolności obywatelskich w opracowywaniu polityki ochrony prywatności w Departamencie; przygotowuje sprawozdania dotyczące prywatności i przekazuje je Prezydentowi i Kongresowi; a także dokonuje przeglądu praktyk dotyczących przetwarzania informacji, aby zapewnić zgodność tych praktyk z zasadami ochrony prywatności i wolności obywatelskich. Biura Ochrony Prywatności i Wolności Obywatelskich umieszcza informacje o swoich obowiązkach na ogólnodostępnej stronie internetowej http://www.justice.gov/opcl.

(iv) Zgodnie z tytułem 42 § 2000ee i nast. U.S.C., Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi stale dokonuje przeglądu (i) strategii politycznych i procedur oraz ich wdrażania, a także departamentów,

agencji i podmiotów władzy wykonawczej związanych ze staraniami na rzecz ochrony narodu przed terroryzmem w celu zapewnienia ochrony prywatności i wolności obywatelskich oraz (ii) innych działań prowadzonych przez władzę wykonawczą związanych z takimi staraniami w celu ustalenia, czy takie działania zapewniają odpowiednią ochronę prywatności i wolności obywatelskich oraz czy są zgodne z obowiązującymi przepisami prawa, regulacjami i polityką w zakresie prywatności i wolności obywatelskich. Rada Nadzoru otrzyma od urzędników ds. prywatności i urzędników ds. wolności obywatelskich sprawozdania i inne informacje oraz dokona ich przeglądu, a w stosownych przypadkach przekaże im zalecenia dotyczące prowadzonych przez nich działań. Na mocy sekcji 803 zaleceń wykonawczych zawartych w ustawie z 2007 r. o Komisji utworzonej w wyniku zamachów z 11 września, skodyfikowanej w tytule 42 § 2000ee-1 U.S.C., urzędnicy ds. prywatności i wolności obywatelskich z ośmiu agencji federalnych (w tym Sekretarz Obrony, Sekretarz Bezpieczeństwa Wewnętrznego, Dyrektor Krajowych Służb Wywiadowczych i Dyrektor Centralnej Agencji Wywiadowczej) oraz wszelkie dodatkowe agencje wyznaczone przez Radę są zobowiązani przekazać Radzie Nadzoru nad Prywatnością i Wolnościami Obywatelskimi okresowe sprawozdanie, obejmujące m.in. liczbę i charakter skarg dotyczących domniemanych naruszeń złożonych w danej agencji oraz rozstrzygnięcia w tych sprawach. Na podstawie ustawy umożliwiającej funkcjonowanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi Rada otrzyma wspomniane sprawozdania, a w stosownych przypadkach przekaże urzędnikom ds. prywatności i wolności obywatelskich zalecenia dotyczące prowadzonych przez nich działań.

ZAŁĄCZNIK IV

Pismo przewodniczącej Federalnej Komisji Handlu Edith Ramirez

Dnia 7 lipca 2016 r.

Za pośrednictwem poczty elektronicznej

Věra Jourová
Komisarz ds. sprawiedliwości, konsumentów i równouprawnienia płci
Komisja Europejska
Rue de la Loi/Wetstraat 200
1049 Bruxelles/Brussel
Belgia

Szanowna Pani Komisarz!

Federalna Komisja Handlu Stanów Zjednoczonych („FTC") docenia możliwość przedstawienia sposobu, w jaki stosuje nowe ramy Tarczy Prywatności UE-USA („ramy Tarczy Prywatności" lub „ramy"). Wierzymy, że wspomniane ramy odegrają kluczową rolę w ułatwianiu przeprowadzania transakcji handlowych chroniących prywatność w świecie, który jest coraz bardziej pełny wzajemnych powiązań. Ramy umożliwią przedsiębiorstwom dokonywanie ważnych operacji w gospodarce światowej, przy jednoczesnym zagwarantowaniu, że konsumenci unijni zachowają istotne gwarancje ochrony prywatności. FTC od dawna angażuje się w ochronę prywatności ponad granicami i uczyni priorytet z wdrażania nowych ram. Poniżej opisujemy w zarysie, jak bardzo FTC była zaangażowana w przeszłości w egzekwowanie przepisów dotyczących ochrony prywatności, w tym pierwotnego programu „bezpieczna przystań", jak również wyjaśniamy jej podejście do wdrażania nowych ram.

W 2000 r. FTC zobowiązała się publicznie do realizacji programu „bezpieczna przystań". W tamtym czasie ówczesny przewodniczący FTC Robert Pitofsky wysłał do Komisji Europejskiej pismo, w którym FTC zobowiązuje się do zdecydowanego stosowania zasad dotyczących prywatności określonych w programie „bezpieczna przystań". FTC nadal podtrzymuje to zobowiązanie poprzez prowadzenie prawie 40 działań służących wykonaniu przepisów prawa, licznych dodatkowych dochodzeń oraz poprzez współpracę z poszczególnymi europejskimi organami ochrony danych („unijne organy ochrony danych") w sprawach będących przedmiotem wspólnego zainteresowania.

Po tym jak w listopadzie 2013 r. Komisja Europejska zgłosiła obawy dotyczące prowadzenia i wykonania programu „bezpieczna przystań" wspólnie z Departamentem Handlu Stanów Zjednoczonych rozpoczęliśmy konsultacje z urzędnikami z Komisji Europejskiej w celu zbadania sposobów na ich usprawnienie. W trakcie tych konsultacji, w dniu 6 października 2015 r., Trybunał Sprawiedliwości wydał orzeczenie w sprawie Schrems, w którym m.in. unieważnił decyzję Komisji Europejskiej w sprawie adekwatności ochrony przewidzianej w programie „bezpieczna przystań". Po wydaniu orzeczenia nadal współpracowaliśmy z Departamentem Handlu i Komisją Europejską nad wzmocnieniem ochrony prywatności zapewnianej osobom fizycznym z Unii Europejskiej. Ramy Tarczy Prywatności są wynikiem trwających konsultacji. Podobnie jak było w przypadku programu „bezpieczna przystań" FTC niniejszym zobowiązuje się do zdecydowanego wykonywania nowych ram. Niniejsze pismo stanowi tego świadectwo.

Warto zauważyć, że potwierdzamy nasze zobowiązanie w czterech kluczowych obszarach: 1) nadawania priorytetowego znaczenia zgłoszeniom i dochodzeniom; 2) przeciwdziałania fałszywym lub wprowadzającym w błąd oświadczeniom dotyczącym uczestnictwa w programie Tarczy Prywatności; 3) stałego monitorowania decyzji; oraz 4) zwiększenia zaangażowania i współpracy z unijnymi organami ochrony danych w zakresie egzekwowania prawa. Poniżej przedstawiamy szczegółowe informacje o każdym ze wspomnianych zobowiązań i odpowiedni kontekst o roli FTC w zakresie chronienia prywatności konsumentów i egzekwowania programu „bezpieczna przystań" oraz szerszy kontekst prywatności w Stanach Zjednoczonych ([1]).

I. KONTEKST

A. **Działania FTC w zakresie polityki dotyczącej prywatności i jej egzekwowania**

FTC przysługują szerokie uprawnienia w dziedzinie wykonywania przepisów 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

([1]) Dodatkowe informacje o federalnych i stanowych przepisach Stanów Zjednoczonych przedstawiliśmy w załączniku A, zaś podsumowanie naszych ostatnich działań służących egzekwowaniu przepisów prawa dotyczących prywatności i bezpieczeństwa przedstawiliśmy w załączniku B. To podsumowanie dostępne jest również na stronie internetowej FTC pod adresem https://www.ftc.gov/reports/privacy-data-security-update-2015.

przepisy w celu ochrony prywatności i bezpieczeństwa danych konsumentów. W prawie pierwotnym stosowanym przez FTC, czyli w ustawie o Federalnej Komisji Handlu, zakazuje się „nieuczciwych" i „wprowadzających w błąd" czynów lub praktyk handlowych lub wpływających na handel ([1]). Podanie informacji, zaniechanie lub działanie jest wprowadzające w błąd, jeżeli w istotny sposób wprowadza w błąd konsumenta działającego rozsądnie w danych okolicznościach ([2]). Czyn lub działanie są nieuczciwe, jeżeli powodują lub mogą spowodować znaczną szkodę konsumenta, której w sposób rozsądny nie da się uniknąć, a której jednocześnie nie równoważą korzyści osiągane przez konsumentów lub konkurencję ([3]). 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.

Na podstawie ustawy o Federalnej Komisji Handlu FTC przysługuje właściwość w obszarze „praktyk handlowych lub wpływających na handel". FTC nie przysługują uprawnienia na gruncie prawa karnego i 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 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 ([4]). 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.

Wykonanie jest kluczowym elementem polityki FTC w zakresie ochrony prywatności. Do tej pory FTC wniósł ponad 500 spraw dotyczących ochrony prywatności i bezpieczeństwa informacji o konsumentach. Sprawy te obejmują zarówno informacje dostępne offline, jak i online oraz obejmują działania służące egzekwowaniu przepisów prawnych przeciwko dużym i małym przedsiębiorstwom, którym zarzuca się, że nie są w stanie właściwie rozporządzać wrażliwymi danymi konsumentów, chronić danych osobowych konsumentów, zainstalowały oprogramowanie szpiegujące lub inne oprogramowanie złośliwe na komputerach konsumentów, złamały zasadę „Proszę nie dzwonić" oraz inne zasady telemarketingowe oraz nieprawidłowo gromadziły i udostępniały dane konsumentów na urządzeniach mobilnych. Działania FTC służące egzekwowaniu przepisów prawnych – zarówno w świecie rzeczywistym, jak i cyfrowym – stanowią ważne przesłanie dla przedsiębiorstw o konieczności ochrony prywatności konsumentów.

FTC wszczęła również szereg inicjatyw politycznych mających na celu zwiększenie prywatności konsumentów, które świadczą o jej działaniach mających na celu wdrażanie regulacji. FTC prowadziła warsztaty i opublikowała sprawozdania, w których rekomenduje najlepsze praktyki ukierunkowane na zwiększenie prywatności w ekosystemie urządzeń przenośnych; zwiększenie przejrzystości branży obejmującej pośredników danych; maksymalizację korzyści związanych z dużym zbiorem danych, przy jednoczesnym ograniczaniu ryzyka, w szczególności dla konsumentów o niskich dochodów, w przypadku których świadczone usługi są na niedostatecznym poziomie, oraz podkreślenie wpływu technologii takich jak rozpoznawanie twarzy i internet rzeczy na prywatność i bezpieczeństwo.

FTC angażuje się również w kształcenie konsumentów i przedsiębiorców, tak aby zwiększyć wpływ swoich działań mających na celu wdrażanie regulacji i inicjatyw rozwoju polityki. FTC korzystała z różnorodnych narzędzi – publikacji, zasobów internetowych, warsztatów i mediów społecznościowych – w celu zapewnienia materiałów dydaktycznych na różne tematy, w tym na temat aplikacji mobilnych, prywatności dzieci i bezpieczeństwa danych. Ostatnio Komisja uruchomiła inicjatywę „Zacznijmy od bezpieczeństwa" (ang. Start With Security), która obejmuje nowe wytyczne dla przedsiębiorstw bazujące na doświadczeniu czerpanym ze spraw prowadzonych przez agencje, które dotyczyły bezpieczeństwa danych oraz obejmuje serię warsztatów w całym kraju. Ponadto FTC od dawna jest liderem w kształceniu konsumentów w zakresie podstawowego bezpieczeństwa komputerowego. W ubiegłym roku nasza strona internetowa OnGuard Online i jej hiszpański odpowiednik, Alerta en Línea, miały 5 mln odsłon.

B. **Ochrona prawna zapewniana konsumentom unijnym przez Stany Zjednoczone**

Ramy będą działać w kontekście większego amerykańskiego systemu zapewniającego ochronę prywatności, który będzie również chronił na wiele sposobów konsumentów UE.

([1]) Tytuł 15 § 45 lit. a) U.S.C.
([2]) Zob. oświadczenie polityczne FTC o oszustwie, załączone do sprawy Cliffdale Assocs., Inc., 103 FTC. 110, 174 (1984), dokument dostępny pod adresem: https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.
([3]) Zob. tytuł 15 § 45 lit. n) U.S.C.; oświadczenie polityczne FTC o nieuczciwości, załączone do sprawy Int'l Harvester Co., 104 FTC. 949, 1070 (1984), dokument dostępny pod adresem: https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
([4]) Zob. sprawa California Dental Ass'n przeciwko FTC, 526 Stany Zjednoczone 756 (1999).

Zakaz ustanowiony w ustawie o Federalnej Komisji Handlu 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, w tym służących przywróceniu stanu poprzedniego, które są dostępne w celu ochrony konsumentów krajowych podczas ochrony konsumentów zagranicznych.

W istocie działania służące wykonaniu przepisów prowadzone przez FTC korzystnie wypływają zarówno na amerykańskich, jak i zagranicznych konsumentów. Na przykład postępowania służące wykonaniu sekcji 5 ustawy o Federalnej Komisji Handlu, prowadzone przez FTC, chroniły prywatność amerykańskich i zagranicznych konsumentów W toku sprawy przeciwko pośrednikowi w obrocie informacjami, Accusearch, FTC twierdziła, że sprzedaż poufnych zapisów rozmów osobom trzecim przez przedsiębiorstwo bez wiedzy lub zgody konsumentów stanowiła nieuczciwą praktykę naruszającą sekcję 5 ustawy o Federalnej Komisji Handlu. Accusearch sprzedał informacje dotyczące zarówno konsumentów amerykańskich, jak i zagranicznych ([1]). Sąd nałożył na Accusearch zakaz dotyczący między innymi wprowadzania do obrotu lub sprzedaży danych osobowych konsumentów bez pisemnej zgody, chyba że uzyskano je zgodnie z prawem z publicznie dostępnych informacji oraz zarządził zwrot zysków w wysokości niemal 200 000 USD ([2]).

Innym przykładem jest zawarcie porozumienia przez FTC z TRUSTe. To sprawia, że konsumenci, w tym konsumenci w Unii Europejskiej, mogą polegać na oświadczeniach złożonych przez światowy organ samoregulacyjny dotyczących przeprowadzonego przeglądu i certyfikacji krajowych i zagranicznych usług internetowych ([3]). Co istotne, nasze działanie przeciwko TRUSTe wzmacnia również w większym stopniu system samoregulowania ochrony prywatności poprzez zapewnienie odpowiedzialności jednostek, które odgrywają ważną rolę w programach samoregulacji, w tym transgranicznych ramach ochrony prywatności.

FTC zapewnia również wykonanie innych przepisów szczególnych, których gwarancje rozciągają się na konsumentów niepochodzących ze Stanów Zjednoczonych – 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 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. Poza przepisami amerykańskiego prawa federalnego, których wykonanie FTC egzekwuje, dodatkowe korzyści dla konsumentów z UE zapewniają pewne inne federalne i stanowe przepisy dotyczące ochrony konsumentów i ochrony prywatności.

C. **Wdrażanie programu „bezpieczna przystań”**

FTC – w ramach swojego programu stosowania zasad ochrony prywatności i bezpieczeństwa – podejmuje starania, aby chronić konsumentów z UE poprzez wszczynanie postępowań, które mają przeciwdziałać naruszeniom programu „bezpieczna przystań”. FTC wszczęła 39 postępowań dotyczących programu„bezpieczna przystań”: 36 dotyczących domniemanych fałszywych oświadczeń o certyfikacji oraz trzy sprawy – przeciwko Google, Facebookowi i Myspace – dotyczące domniemanych naruszeń programu „bezpieczna przystań” ([4]). Te sprawy wykazują, że można wyegzekwować certyfikację oraz że nieprzestrzeganie zasad pociąga za sobą skutki. Na podstawie decyzji wydanej w następstwie porozumienia zawierającej zobowiązanie na okres dwudziestu lat Google, Facebooka i Myspace mają wdrożyć kompleksowe programy ochrony prywatności, które muszą zostać odpowiednio opracowane w celu przeciwdziałania zagrożeniom dla ochrony prywatności związanym z rozwojem nowych i istniejących produktów i usług oraz zarządzaniem tymi produktami i usługami, a także w celu ochrony prywatności i poufności danych osobowych. W ramach tych kompleksowych programów ochrony prywatności, których ustanowienie zostało nakazane powyższymi decyzjami, należy wskazać istotne przewidywalne zagrożenia i wprowadzić środki kontroli, aby zapobiec tym zagrożeniom. Przedsiębiorstwa muszą również przeprowadzać regularne i niezależne oceny swoich programów ochrony

([1]) Zob. Urząd Komisarza ds. Ochrony Prywatności w Kanadzie, skarga w sprawie PIPEDA przeciwko Accusearch, Inc. prowadzącemu działalność pod firmą Abika.com: https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Urząd Komisarza ds. Ochrony Prywatności w Kanadzie przedłożył pismo w charakterze *amicus curiae* w postępowaniu odwoławczym w sprawie wszczętej przez FTC i przeprowadził własne dochodzenie, w wyniku którego stwierdził, że praktyki Accusearch naruszyły również prawo Kanady.

([2]) Zob. FTC przeciwko Accusearch, Inc., nr 06CV015D (Sąd pierwszej instancji dla okręgu Wyoming 20.12.2007), utrzymany w mocy wyrokiem Sądu Apelacyjnego, 570 F.3d 1187 (Sąd Apelacyjny dla Dziesiątego Okręgu, 2009).

([3]) Zob. sprawa True Ultimate Standards Everywhere, Inc., nr C-4512 (F.T.C. 12.3.2015) (decyzja i nakaz), dokument dostępny pod adresem: https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

([4]) Zob. sprawa Google, Inc., nr C-4336 (F.T.C. 13 października 2011 r.) (decyzja i nakaz), dokument dostępny pod adresem: https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; sprawa Facebook, Inc., nr C-4365 (F.T.C. 27 lipca 2012 r.) (decyzja i nakaz), dokument dostępny pod adresem: https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; sprawa Myspace LLC, nr C-4369 (F.T.C. 30 sierpnia 2012 r.) (decyzja i nakaz), dokument dostępny pod adresem: https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

prywatności; oceny te należy przedkładać FTC. W decyzjach zakazuje się również podawania przez te przedsiębiorstwa fałszywych informacji na temat ich praktyk ochrony prywatności i uczestnictwa w jakimkolwiek programie ochrony prywatności lub bezpieczeństwa. Zakaz ten ma również zastosowanie do działań i praktyk przedsiębiorstw w nowych ramach Tarczy Prywatności. FTC może dochodzić wykonania tych decyzji, występując na drogę sądową w celu nałożenia sankcji na gruncie prawa cywilnego. I faktycznie – w 2012 r. Google zapłacił rekordową karę na gruncie prawa cywilnego wynoszącą 22,5 mln USD Decyzje wydane przez FTC umożliwiają w rezultacie ochronę ponad miliarda konsumentów na całym świecie, w tym setek milionów osób mieszkających w Europie.

FTC skupiła się również na sprawach związanych z fałszywymi, zwodniczymi lub wprowadzającymi w błąd oświadczeniami dotyczącymi uczestnictwa w programie „bezpieczna przystań". FTC traktuje te oświadczenia poważnie. Na przykład w sprawie FTC przeciwko Karnani FTC w 2011 r. wszczęła postępowanie przeciwko sprzedawcy internetowemu w Stanach Zjednoczonych, twierdząc, że sprzedawca i jego przedsiębiorstwo wprowadzili w błąd brytyjskich konsumentów, sugerując, że siedziba przedsiębiorstwa znajduje się w Zjednoczonym Królestwie, w tym poprzez wykorzystywanie domeny.uk oraz podawanie brytyjskiej waluty i odniesień do brytyjskiego systemu pocztowego ([1]). Gdy konsumenci otrzymali jednak produkty, odkryli ku swojemu zaskoczeniu, że były one obciążone cłami przywozowymi, przy czym gwarancje były nieważne w Zjednoczonym Królestwie, a z uzyskaniem zwrotu pieniędzy wiązały się dodatkowe koszty. FTC przedstawiła również zarzuty dotyczące wprowadzenia konsumentów w błąd co do uczestnictwa sprzedawcy w programie „bezpieczna przystań". Należy zauważyć, że wszyscy poszkodowani byli ze Zjednoczonego Królestwa.

Wiele z naszych innych spraw związanych ze stosowaniem programu „bezpieczna przystań" dotyczyło podmiotów, które przystąpiły do programu „bezpieczna przystań", ale nie dokonały ponownej corocznej certyfikacji, a nadal przedstawiały się jako jego aktywni członkowie. Jak omówiono to dalej poniżej, FTC zobowiązuje się również do przeciwdziałania fałszywym oświadczeniom dotyczącym uczestnictwa w programie Tarczy Prywatności. Ta strategiczna działalność służąca wykonywaniu przepisów prawa uzupełni wzmożone działania Departamentu Handlu podejmowane w celu kontroli przestrzegania wymogów programu w zakresie certyfikacji i ponownej certyfikacji, działania Departamentu związane z monitorowaniem efektywnego przestrzegania tych wymogów, obejmujące wykorzystanie kwestionariuszy wysyłanych do uczestników programu, oraz wzmożone starania Departamentu podejmowane w celu zidentyfikowania fałszywych oświadczeń dotyczących uczestnictwa w programie i przypadków niewłaściwego wykorzystywania jakiegokolwiek znaku certyfikacyjnego bez pozwolenia ([2]).

II. OKREŚLANIE PIERWSZEŃSTWA ZGŁOSZEŃ I ICH BADANIE

Podobnie jak w przypadku programu „bezpieczna przystań" tak i w tym programie FTC zobowiązuje się do przyznania pierwszeństwa zgłoszeniom dotyczącym Tarczy Prywatności z państw członkowskich UE. Pierwszeństwo damy również zgłoszeniom dotyczącym nieprzestrzegania wytycznych samoregulacyjnych odnoszących się do ram Tarczy Prywatności otrzymanych od organów samoregulacyjnych i innych niezależnych organów rozstrzygania sporów.

Aby ułatwić dokonywanie zgłoszeń z państw członkowskich UE w ramach programu FTC opracowuje ujednoliconą procedurą dokonywania zgłoszeń i przekazuje wytyczne państwom członkowskim UE na temat rodzaju informacji, które najbardziej ułatwią FTC rozpatrywanie zgłoszeń. W ramach tych starań FTC wyznaczy 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 zgłoszenia z państwa członkowskiego UE lub od organów samoregulacyjnych FTC może podjąć szereg działań, aby zaradzić powstałym problemom. Przykładowo możemy dokonać przeglądu polityk ochrony prywatności przedsiębiorstwa, uzyskać dalsze informacje bezpośrednio od przedsiębiorstwa lub od osób 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 zwiększenie wiedzy konsumentów lub przedsiębiorstw, i w stosownych przypadkach, wszcząć odpowiednie postępowanie.

FTC zobowiązuje się również do udostępniania informacji 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

([1]) Zob. FTC przeciwko Karnani, nr 2:09-cv-05276 (Okręg centralny w Kalifornii 20.5.2011) (orzeczenie ostateczne w wyniku porozumienia stron), dokument dostępny pod adresem: https://www ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; zob. również Lesley Fair, FTC Business Center Blog, „Around the World in Shady Ways", https://www.ftc.gov/blog/2011/06/around-world-shady-ways (9 czerwca 2011 r.).

([2]) Pismo Kena Hyatta, pełniącego obowiązki podsekretarza handlu międzynarodowego, administracji handlu międzynarodowego do Věry Jourovej, komisarz ds. sprawiedliwości, konsumentów i równouprawnienia płci.

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 współprace z unijnymi organami ochrony danych, aby udzielić wsparcie 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 ([1]). 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 ([2]).

Poza określaniem pierwszeństwa zgłoszeń dotyczących Tarczy Prywatności z państw członkowskich UE i od organów samoregulacyjnych ([3]), FTC zobowiązuje się do badania z urzędu możliwych naruszeń ram Tarczy Prywatności przy zastosowaniu właściwych narzędzi.

Już od ponad dziesięciu lat FTC prowadzi solidny program dochodzenia problemów związanych z ochroną prywatności i bezpieczeństwem, który angażuje podmioty komercyjne. W ramach tego dochodzenia FTC rutynowa bada, czy dana jednostka podawała informacje na temat uczestnictwa w programie „bezpieczna przystań". Jeżeli jednostka podawała takie informacje, a w postępowaniu wykryto oczywiste naruszenia programu „bezpieczna przystań", FTC uwzględniała zarzuty naruszenia tego programu w swoich działaniach służących egzekwowaniu przepisów prawa. W ramach nowego programu będziemy nadal prezentować tę aktywną postawę. Co ważniejsze, FTC przeprowadza znacznie więcej postępowań dochodzeniowych w stosunku do liczby tych, które skutkują podjęciem publicznych działań służących egzekwowaniu przepisów prawa. Wiele postępowań FTC kończy się, ponieważ pracownicy FTC nie stwierdzają żadnego oczywistego naruszenia prawa. Ze względu na to, że postępowanie dochodzeniowe prowadzone przez FTC nie są ogólnodostępne i mają charakter poufny, często nie upublicznia się faktu zakończenia postępowania.

Blisko 40 działań służących egzekwowaniu przepisów prawna podjętych przez FTC w związku z programem „bezpieczna przystań" stanowi dowód na zaangażowanie tego podmiotu w aktywne wdrażanie wymogów transgranicznych programów ochrony prywatności. W toku regularnie prowadzonych postępowań dotyczących ochrony prywatności i postępowań sprawdzających FTC będzie wyszukiwać potencjalne naruszenia tych ram.

III. PRZECIWDZIAŁANIE FAŁSZYWYM LUB WPROWADZAJĄCYM W BŁĄD OŚWIADCZENIOM DOTYCZĄCYM UCZESTNICTWA W PROGRAMIE TARCZY PRYWATNOŚCI

Jak wskazano powyżej FTC podejmie działania przeciwko podmiotom, które podają fałszywe informacje na temat ich uczestnictwa w programie. FTC rozpatrując wnioski, przyzna pierwszeństwo zgłoszeniom z Departamentu Handlu dotyczącym podmiotów, w przypadku których departament stwierdzi, że niezasadnie podają się za obecnych członków programu lub niewłaściwie korzystają z jakiegokolwiek znaku certyfikacyjnego bez pozwolenia.

Ponadto zauważamy, że jeżeli w polityce ochrony prywatności podmiotu zobowiązano się do przestrzegania zasad Tarczy Prywatności, sam fakt, iż podmiot nie dokona lub nie odnowi rejestracji w Departamencie Handlu może skutkować podjęciem przez FTC działań w celu wyegzekwowania tych zobowiązań w ramach programu.

([1]) 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.

([2]) W latach budżetowych 2012–2015 przykładowo FTC skorzystała ze swojego uprawnienia do udostępniania informacji na podstawie amerykańskiej ustawy o bezpieczeństwie w sieci w odpowiedzi na prawie 60 wniosków od zagranicznych organów i wydała blisko 60 wezwań do przedstawienia dokumentów w postępowaniu cywilnym (takie wezwanie jest odpowiednikiem wezwania administracyjnego), aby wesprzeć dochodzenie w 25 zagranicznych sprawach.

([3]) Chociaż FTC nie rozstrzyga indywidualnych skarg konsumenckich ani nie pośredniczy w ich rozstrzyganiu, FTC potwierdza, że będzie przyznawać pierwszeństwo zgłoszeniom dotyczącym Tarczy Prywatności 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 obywateli, aby złożyć skargę do FTC; jest on dostępny pod adresem: www.ftc.gov/complaint. W przypadku indywidualnych skarg dotyczących Tarczy Prywatności najbardziej użyteczną drogą dla osób fizycznych z Unii Europejskiej może być jednak wnoszenie skarg do organu ochrony danych lub innego pozasądowego organu rozstrzygania sporów w ich państwie członkowskim.

IV. MONITOROWANIE DECYZJI

FTC potwierdza również swoje zobowiązanie do monitorowania decyzji służących wykonaniu przepisów na potrzeby zapewnienia zgodności z ramami Tarczy Prywatności.

Wymóg przestrzegania ram będziemy realizować za pomocą różnych odpowiednich nakazów w przyszłych decyzjach FTC dotyczących programu. Obejmuje to zakaz podawania fałszywych informacji dotyczących programu i innych programów ochrony prywatności, jeżeli są one podstawą postępowania wszczętego przez FTC.

Z pomocą przychodzą w tym wypadku postępowania przeprowadzone przez FTC w związku z pierwotnym programem „bezpieczna przystań". We wszystkich decyzjach wydanych w 36 sprawach związanych z fałszywymi lub wprowadzającymi w błąd oświadczeniami dotyczącymi certyfikacji w ramach programu „bezpieczna przystań" zakazano podawania fałszywych informacji na temat uczestnictwa danego przedsiębiorstwa w tym programie lub w jakimkolwiek innym programie ochrony prywatności lub bezpieczeństwa, a także wprowadzono wymóg, aby dane przedsiębiorstwo udostępniało FTC sprawozdania z przestrzegania zasad programu. W sprawach, które wiązały się z naruszeniem zasad programu „bezpieczna przystań", wobec przedsiębiorstw wprowadzono wymóg wdrażania kompleksowych programów ochrony prywatności i corocznej oceny tych programów przez dwadzieścia lat przez niezależne osoby trzecie oraz przedkładania tej oceny FTC.

Naruszenia decyzji administracyjnych FTC mogą skutkować nałożeniem kar na gruncie prawa cywilnego w wysokości do 16 000 USD za każde naruszenie lub 16 000 USD za każdy dzień trwania naruszenia ([1]), 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 programu„bezpieczna przystań", co czyni w przypadku wszystkich wydawanych przez siebie decyzji. FTC bardzo poważnie traktuje wykonanie swoich decyzji dotyczących ochrony prywatności i bezpieczeństwa danych i podejmuje w stosownych przypadkach działania służące ich wykonaniu. Przykładowo, jak opisano powyżej, Google zapłacił karę na gruncie prawa cywilnego w wysokości 22,5 mln USD w odpowiedzi na zarzuty naruszenia decyzji wydanej przez FTC. 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 nadal będzie prowadzić internetowy wykaz przedsiębiorstw podlegających decyzjom dotyczącym stosowania zarówno programu „bezpieczna przystań", jak i nowych ram Tarczy Prywatności ([2]). Co więcej, w zasadach Tarczy Prywatności wprowadzono obecnie wymóg wobec przedsiębiorstw podlegających decyzjom FTC lub orzeczeniom sądu wydanym w sprawie nieprzestrzegania zasad, aby podawały one do wiadomości publicznej wszelkie istotne związane z Tarczą Prywatności części jakichkolwiek sprawozdań dotyczących przestrzegania zasad lub sprawozdań oceniających, które przedłożono FTC, w stopniu, na jaki pozwalają na to przepisy i reguły dotyczące poufności.

V. WSPÓŁPRACA Z UNIJNYMI ORGANAMI OCHRONY DANYCH I WSPÓŁPRACA W ZAKRESIE EGZEKWOWANIA PRAWA

FTC uznaje ważną rolę, jaką odgrywają unijne organy ochrony danych w odniesieniu do zapewnienia przestrzegania zasad programu, i zachęca do pogłębionych konsultacji i zacieśniania współpracy w zakresie egzekwowania prawa. Oprócz prowadzenia wszelkich konsultacji z organami ochrony danych w sprawie kwestii dotyczących konkretnych przypadków FTC zobowiązuje się do brania udziału w okresowych spotkaniach z wyznaczonymi przedstawicielami Grupy Roboczej Art. 29 w celu omówienia zagadnień ogólnych związanych z ulepszaniem współpracy w zakresie egzekwowania prawa w ramach programu. Ponadto FTC będzie uczestniczyć, wraz z Departamentem Handlu, Komisją Europejską i przedstawicielami Grupy Roboczej Art. 29, w corocznym przeglądzie ram programu w celu omówienia jego 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. Szczególnie ważne było uruchomienie w zeszłym roku przez FTC we współpracy z jej partnerskimi organami egzekwowania prawa w Unii Europejskiej i na całym świecie systemu ostrzegania w ramach Światowej Sieci na rzecz Prywatności (ang. Global Privacy Enforcement Network, „GPEN") w celu udostępniania informacji na temat dochodzeń i propagowania koordynacji działań w zakresie egzekwowania prawa. Narzędzie ostrzegania w ramach sieci mogłoby okazać się szczególnie przydatne w kontekście programu Tarczy Prywatności. FTC i unijne organy ochrony danych mogłyby wykorzystać je na potrzeby koordynacji dochodzeń w ramach programu i innych tego rodzaju dochodzeń w zakresie ochrony prywatności, w tym jako podstawę udostępniania informacji w celu zapewnienia bardziej skoordynowanej i skuteczniejszej ochrony prywatności konsumentów. Mamy nadzieję na dalszą współpracę z zaangażowanymi unijnymi

([1]) Tytuł 15 § 45 lit. m) U.S.C.; tytuł 16 § 1.98 kodeksu przepisów federalnych (ang. Code of Federal Regulations, „C.F.R.").

([2]) Zob. FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251.

organami w celu rozpowszechniania systemu ostrzegania Światowej Sieci na rzecz Prywatności i opracowania innych narzędzi na potrzeby usprawnienia współpracy w zakresie egzekwowania prawa w sprawach dotyczących ochrony prywatności, w tym w sprawach związanych z programem Tarczy Prywatności.

FTC z zadowoleniem potwierdza swoje zobowiązanie do egzekwowania nowych ram Tarczy Prywatności. Mamy również nadzieję na dalszą współpracę z naszymi kolegami i koleżankami z UE w ramach działań na rzecz ochrony prywatności konsumentów po obu stronach Atlantyku.

Z poważaniem

Edith Ramirez

Przewodnicząca

Dodatek A

Ramy Tarczy Prywatności UE-USA w ogólnym kontekście ochrony prywatności i bezpieczeństwa w Stanach Zjednoczonych

Środki ochrony przewidziane w ramach Tarczy Prywatności UE-USA (zwanych dalej „ramami") funkcjonują w kontekście szerzej pojętych środków ochrony prywatności zapewnionych w ramach całego amerykańskiego porządku prawnego. Po pierwsze, Federalna Komisja Handlu („FTC") przyjęła solidny program na rzecz ochrony prywatności i bezpieczeństwa danych w obszarze praktyk handlowych w Stanach Zjednoczonych chroniący konsumentów na całym świecie. Po drugie, system ochrony prywatności i bezpieczeństwa konsumentów w Stanach Zjednoczonych zmienił się znacząco od 2000 r., kiedy został przyjęty pierwotny program „bezpieczna przystań" UE-USA. Od tego czasu wprowadzono wiele federalnych i stanowych ustaw z zakresu ochrony prywatności i bezpieczeństwa, a liczba sporów sądowych na gruncie prawa publicznego i prywatnego wszczętych w celu wykonania prawa do prywatności znacząco wzrosła. Szeroki zakres amerykańskich środków ochrony prawnej na rzecz ochrony prywatności i bezpieczeństwa konsumentów, mających zastosowanie do praktyk przetwarzania danych handlowych, uzupełnia środki ochrony zapewnione osobom fizycznym z Unii Europejskiej w nowych ramach.

I. OGÓLNY PROGRAM FTC W DZIEDZINIE EGZEKWOWANIA PRZEPISÓW PRAWA W ZAKRESIE OCHRONY PRYWATNOŚCI I BEZPIECZEŃSTWA

FTC jest wiodącą amerykańską agencją ochrony konsumentów odpowiedzialną za ochronę prywatności w sektorze handlu. FTC jest uprawniona do prowadzenia dochodzeń dotyczących nieuczciwych albo wprowadzających w błąd praktyk handlowych naruszających prywatność konsumentów, jak również do egzekwowania przepisów szczególnych dotyczących prywatności, obejmujących bardziej zawężone obszary, chroniących pewne informacje finansowe i dane odnoszące się do zdrowia, informacje o dzieciach i informacje pozwalające na podjęcie pewnych decyzji dotyczących kwalifikowalności konsumentów.

FTC ma wyjątkowe doświadczenie w dziedzinie egzekwowania przepisów dotyczących ochrony prywatności konsumentów. Działania FTC są kierowane przeciwko niezgodnym z prawem praktykom w środowisku *offline* i *online*. Na przykład FTC wszczęła postępowanie przeciwko bardzo znanym spółkom, takim jak Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC, i Snapchat, oraz mniej znanym spółkom. FTC wszczęła postępowanie przeciwko przedsiębiorstwom, które rzekomo wysyłały konsumentom wiadomości spam, instalowały oprogramowanie szpiegujące na komputerach, nie były w stanie zabezpieczyć danych osobowych konsumentów, śledziły konsumentów *online*, naruszały prywatność dzieci, bezprawnie gromadziły informacje przechowywane na urządzeniach mobilnych konsumentów i nie były w stanie zabezpieczyć urządzeń podłączonych do sieci wykorzystywanych do przechowywania danych osobowych. W konsekwencji wydane decyzje przewidywały zwykle bieżące monitorowanie przez FTC przez okres dwudziestu lat, zabraniały dalszych naruszeń prawa i nakładały na przedsiębiorstwa dotkliwe kary finansowe za naruszenie porządku ([1]). Należy zauważyć, że decyzje FTC nie chronią jedynie osób fizycznych, które wniosły skargę; chronią wszystkich konsumentów, którzy będą mieli styczność z przedsiębiorstwem w przyszłości. W kontekście transgranicznym do zakresu właściwości FTC należy ochrona konsumentów na całym świecie przed praktykami na terytorium Stanów Zjednoczonych ([2]).

Dotychczas FTC wszczęła ponad 130 spraw dotyczących spamu i oprogramowania szpiegującego, ponad 120 spraw dotyczących telemarketingu pomimo zgłoszenia do rejestru „Proszę nie dzwonić", ponad 100 spraw dotyczących ustawy o rzetelnej sprawozdawczości kredytowej, prawie 60 spraw dotyczących bezpieczeństwa, więcej niż 50 spraw dotyczących prywatności, prawie 30 spraw o naruszenie ustawy Gramma-Leacha-Blileya oraz ponad 20 spraw dotyczących wykonania ustawy o ochronie prywatności dzieci w internecie („COPPA") ([3]). Poza wszczęciem powyższych spraw FTC przygotowała i opublikowała pisma zawierające ostrzeżenia ([4]).

([1]) Każda jednostka, która się nie zastosuje do decyzji FTC, podlega karze na gruncie prawa cywilnego do 16 000 USD za każde naruszenie lub 16 000 USD za każdy dzień trwania naruszenia. Zob. tytuł 15 § 45 lit. l) U.S.C.; tytuł 16 § 1.98 lit. c) kodeksu przepisów federalnych (ang. Code of Federal Regulations, „C.F.R.").

([2]) Kongres wyraźnie potwierdził uprawnienie FTC do dochodzenia środków ochrony prawnej, w tym mających na celu przywrócenie stanu poprzedniego, w przypadku jakichkolwiek działań lub praktyk obejmujących handel zagraniczny, które 1) powodują lub mogą spowodować możliwe do przewidzenia szkody w Stanach Zjednoczonych lub 2) obejmują prowadzenie istotnych operacji w Stanach Zjednoczonych. Zob. tytuł 15 § 45 lit. a) ppkt 4 U.S.C.

([3]) Niekiedy w następstwie wszczęcia przez Komisję spraw dotyczących ochrony prywatności i bezpieczeństwa można domniemywać, że przedsiębiorstwo stosowało zarówno praktyki wprowadzające w błąd, jak i nieuczciwe praktyki; sprawy te dotyczą również domniemanego naruszenia wielu ustaw, takich jak ustawa o rzetelnej sprawozdawczości kredytowej, ustawa Gramma-Leacha-Blileya oraz ustawa o ochronie prywatności dzieci w internecie.

([4]) Zob. np. komunikat prasowy, FTC, „FTC Warns Children's App Maker BabyBus About Potential COPPA Violations" (22 grudnia 2014 r.), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; komunikat prasowy, FTC, FTC Warns Data Broker Operations of Possible Privacy Violations (7 maja 2013 r.), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; komunikat prasowy, FTC, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (3 kwietnia 2013 r.), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may.

Ze względu na duże znaczenie przypisywane przez FTC egzekwowaniu przepisów dotyczących ochrony prywatności, FTC sprawdza również, czy nie doszło do potencjalnych naruszeń programu „bezpieczna przystań". Od chwili przyjęcia programu „bezpieczna przystań" FTC podjęła z własnej inicjatywy liczne dochodzenia dotyczące przestrzegania jego zasad i wszczęła 39 postępowań przeciwko amerykańskim spółkom ze względu na naruszenie zasad tego programu. FTC będzie nadal prezentować tę aktywną postawę i uzna wdrażanie nowych ram za priorytet.

II. ŚRODKI OCHRONY NA SZCZEBLU FEDERALNYM I STANOWYM NA RZECZ OCHRONY PRYWATNOŚCI KONSUMENTÓW

Przegląd stosowania programu „bezpieczna przystań", który opublikowano jako załącznik do decyzji Komisji Europejskiej w sprawie adekwatności programu „bezpieczna przystań", zawiera wykaz wielu ustaw federalnych i stanowych dotyczących prywatności, obowiązujących w momencie przyjęcia programu „bezpieczna przystań" w 2000 r. ([1]). W tym czasie, oprócz sekcji 5 ustawy o Federalnej Komisji Handlu, wiele ustaw federalnych regulowało gromadzenie i wykorzystywanie danych osobowych do celów handlowych, w tym: ustawa o polityce łączności kablowej, ustawa o ochronie prywatności kierowców, ustawa o ochronie danych w łączności elektronicznej, ustawa o elektronicznym transferze środków, ustawa o rzetelnej sprawozdawczości kredytowej, ustawa Gramma-Leacha-Blileya, ustawa o prawie do poufności informacji finansowych, ustawa o ochronie konsumentów usług telefonicznych oraz ustawa o ochronie prywatności rejestrów dotyczących sprzedaży i wypożyczeń taśm wideo. W wielu stanach obowiązywały również w tych obszarach analogiczne ustawy.

Od 2000 r. doszło do licznych zmian na szczeblu federalnym i stanowym, które zapewniają dodatkowe środki ochrony prywatności konsumenta ([2]). Na szczeblu federalnym, na przykład, w 2013 r. FTC wprowadziła zasadę dotyczącą ustawy o ochronie prywatności dzieci w internecie, tak aby zapewnić dodatkowe środki ochrony danych osobowych dzieci. FTC wydała również dwie zasady wdrażające ustawę Gramma-Leacha-Blileya – zasadę dotyczącą prywatności i zasadę dotyczącą zabezpieczeń – które nakładają na instytucje finansowe obowiązek ([3]) ujawniania praktyk dotyczących wymiany informacji i wdrożenia kompleksowego programu na rzecz bezpieczeństwa informacji, by chronić dane konsumentów ([4]). Podobnie ustawa o rzetelnym i dokładnym zapisie informacji o transakcjach kredytowych („FACTA"), przyjęta w 2003 r., uzupełnia istniejące od dawna ustawy amerykańskie dotyczące kredytów w celu określenia wymogów ukrywania (ang. *data masking*) pewnych wrażliwych danych finansowych, ich wymiany oraz usuwania. FTC opublikowała szereg zasad na podstawie ustawy o rzetelnym i dokładnym zapisie informacji o transakcjach kredytowych, dotyczących m.in. prawa konsumenta do otrzymania nieodpłatnego rocznego sprawozdania kredytowego; wymogów dotyczących bezpiecznego usuwania informacji dotyczących sprawozdania na temat konsumenta; prawa konsumenta do zrezygnowania z otrzymywania pewnych ofert kredytowych i ubezpieczeniowych (klauzula *opt-out*); prawa konsumenta do zastosowania klauzuli *opt-out* w odniesieniu do wykorzystywania informacji przekazywanych przez jednostkę powiązaną w celu przedstawienia oferty marketingowej ich produktów i usług; oraz wymogów dla instytucji finansowych i wierzycieli na potrzeby wdrożenia programów dotyczących zapobiegania i wykrywania kradzieży tożsamości ([5]). Ponadto zasady opublikowane na podstawie ustawy o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych zostały zweryfikowane w 2013 r., co oznaczało uzupełnienie ich o dodatkowe gwarancje ochrony prywatności i bezpieczeństwa danych osobowych odnoszących się do zdrowia ([6]). Zasady chroniące konsumentów przed niechcianym telemarketingiem, automatycznymi połączeniami telefonicznymi oraz spamem również zostały już wdrożone. Kongres przyjął również ustawy nakładające na pewne spółki gromadzące dane na temat zdrowia obowiązek poinformowania konsumentów, gdyby doszło do naruszenia przepisów ([7]).

Stany były zawsze bardzo aktywne w przyjmowaniu ustaw dotyczących ochrony prywatności i bezpieczeństwa. Od 2000 r. czterdzieści siedem stanów, dystrykt Kolumbii, Guam, Puerto Rico i Wyspy Dziewicze przyjęły ustawy

([1]) Zob. Departament Handlu Stanów Zjednoczonych, przegląd stosowania programu „bezpieczna przystań", https://build.export.gov/main/safeharbor/eu/eg_main_018476.

([2]) Aby zapoznać się z bardziej kompleksowym skróconym opisem środków ochrony prawnej w Stanach Zjednoczonych – zob. Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (wydanie 5, 2015 r.).

([3]) Instytucje finansowe, na podstawie ustawy Gramma-Leacha-Blileya, zostały zdefiniowane bardzo szeroko, aby objąć wszystkie przedsiębiorstwa, które są „znacząco zaangażowane" w sprzedaż produktów finansowych lub świadczenie usług finansowych. Obejmuje to na przykład przedsiębiorstwa umożliwiające szybkie zrealizowanie czeku (ang. *check-cashing businesses*), podmioty udzielające pożyczki krótkoterminowe bez zabezpieczenia (ang. *payday lenders*), pośredników hipotecznych, pożyczkodawców niebędących bankami, rzeczoznawców dokonujących oceny mienia lub nieruchomości oraz profesjonalistów przygotowujących coroczne deklaracje podatkowe.

([4]) Na podstawie ustawy o ochronie konsumentów w obszarze usług finansowych z 2010 r. („CFPA"), Zbiór Ustaw Prawa Publicznego, tytuł X Pub. L. 111-203, 124 Stat. 1955 (21 lipca 2010 r.) (również znanej jako „ustawa Dodda-Franka dotycząca ochrony konsumentów i reformy Wall Street") większość uprawnień FTC w zakresie stanowienia prawa przyznanych jej na podstawie ustawy Gramma-Leacha-Blileya została przeniesiona na Biuro Ochrony Konsumentów w Obszarze Usług Finansowych („CFPB"). FTC nadal przysługują uprawnienia, na podstawie ustawy Gramma-Leacha-Blileya, w zakresie egzekwowania prawa, jak również uprawnienia w zakresie stanowienia prawa na potrzeby zasady gwarancji i ograniczone uprawnienia w zakresie stanowienia prawa na podstawie zasady dotyczącej prywatności w odniesieniu do sprzedawców samochodów.

([5]) Na podstawie ustawy o ochronie konsumentów w obszarze usług finansowych Komisja dzieli uprawnienia do egzekwowania przepisów przyznane na mocy ustawy o rzetelnej sprawozdawczości kredytowej z CFPB, lecz w znacznej mierze uprawnienia te zostały przeniesione na CFPB (z wyjątkiem zasady systemu ostrzegawczego i zasad usuwania).

([6]) Zob. tytuł 45 C.F.R. pkt 160, 162, 164.

([7]) Zob. np. amerykańska ustawa o ożywieniu i reinwestowaniu (ang. *American Recovery & Reinvestment Act*) z 2009 r., Zbiór Ustaw Prawa Publicznego, Pub. L. No. 111-5, 123 Stat. 115 (2009 r.). i właściwe rozporządzenia – tytuł 45 kodeksu przepisów federalnych § 164.404-164.414; tytuł 16 kodeksu przepisów federalnych pkt 318.

nakładające na przedsiębiorstwa obowiązek powiadamiania osób fizycznych o naruszeniu zasad bezpieczeństwa w odniesieniu do danych osobowych ([1]). W co najmniej trzydziestu dwóch stanach i Puerto Rico obowiązują ustawy dotyczące usuwania danych określające wymogi niszczenia lub usuwania danych osobowych ([2]). Szereg stanów przyjął ustawy ogólne dotyczące bezpieczeństwa danych. Ponadto w Kalifornii przyjęto różne ustawy dotyczące prywatności, w tym nakładające na spółki obowiązek stosowania polityk dotyczących prywatności i ujawniania praktyk „Nie śledzę" (ang. *Do Not Track*) ([3]), ustawę „Shine the Light" wprowadzającą obowiązek zapewnienia większej przejrzystości przez pośredników w obrocie danymi ([4]) oraz ustawę, która uprawnia małoletnich do usuwania niektórych informacji z mediów społecznościowych ([5]). Na mocy tych ustaw i innych aktów stanowiących podstawę prawną rządy federalne i stanowe nakładały znaczące grzywny na spółki, które nie przestrzegały zasady ochrony prywatności i bezpieczeństwa w odniesieniu do danych osobowych konsumentów ([6]).

Postępowania na gruncie prawa prywatnego również doprowadziły do wydania korzystnych wyroków i zawarcia korzystnych ugód, co przyczyniło się zwiększenia ochrony prywatności i bezpieczeństwa danych konsumentów. Na przykład w 2015 r. Target zgodził się wypłacić 10 mln USD na podstawie postanowień ugody zawartej z konsumentami, którzy twierdzili, że ich informacje finansowe zostały wystawione na niebezpieczeństwo ze względu na znaczne naruszenie przepisów o ochronie danych. W 2013 r. AOL przystał na wypłacenie 5 mln USD w ramach ugody zawartej po wytoczeniu powództwa zbiorowego z tytułu domniemanego niedostatecznego procesu anonimizacji związanego z ujawnieniem zapytań w wyszukiwarkach setek tysięcy członków AOL. Ponadto sąd federalny zatwierdził wypłatę 9 mln USD przez Netflix z tytułu domniemanego przechowywania rejestrów historycznych dotyczących wypożyczeń niezgodnie z ustawą o ochronie prywatności rejestrów dotyczących sprzedaży i wypożyczeń taśm wideo z 1988 r. Sądy federalne w Kalifornii zatwierdziły dwie odrębne ugody z Facebookiem, jedną przewidującą wypłatę 20 mln USD i drugą – 9,5 mln USD, ze względu na gromadzenie danych osobowych jego użytkowników, wykorzystywanie i wymianę tych danych przez spółkę. W 2008 r. sąd stanowy w Kalifornii zatwierdził ugodę z LensCrafters opiewającą na 20 mln USD w sprawie dotyczącej niezgodnego z prawem ujawnienia informacji medycznych konsumentów.

Reasumując, Stany Zjednoczone zapewniają znaczącą ochronę prawną prywatności i bezpieczeństwa konsumentów, o czym świadczy niniejsze podsumowanie. Nowe ramy Tarczy Prywatności, które zapewniają znaczące gwarancje na rzecz osób fizycznych z Unii Europejskiej, będą działały w ramach szerszego systemu, w którym ochrona prywatności i bezpieczeństwa konsumentów stanowi ważny priorytet.

([1]) Zob. np. Krajowa Konferencja Stanowych Legislatur (ang. *National Conference of State Legislatures*), *State Security Breach Notification Laws* (4 stycznia 2016 r.), dokument dostępny pod adresem: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

([2]) Krajowa Konferencja Stanowych Legislatur, *Data Disposal Laws* (12 stycznia 2016 r.), dokument dostępny pod adresem: http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

([3]) Kalifornijski kodeks postępowania w określonych zawodach (ang. *Cal. Bus. & Professional Code*) § 22575-22579.

([4]) Kalifornijski kodeks cywilny. Kodeks § 1798.80-1798.84.

([5]) Kalifornijski kodeks postępowania w określonych zawodach § 22580-22582.

([6]) Zob. Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines* [w:] Computerworld (17 lutego 2014 r.), dokument dostępny pod adresem: http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1.

ZAŁĄCZNIK V

Pismo sekretarza transportu Anthony'ego Foxxa

Dnia 19 lutego 2016 r.

Komisarz Věra Jourová
Komisja Europejska
Rue de la Loi/Wetstraat 200
1 049 l 049 Bruxelles/Brussel
Belgia

Re: Ramy Tarczy Prywatności UE-USA

Szanowna Pani Komisarz!

Departament Transportu Stanów Zjednoczonych („Departament") docenia możliwość przedstawienia swojej roli we wspieraniu Tarczy Prywatności UE-USA. Te ramy odgrywają kluczową rolę w ochronie danych osobowych przekazywanych w transakcjach handlowych w świecie coraz bardziej pełnym wzajemnych powiązań. Ramy umożliwiają przedsiębiorstwom prowadzenie ważnych operacji w gospodarce światowej, przy jednoczesnym zapewnieniu utrzymania istotnej ochrony prywatności konsumentów UE.

Departament Transportu po pierwsze publicznie wyraził swoje zobowiązanie do egzekwowania zasad programu „bezpieczna przystań" w piśmie wysłanym do Komisji Europejskiej ponad 15 lat temu. W tym piśmie Departament Transportu zobowiązał się do zdecydowanego egzekwowania zasad dotyczących prywatności określonych w programie „bezpieczna przystań". Departament Transportu podtrzymuje to zobowiązanie, a niniejsze pismo stanowi tego świadectwo.

W szczególności Departament Transportu odnawia swoje zobowiązanie w następujących obszarach kluczowych. Są to: 1) przyznawanie pierwszeństwa dochodzeniu domniemanych naruszeń Tarczy Prywatności; 2) podejmowanie odpowiednich działań służących egzekwowaniu przepisów prawa wobec jednostek, które składają fałszywe lub wprowadzające w błąd oświadczenia dotyczące certyfikacji Tarczy Prywatności; oraz 3) monitorowanie i publikowanie rozstrzygnięć dotyczących naruszeń Tarczy Prywatności. Przekazujemy informacje na temat przestrzegania każdego z tych zobowiązań i w razie konieczności informacje związane z rolą Departamentu Transportu w obszarze ochrony prywatności konsumentów i stosowania ram Tarczy Prywatności.

I. KONTEKST

A. **Uprawnienia Departamentu Transportu w zakresie ochrony prywatności**

Departament jest bardzo zaangażowany w zapewnianie ochrony informacji dostarczonych przez konsumentów przewoźnikom lotniczym i pośredników sprzedaży biletów. Uprawnienie Departamentu Transportu 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 lub nieuczciwych metod konkurencji" w sprzedaży usług transportu lotniczego, które to praktyki lub metody skutkują lub mogą skutkować szkodą dla konsumenta. Przepis § 41712 wzorowano na sekcji 5 ustawy o Federalnej Komisji Handlu (FTC) (tytuł 15 § 45 U.S.C.). Zgodnie ze stosowaną przez nas wykładnią przepisu dotyczącego nieuczciwych lub wprowadzających w błąd praktyk przewoźnik lotniczy lub pośrednik sprzedaży biletów nie może: 1) naruszać warunków swojej polityki ochrony prywatności; ani 2) gromadzić ani też ujawniać informacji prywatnych w sposób, który prowadzi do naruszenia porządku publicznego, jest niemoralny lub skutkuje poważną szkodą dla konsumenta, której nie równoważą jakiekolwiek korzyści wyrównawcze. Zgodnie ze stosowaną przez nas wykładnią § 41712 przewoźnicy i pośrednicy sprzedaży biletów nie mogą: 1) naruszać żadnych przepisów wydanych przez Departament, w których konkretne praktyki ochrony prywatności uznano za nieuczciwe lub wprowadzające w błąd; ani 2) naruszać przepisów ustawy o ochronie prywatności dzieci w internecie ani przepisów wykonawczych do tej ustawy wydanych przez FTC. Na mocy prawa federalnego Departament Transportu 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 ochrony prywatności obowiązujących w ramach Tarczy Prywatności, 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 ochrony prywatności w ramach Tarczy Prywatności, jakiekolwiek nieprzestrzeganie tych zasad przez przewoźnika lub pośrednika sprzedaży biletów stanowi naruszenie § 41712.

B. **Praktyki w zakresie egzekwowania prawa**

Urząd ds. Egzekwowania Prawa i Prowadzenia Postępowań w Lotnictwie będący jednostką Departamentu (Urząd ds. Egzekwowania Prawa w Lotnictwie) (ang. *Office of Aviation Enforcement and Proceedings*) 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 Departamentu Transportu ([1]).

Jeżeli nie osiągnięto zasadnego i odpowiedniego porozumienia w sprawie, Urząd ds. Egzekwowania Prawa w Lotnictwie ma prawo wszcząć odpowiednie postępowanie, które obejmuje postępowanie dowodowe przed sędzią administracyjnym w Departamencie Transportu. 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 27 500 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 Urząd ds. Egzekwowania Prawa w Lotnictwie, 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 ramowych Tarczy Prywatności, 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 Departament Transportu 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 Departament Transportu**

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. Departament Transportu 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. Departament Transportu wykorzystuje i nadal będzie wykorzystywał wszystkie środki ochrony prawnej, które służą ochronie zarówno zagranicznych, jak i amerykańskich konsumentów przed nieuczciwymi lub wprowadzającymi w błąd praktykami stosowanymi w transporcie lotniczym przez jednostki regulowane.

Departament Transportu zapewnia również, w odniesieniu do przewoźników lotniczych, egzekwowanie innych przepisów szczególnych, które rozszerzając zakres ochrony na konsumentów niepochodzących ze Stanów Zjednoczonych – 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. Departament Transportu jest uprawniony do podjęcia działania służącego egzekwowaniu przepisów prawa 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 TARCZY PRYWATNOŚCI

Jeżeli przewoźnik lotniczy lub pośrednik sprzedaży biletów postanawia zostać uczestnikiem programu Tarczy Prywatności, a Departament otrzymuje skargę, że taki przewoźnik lotniczy lub pośrednik sprzedaży biletów dokonał domniemanego naruszenia zasady programu, Departament podejmie następujące kroki w celu zdecydowanego egzekwowania zasad programu.

([1]) http://www.transportation.gov/airconsumer/privacy-complaints.

A. **Przyznawanie pierwszeństwa dochodzeniu domniemanych naruszeń**

Urząd ds. Egzekwowania Prawa w Lotnictwie wchodzący w skład Departamentu zbada każdą skargę, w której zarzuca się domniemane naruszenie Tarczy Prywatności (w tym skargi otrzymane od unijnych organów ochrony danych), i podejmie działanie służące egzekwowaniu przepisów prawa, jeżeli pojawią się dowody wskazujące na naruszenie. Ponadto Urząd ds. Egzekwowania Prawa w Lotnictwie będzie współpracował z FTC i Departamentem Handlu oraz przyzna pierwszeństwo sprawom dotyczącym zarzutów nieprzestrzegania zobowiązań z zakresu ochrony prywatności w ramach Tarczy Prywatności przez jednostki regulowane.

Po otrzymaniu skargi na domniemane naruszenie ram Tarczy Prywatności Urząd ds. Egzekwowania Prawa w Lotnictwie wchodzący w skład Departamentu 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 osób 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 Tarczy Prywatności 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 przepisów prawa w ramach Tarczy Prywatności.

B. **Przeciwdziałanie fałszywym lub wprowadzającym w błąd oświadczeniom dotyczącym uczestnictwa**

Departament podtrzymuje zobowiązanie do badania naruszeń Tarczy Prywatności, w tym fałszywych lub wprowadzających w błąd oświadczeń dotyczących uczestnictwa w programie Tarczy Prywatności. Rozpatrując wnioski, przyznamy pierwszeństwo zgłoszeniom z Departamentu Handlu dotyczącym podmiotów, w przypadku których stwierdzimy, że niezasadnie podają się za obecnych członków programu Tarczy Prywatności lub korzystają z jakiegokolwiek znaku certyfikacyjnego Tarczy Prywatności bez pozwolenia.

Ponadto chcielibyśmy zauważyć, że jeżeli w polityce ochrony prywatności podmiotu zobowiązano się do przestrzegania istotnych zasad Tarczy Prywatności, sam fakt, iż podmiot nie dokona lub nie odnowi rejestracji w Departamencie Handlu może skutkować podjęciem przez Departament Transportu działań w celu wyegzekwowania tych zobowiązań.

C. **Monitorowanie i publikowanie decyzji służących egzekwowaniu przepisów w sprawach naruszeń**

Urząd ds. Egzekwowania Prawa w Lotnictwie wchodzący w skład Departamentu podtrzymuje również swoje zobowiązanie do monitorowania decyzji na potrzeby zapewnienia zgodności z zasadami programu Tarczy Prywatności. W szczególności, jeżeli urząd wyda decyzję, w której nakaże przewoźnikowi lotniczemu lub pośrednikowi sprzedaży biletów powstrzymanie się od przyszłych naruszeń Tarczy Prywatności 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 Tarczy Prywatności były dostępne na jego stronie internetowej.

Mamy nadzieję na dalszą współpracę w sprawach związanych z Tarczą Prywatności 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

Anthony R. Foxx

Sekretarz transportu

ZAŁĄCZNIK VI

Pismo głównego radcy Roberta Litta
Urząd Dyrektora Krajowych Służb Wywiadowczych

Dnia 22 lutego 2016 r.

Justin S. Antonipillai
Doradca
Departamentu Handlu Stanów Zjednoczonych
1401 Constitution Ave., NW
Waszyngton, DC 20230

Ted Dean
Zastępca Wicesekretarza
Urząd ds. Handlu Międzynarodowego
1401 Constitution Ave., NW
Waszyngton, DC 20230

Szanowni Państwo!

W ciągu ostatnich dwóch i pół roku Stany Zjednoczone przekazały wiele istotnych informacji w kontekście negocjacji dotyczących Tarczy Prywatności UE-USA na temat gromadzenia danych przez Wspólnotę Wywiadowczą w wyniku rozpoznania radioelektronicznego. Obejmowały one informacje na temat obowiązujących ram prawnych, wielopoziomowego nadzoru nad tymi działaniami, wysokiej przejrzystości tych działań oraz ogólnej ochrony prywatności i wolności obywatelskich w celu wspierania Komisji Europejskiej w określaniu odpowiedniego poziomu tej ochrony, jako że działania te wiązały się z wyjątkiem od zasad Tarczy Prywatności dotyczącym bezpieczeństwa narodowego. W niniejszym piśmie podsumowano przekazane informacje.

I. DYREKTYWA POLITYCZNA PREZYDENTA NR 28 I PROWADZENIE PRZEZ USA DZIAŁALNOŚCI W ZAKRESIE ROZPOZNANIA RADIOELEKTRONICZNEGO

Wspólnota Wywiadowcza Stanów Zjednoczonych gromadzi dane wywiadowcze w wysoce kontrolowany sposób, w ścisłej zgodności z przepisami prawa amerykańskiego, podlegający wielu szczeblom nadzoru, z uwzględnieniem istotnych priorytetów wywiadu zagranicznego i bezpieczeństwa narodowego. Gromadzenie danych w wyniku rozpoznania radioelektroniczne przez Stany Zjednoczone podlega różnorodnym przepisom prawnym i strategiom politycznych, w tym Konstytucji Stanów Zjednoczonych, ustawie o kontroli wywiadu (tytuł 50 § 1801 i nast. U.S.C.), rozporządzeniu wykonawczemu 12333 i jego procedurom wykonawczym, wytycznym Prezydenta oraz licznym procedurom i wytycznym, zatwierdzonym przez Sąd ds. Nadzoru nad Obcym Wywiadem (ang. Foreign Intelligence Surveillance Court) i Prokuratora Generalnego, którymi wprowadzono dodatkowe zasady dotyczące ograniczenia, zatrzymywania, wykorzystywania i rozpowszechniania danych wywiadowczych ([1]).

a. **Przegląd dyrektywy politycznej Prezydenta nr 28**

W styczniu 2014 r. prezydent Obama wygłosił przemówienie, w którym przedstawił różne reformy obejmujące działania USA w zakresie rozpoznania radioelektronicznego, a także wydał dyrektywę polityczną Prezydenta nr 28 dotyczącą tych działań ([2]). Prezydent podkreślił, że działania USA w zakresie rozpoznania radioelektronicznego zapewniają większe bezpieczeństwo nie tylko naszego państwa i naszych wolności, lecz również bezpieczeństwa i wolności innych państw, w tym państw członkowskich UE, które korzystają z danych gromadzonych przez amerykańskie agencje wywiadu w celu ochrony własnych obywateli.

W dyrektywie politycznej Prezydenta nr 28 wprowadzono szereg zasad i wymogów, które mają zastosowanie do wszystkich działań USA w zakresie rozpoznania radioelektronicznego i do wszystkich osób, bez względu na obywatelstwo lub miejsce zamieszkania. W szczególności wprowadzono pewne wymogi w odniesieniu do procedur w celu uregulowania gromadzenia, zatrzymywania i rozpowszechniania danych osobowych dotyczących osób niebędących obywatelami i rezydentami Stanów Zjednoczonych, pozyskanych w wyniku rozpoznania radioelektronicznego prowadzonego przez Stany Zjednoczone. Te wymogi przedstawiono bardziej szczegółowo poniżej, ale można je podsumować w następujący sposób:

— w dyrektywie politycznej Prezydenta podkreślono, że Stany Zjednoczone gromadzą dane w wyniku rozpoznania radioelektronicznego wyłącznie w zakresie dozwolonym w ustawie, rozporządzeniu wykonawczym lub innych wytycznych Prezydenta,

([1]) Więcej informacji na temat działań wywiadowczych Stanów Zjednoczonych można znaleźć w internecie i są one ogólnodostępne za pośrednictwem serwisu Wspólnoty Wywiadowczej „IC on the Record" (www.icontherecord.tumblr.com), ogólnodostępnej strony internetowej Urzędu Dyrektora Krajowych Służb Wywiadowczych poświęconej zwiększaniu publicznej widoczności działań wywiadowczych rządu.

([2]) Dostępne pod adresem https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— w dyrektywie politycznej Prezydenta wprowadzono procedury w celu zapewnienia, aby działania w zakresie rozpoznania radioelektronicznego były prowadzone jedynie dla realizacji uzasadnionych i dozwolonych celów bezpieczeństwa narodowego,

— w dyrektywie politycznej Prezydenta wprowadzono wymóg, aby ochrona prywatności i wolności obywatelskie stanowiły integralny element w toku planowania działań w zakresie rozpoznania radioelektronicznego. W szczególności Stany Zjednoczone nie gromadzą danych wywiadowczych na potrzeby wyeliminowania krytycznych opinii lub sprzeciwu bądź wywołania krytyki lub sprzeciwu; na niekorzyść danej jednostki ze względu na jej pochodzenie etniczne, pochodzenie rasowe, płeć, orientację seksualną lub religię; lub w celu przyznania korzyści handlowej amerykańskim przedsiębiorstwom i sektorom biznesowym,

— w dyrektywie politycznej Prezydenta nakazano, aby gromadzenie danych w wyniku rozpoznania radioelektronicznego było dostosowane do określonych potrzeb oraz aby dane gromadzone hurtowo w wyniku rozpoznania radioelektronicznego były wykorzystywane jedynie do ściśle określonych celów,

— w dyrektywie politycznej Prezydenta nakazano, aby Wspólnota Wywiadowcza przyjęła procedury „odpowiednio zaplanowane w celu ograniczenia rozpowszechniania i zatrzymywania danych osobowych zgromadzonych w wyniku rozpoznania radioelektronicznego", a w szczególności procedury rozszerzające pewne rodzaje ochrony danych osobowych osób będących obywatelami i rezydentami Stanów Zjednoczonych na dane osób niebędących obywatelami i rezydentami Stanów Zjednoczonych,

— przyjęto i opublikowano procedury dla agencji dotyczące wdrożenia dyrektywy politycznej Prezydenta nr 28.

Stosowanie procedur i form ochrony przewidzianych w niniejszym piśmie do Tarczy Prywatności jest jasne. Gdy dane zostały przekazane korporacjom w Stanach Zjednoczonych zgodnie z zasadami Tarczy Prywatności, lub w praktyce w dowolny sposób, amerykańskie agencje wywiadu mogą uzyskać te dane od tych korporacji tylko wtedy, gdy ich wniosek jest zgodny z ustawą o kontroli wywiadu lub został złożony na podstawie jednego z przepisów ustawowych dotyczących wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego, które omówiono poniżej ([1]). Ponadto bez potwierdzenia doniesień medialnych sugerujących, że Wspólnota Wywiadowcza Stanów Zjednoczonych gromadzi dane z kabli transatlantyckich, podczas gdy dane są przekazywane do Stanów Zjednoczonych, lub zaprzeczenia tym twierdzeniom: gdyby Wspólnota Wywiadowcza Stanów Zjednoczonych gromadziła dane z kabli transatlantyckich, jej działanie podlegałoby ograniczeniom i gwarancjom przedstawionym w niniejszym dokumencie, w tym wymogom dyrektywy politycznej Prezydenta nr 28.

b. **Ograniczenia gromadzenia danych**

W dyrektywie politycznej Prezydenta nr 28 przedstawiono wiele istotnych zasad ogólnych, którym podlega gromadzenie danych w wyniku rozpoznania radioelektronicznego.

— Gromadzenie danych w wyniku rozpoznania radioelektronicznego musi zostać zatwierdzone w drodze ustawy lub zezwolenia Prezydenta i należy je przeprowadzić zgodnie z konstytucją i prawem.

— W ramach rozpoznania radioelektronicznego prywatność i wolności obywatelskie muszą być integralną częścią planowania działań.

— Dane będą gromadzone w wyniku rozpoznania radioelektronicznego wyłącznie wtedy, gdy uzasadni to ważny cel działań wywiadowczych lub kontrowywiadowczych.

— Stany Zjednoczone nie będą gromadzić danych wywiadowczych w wyniku rozpoznania radioelektronicznego na potrzeby wyeliminowania krytycznych opinii lub sprzeciwu bądź wywołania krytyki lub sprzeciwu.

— Stany Zjednoczone nie będą gromadzić danych wywiadowczych w wyniku rozpoznania radioelektronicznego na niekorzyść danej jednostki ze względu na jej pochodzenie etniczne, pochodzenie rasowe, płeć, orientację seksualną lub religię tej osoby.

— Stany Zjednoczone nie będą gromadzić danych wywiadowczych w wyniku rozpoznania radioelektronicznego w celu przyznania korzyści handlowej amerykańskim przedsiębiorstwom i sektorom biznesowym.

— Działania USA w ramach rozpoznania radioelektronicznego zawsze muszą być dostosowane do danych potrzeb przy uwzględnieniu dostępności innych źródeł danych. Oznacza to między innymi, że gromadzenie danych w wyniku rozpoznania radioelektronicznego należy – zawsze, gdy jest to możliwe – przeprowadzać w ukierunkowany sposób, a nie hurtowo.

Wymóg, aby działalność w zakresie rozpoznania radioelektronicznego była „dostosowana do danych potrzeb" ma zastosowanie do sposobu, w jaki gromadzone są dane w wyniku rozpoznania radioelektronicznego oraz do tego, co faktycznie jest gromadzone. Przykładowo – określając, czy należy zgromadzić dane w wyniku rozpoznania radioelektronicznego, Wspólnota Wywiadowcza musi – w stosownych przypadkach i w miarę możliwości – uwzględnić dostępność

([1]) Organy egzekwowania prawa lub agencje regulacyjne mogą wystąpić do korporacji o przekazanie danych do celów dochodzeniowych w Stanach Zjednoczonych zgodnie z innymi aktami stanowiącymi podstawę prawną na gruncie przepisów prawa karnego, z zakresu administracji cywilnej i przepisów regulacyjnych, które wykraczają poza zakres niniejszego dokumentu ograniczającego się do aktów stanowiących podstawę prawną na gruncie przepisów z zakresu bezpieczeństwa narodowego.

innych danych, w tym źródeł dyplomatycznych lub publicznych, i ustalić priorytety gromadzenia danych za pomocą tych środków. Co więcej, w strategiach politycznych jednostek Wspólnoty Wywiadowczej należy wprowadzić wymóg, aby – zawsze, gdy jest to możliwe – gromadzenie danych koncentrowało się na określonych celach lub zagadnieniach związanych z wywiadem zagranicznym przy każdorazowym zastosowaniu wyróżników (np. określonych urządzeń, terminów umożliwiających selekcję i wskaźników).

Ważne jest, aby informacje dostarczone Komisji postrzegać jako całość. O tym, co jest możliwe do zrealizowania, nie decydują osoby fizyczne wedle własnego uznania, ale kwestia ta podlega strategiom politycznym, które agencje wydały na podstawie dyrektywy politycznej Prezydenta nr 28 – którą opublikowano – i innym procesom opisanym w dyrektywie ([1]). Zgodnie z dyrektywą polityczną Prezydenta nr 28 hurtowe gromadzenie informacji w ramach rozpoznania radioelektronicznego stanowi gromadzenie, które „ze względów technicznych i operacyjnych, jest dokonywane bez wykorzystania wyróżników (np. konkretnych identyfikatorów, terminów umożliwiających selekcję itp.)". W tym kontekście w dyrektywie politycznej Prezydenta nr 28 uznano, że jednostki Wspólnoty Wywiadowczej muszą w pewnych okolicznościach gromadzić hurtowo dane w wyniku rozpoznania radioelektronicznego, aby określić nowe lub pojawiające się zagrożenia i inne kluczowe dla bezpieczeństwa narodowego informacje, które są często ukryte w dużych i złożonych systemach nowoczesnej światowej komunikacji. W dyrektywie uwzględniono również również obawy dotyczące prywatności i wolności obywatelskich związane z hurtowym gromadzeniem danych w wyniku rozpoznania radioelektronicznego. W dyrektywie politycznej Prezydenta nr 28 nakazano zatem Wspólnocie Wywiadowczej ustalenie wykazu innych rozwiązań, które umożliwiłyby gromadzenie danych w wyniku rozpoznania radioelektronicznego w ukierunkowany sposób zamiast gromadzenia ich hurtowo. W związku z tym jednostki Wspólnoty Wywiadowczej powinny – zawsze, gdy jest to możliwe – gromadzić dane w wyniku rozpoznania radioelektronicznego w sposób ukierunkowany, a nie hurtowy. ([2]). Zasady te zapewniają, aby wyjątek dotyczący hurtowego gromadzenia danych nie stał się zasadą ogólną.

Koncepcja „zasadności" stanowi podstawową zasadę prawa amerykańskiego. Oznacza, że jednostki Wspólnoty Wywiadowczej nie będą musiały przyjmować jakichkolwiek środków, które są teoretycznie możliwe, ale będą zobowiązane do zrównoważenia swoich działań służących ochronie uzasadnionych interesów w zakresie prywatności i wolności obywatelskich za pomocą praktycznych wymogów dotyczących działalności w zakresie rozpoznania radioelektronicznego. Również w tym wypadku opublikowano strategie polityczne agencji i pewne jest, że sformułowanie „odpowiednio zaplanowane w celu ograniczenia rozpowszechniania i zatrzymywania danych osobowych zgromadzonych w wyniku rozpoznania radioelektronicznego" nie podważa zasady ogólnej.

W dyrektywie politycznej Prezydenta nr 28 przewidziano również, że dane gromadzone hurtowo w wyniku rozpoznania radioelektronicznego można wykorzystywać wyłącznie w sześciu ściśle określonych celach: wykrywania pewnych działań sił zagranicznych i przeciwdziałania im; walki z terroryzmem; przeciwdziałania proliferacji; cyberbezpieczeństwa; wykrywania zagrożeń dla amerykańskich lub sojuszniczych sił zbrojnych i przeciwdziałania tym zagrożeniom; oraz zwalczania transgranicznych zagrożeń przestępstwami, w tym unikania sankcji. Doradca Prezydenta ds. bezpieczeństwa narodowego w porozumieniu z Dyrektorem Krajowych Służb Wywiadowczych będzie co roku dokonywał analizy tych dozwolonych przypadków hurtowego gromadzenia danych w wyniku rozpoznania radioelektronicznego, aby sprawdzić, czy nie należy ich zmienić. Dyrektor Krajowych Służb Wywiadowczych będzie publikował ten wykaz w jak największym możliwym zakresie, na jaki pozwalają wymogi bezpieczeństwa narodowego. Stanowi to istotne i przejrzyste ograniczenie hurtowego gromadzenia danych w wyniku rozpoznania radioelektronicznego.

Ponadto jednostki Wspólnoty Wywiadowczej wdrażające dyrektywę polityczną Prezydenta nr 28 wzmocniły istniejące praktyki i normy analityczne w zakresie zapytań dotyczących niepoddanych ocenie przypadków rozpoznania radioelektronicznego intelligence ([3]). Analitycy muszą uporządkować swoje zapytania lub inne warunki i techniki wyszukiwania w celu zapewnienia, aby pozwalały one na wskazanie danych wywiadowczych istotnych z perspektywy ważnego zadania z zakresu działań wywiadu zagranicznego lub egzekwowania prawa. W tym celu jednostki Wspólnoty Wywiadowczej muszą zagwarantować, że zapytania dotyczące osób będą koncentrować się na tych kategoriach danych gromadzonych w wyniku rozpoznania radioelektronicznego, które odpowiadają wymogom wywiadu zagranicznego lub egzekwowania prawa, tak aby zapobiec wykorzystaniu danych osobowych w sposób niezgodny z tymi wymogami.

Należy podkreślić, że wszelkie działania z zakresu hurtowego gromadzenia danych związane z komunikacją internetową, jakie przeprowadza Wspólnota Wywiadowcza Stanów Zjednoczonych za pomocą rozpoznania radioelektronicznego, odbywają się w internecie na małą skalę. Ponadto stosowanie ukierunkowanych zapytań, jak opisano powyżej, zapewnia, aby analizie poddawane były wyłącznie te dane, które uznaje się za potencjalnie ważne z punktu widzenia działań wywiadowczych. Ograniczenia te mają na celu ochronę prywatności i wolności obywatelskich wszystkich osób, niezależnie od ich narodowości i miejsca zamieszkania.

([1]) Dostępny na stronie www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Procedury te służą wdrożeniu ukierunkowanych i dostosowanych do indywidualnych potrzeb rozwiązań omówionych w niniejszym piśmie, w sposób właściwy dla każdej jednostki Wspólnoty Wywiadowczej.

([2]) Jako przykład można podać procedury Agencji Bezpieczeństwa Narodowego służące wdrożeniu dyrektywy politycznej Prezydenta nr 28, zgodnie z którymi „[z]awsze, gdy jest to możliwe, gromadzenie danych odbywa się przy zastosowaniu co najmniej jednego terminu umożliwiającego selekcję, aby gromadzenie danych mogło skupiać się na konkretnych celach związanych z wywiadem zagranicznym (np. określonych znanych międzynarodowych terrorystach lub grupach terrorystycznych) lub określonych zagadnieniach związanych z wywiadem zagranicznym (np. rozprzestrzenianiu broni masowego rażenia przez zagraniczne siły lub ich przedstawicieli)".

([3]) Dostępny pod adresem: http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Stany Zjednoczone wprowadzają szczegółowe procesy w celu zapewnienia, aby działania w zakresie rozpoznania radioelektronicznego były prowadzone jedynie dla realizacji stosownych celów bezpieczeństwa narodowego. Każdego roku Prezydent, po przeprowadzeniu szeroko zakrojonego i formalnego procesu międzyagencyjnego, ustala najwyższe krajowe priorytety w zakresie gromadzenia danych przez służby wywiadowcze. Dyrektor Krajowych Służb Wywiadowczych jest odpowiedzialny za wpisanie tych priorytetów w ramy amerykańskich priorytetów wywiadowczych. Na mocy dyrektywy politycznej Prezydenta nr 28 wzmocniono i usprawniono proces międzyagencyjny, aby zapewnić przegląd i zatwierdzanie wszystkich priorytetów wywiadowczych Wspólnoty Wywiadowczej przez decydentów wysokiego szczebla. Dyrektywa Wspólnoty Wywiadowczej nr 204, która zawiera dalsze wytyczne dotyczące ram amerykańskich priorytetów wywiadowczych, została uaktualniona w styczniu 2015 r. o wymogi dyrektywy politycznej Prezydenta nr 28 ([1]). Mimo że ramy amerykańskich priorytetów wywiadowczych są poufne, informacje związane ze szczegółowymi amerykańskimi priorytetami wywiadowczymi w odniesieniu do krajów trzecich są udostępniane co roku w jawnym dokumencie „Ocena zagrożenia globalnego" (ang. Worldwide Threat Assessment) sporządzanym przez Dyrektora Krajowych Służb Wywiadowczych, który jest również ogólnodostępny na stronie internetowej Urzędu Dyrektora Krajowych Służb Wywiadowczych.

Priorytety określone w ramach amerykańskich priorytetów wywiadowczych są stosunkowo ogólne. Obejmują one takie kwestie jak dążenie do zwiększenia potencjału jądrowego oraz w zakresie rakietowych pocisków balistycznych przez określonych przeciwników zagranicznych, skutki korupcji karteli narkotykowych oraz naruszenia praw człowieka w określonych państwach. Mają one zastosowanie nie tylko przy rozpoznaniu radioelektronicznym, lecz we wszystkich działaniach wywiadowczych. Organem odpowiedzialnym za przełożenie priorytetów zawartych w ramach amerykańskich priorytetów wywiadowczych na faktyczne gromadzenie danych w wyniku rozpoznania radioelektronicznego jest Krajowy Komitet Rozpoznania Radioelektronicznego (ang. National Signals Intelligence Committee), czyli SIGCOM. Funkcjonuje on pod auspicjami Dyrektora Agencji Bezpieczeństwa Narodowego (NSA), wyznaczonego na mocy rozporządzenia wykonawczego nr 12333 na „kierownika ds. rozpoznania radioelektronicznego" odpowiedzialnego za nadzór nad rozpoznaniem radioelektronicznym we Wspólnocie Wywiadowczej oraz jego koordynację pod nadzorem zarówno Sekretarza Obrony, jak i Dyrektora Krajowych Służb Wywiadowczych. W SIGCOM zasiadają przedstawiciele wszystkich agencji Wspólnoty Wywiadowczej, a po całkowitym wdrożeniu przez Stany Zjednoczone dyrektywy politycznej Prezydenta nr 28 w jego składzie znajdą się także przedstawiciele wszystkich innych departamentów i agencji, których polityka jest związana z rozpoznaniem radioelektronicznym.

Wszystkie departamenty i agencje USA korzystające z danych pozyskanych w wyniku działań służb wywiadowczych składają wnioski o gromadzenie danych do SIGCOM. SIGCOM rozpatruje te wnioski, upewnia się co do ich zgodności z ramami amerykańskich priorytetów wywiadowczych oraz przydziela im priorytety według poniższych kryteriów.

— Czy rozpoznanie radioelektroniczne jest w stanie dostarczyć przydatnych informacji w danym przypadku czy istnieją lepsze i bardziej opłacalne źródła informacji pozwalające na spełnienie tego wymogu, np. obrazy lub informacje pochodzące z ogólnodostępnych źródeł?

— Jak bardzo potrzebne są te informacje? Jeżeli nadano im wysoki priorytet w ramach amerykańskich priorytetów wywiadowczych, najczęściej będą miały wysoki priorytet w odniesieniu do rozpoznania radioelektronicznego.

— Jaki rodzaj rozpoznania radioelektronicznego mógłby zostać zastosowany?

— Czy proces gromadzenia danych jest maksymalnie dostosowany do danych potrzeb? Czy powinny obowiązywać ograniczenia czasowe, geograficzne lub inne?

W procesie dotyczącym wymogów w zakresie rozpoznania radioelektronicznego Stanów Zjednoczonych wymagane jest także wyraźne uwzględnienie innych czynników, mianowicie:

— Czy docelowe dane, które mają być gromadzone, lub metodyka zastosowana w tym celu są szczególnie wrażliwe? Jeżeli tak, niezbędne będzie dokonanie oceny przez decydentów wysokiego szczebla.

— Czy gromadzenie danych będzie stanowić nieuzasadnione ryzyko dla prywatności i wolności obywatelskich, niezależnie od narodowości?

— Czy są konieczne dodatkowe gwarancje dotyczące rozpowszechniania i zatrzymywania danych na potrzeby ochrony prywatności lub interesów bezpieczeństwa narodowego?

Ponadto pod koniec procesu przeszkolony personel Agencji Bezpieczeństwa Narodowego analizuje priorytety zatwierdzone przez SIGCOM oraz bada i określa konkretne terminy umożliwiające selekcję, takie jak numery telefonów czy adresy e-mail, które mają posłużyć do gromadzenia danych wywiadowczych w ramach realizacji tych priorytetów. Każdy z identyfikatorów musi zostać poddany kontroli i zatwierdzony zanim zostanie wprowadzony do systemów gromadzenia danych NSA. Jednak nawet wtedy miejsce, w którym dokonuje się właściwego gromadzenia danych oraz to, czy działania te zostaną podjęte, będą zależeć częściowo od dodatkowych względów takich jak dostępność

([1]) Dostępny pod adresem: http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

odpowiednich środków pozyskiwania danych. Proces ten zapewnia, że cele gromadzenia danych w ramach rozpoznania radioelektronicznego USA odzwierciedlają uzasadnione i istotne potrzeby wywiadu. Oczywiście, gdy gromadzenie danych przebiega zgodnie z ustawą o kontroli wywiadu, Agencja Bezpieczeństwa Narodowego i inne agencje muszą respektować dodatkowe ograniczenia zatwierdzone przez Sąd ds. Nadzoru nad Obcym Wywiadem. Podsumowując, ani Agencja Bezpieczeństwa Narodowego, ani żadna inna agencja wywiadu USA nie decyduje samodzielnie o tym, jakie informacje należy pozyskać.

Proces ten zasadniczo gwarantuje, że wszystkie priorytety wywiadowcze są określane przez decydentów wysokiego szczebla, którzy są w stanie najlepiej zdefiniować wymagania wywiadu USA, oraz że decydenci uwzględniają nie tylko potencjalną wartość informacji, lecz także ryzyko związane z ich pozyskiwaniem, w tym ryzyko dla prywatności, państwowych interesów gospodarczych oraz stosunków międzynarodowych.

Jeśli chodzi o dane przekazywane do Stanów Zjednoczonych zgodnie z Tarczą Prywatności, pomimo że Stany Zjednoczone nie mogą potwierdzić szczegółowych metod i działań służb wywiadowczych ani im zaprzeczyć, wymogi dyrektywy politycznej Prezydenta nr 28 dotyczą wszelkich działań związanych z rozpoznaniem radioelektronicznym prowadzonych przez Stany Zjednoczone, bez względu na rodzaj lub źródło pozyskiwanych informacji. Co więcej, ograniczenia i gwarancje właściwe dla gromadzenia danych w ramach rozpoznania radioelektronicznego dotyczą danych zgromadzonych w ten sposób dla każdego zatwierdzonego celu, zarówno celów stosunków narodowych, jak i bezpieczeństwa narodowego.

Procedury opisane powyżej świadczą o wyraźnym zaangażowaniu w zapobieganie gromadzenia danych w ramach rozpoznania radioelektronicznego w sposób dowolny i bezkrytyczny oraz we wdrażanie – na najwyższych szczeblach naszego rządu – zasady rozsądnego działania. Dyrektywa polityczna Prezydenta nr 28 i agencyjne procedury wdrażające objaśniają nowe i obowiązujące ograniczenia, aby bardziej szczegółowo zobrazować cel, dla którego Stany Zjednoczone stosują rozpoznanie radioelektroniczne i pozyskują w ten sposób informacje. Powinny one zapewnić, że działania w ramach rozpoznania radioelektronicznego są i będą przeprowadzane jedynie dla dalszych uzasadnionych celów wywiadu.

c. **Ograniczenia dotyczące zatrzymywania i rozpowszechniania**

Zgodnie z sekcją 4 dyrektywy politycznej Prezydenta nr 28 każdą agencję Wspólnoty Wywiadowczej obowiązują wyraźne ograniczenia dotyczące zatrzymywania i rozpowszechniania danych osobowych osób nieposiadających obywatelstwa Stanów Zjednoczonych pozyskanych w wyniku rozpoznania radioelektronicznego; ograniczenia te są porównywalne do ograniczeń w przypadku obywateli Stanów Zjednoczonych. Zasady te uwzględnione są w procedurach każdej z agencji Wspólnoty Wywiadowczej przedstawionych w lutym 2015 oraz ogólnodostępnych. Aby dane osobowe kwalifikowały się do zatrzymania lub rozpowszechniania jako dane wywiadowcze, muszą dotyczyć zatwierdzonych potrzeb wywiadu, jak określono w procesie ram amerykańskich priorytetów wywiadowczych opisanym powyżej; być zasadnie uznane za dowód przestępstwa lub spełniać jeden z innych warunków do zatrzymania informacji dotyczących obywateli i rezydentów Stanów Zjednoczonych, które to informacje zostały określone w rozporządzeniu wykonawczym nr 12333 sekcja 2.3.

Informacje, które nie klasyfikują się do wyżej wymienionych kategorii, nie mogą być przetrzymywane przez okres dłuższy niż pięć lat, chyba że Dyrektor Krajowych Służb Wywiadowczych wyraźnie określi, że dalsze ich zatrzymanie leży w interesie bezpieczeństwa narodowego Stanów Zjednoczonych. Agencje Wspólnoty Wywiadowczej muszą zatem usunąć informacje dotyczące osób spoza Stanów Zjednoczonych zgromadzone w wyniku rozpoznania radioelektronicznego po pięciu latach od momentu ich pozyskania, chyba że, na przykład, informacje te zostały uznane za istotne wobec zatwierdzonej potrzeby wywiadu, lub jeśliDyrektor Krajowych Służb Wywiadowczych określi, po rozważeniu opinii urzędnika ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych (ang. ODNI Civil Liberties Protection Officer) oraz urzędników agencji ds. prywatności i wolności obywatelskich, że dalsze zatrzymywanie danych leży w interesie bezpieczeństwa narodowego.

Co więcej, zgodnie ze wszystkimi działaniami agencji wdrażającymi dyrektywę polityczną Prezydenta nr 28 informacje na temat osoby nie mogą być rozpowszechniane jedynie dlatego, że osoba ta nie jest obywatelem lub rezydentem Stanów Zjednoczonych; Urząd Dyrektora Krajowych Służb Wywiadowczych wydałdyrektywę skierowaną do wszystkich agencji Wspólnoty Wywiadowczej ([1]), by wymóg ten został uwzględniony. Wyraźnie wymaga się, aby personel Wspólnoty Wywiadowczej uwzględniał kwestie ochrony prywatności osób niebędących obywatelami i rezydentami Stanów Zjednoczonych przy sporządzaniu i rozpowszechnianiu sprawozdań służb wywiadowczych. W szczególności dane zgromadzone w wyniku rozpoznania radioelektronicznego dotyczące rutynowych czynności osoby obcego pochodzenia nie byłoby uznane za dane wywiadowcze, które mogłyby być trwale rozpowszechniane lub zatrzymywane jedynie z tego tytułu, chyba że jest to zgodne z jedną z zatwierdzonych potrzeby wywiadu. Stanowi to istotne ograniczenie i odpowiada na obawy Komisji Europejskiej dotyczące szerokiego zakresu definicji danych wywiadowczych określonej w rozporządzeniu wykonawczym nr 12333.

([1]) Dyrektywa skierowana do Wspólnoty Wywiadowczej (ICD) 203, dostępna pod adresem http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

d. **Przestrzeganie zasad i nadzór**

Amerykański system nadzoru służb wywiadowczych określa rygorystyczną i wielowarstwową kontrolę, aby zagwarantować przestrzeganie obowiązującego prawa i procedur, włącznie z tymi, które dotyczą gromadzenia, zatrzymywania oraz rozpowszechniania informacji na temat osób niebędących obywatelami i rezydentami Stanów Zjednoczonych pozyskanych w wyniku rozpoznania radioelektronicznego, co zostało określone w dyrektywie politycznej Prezydenta nr 28. W ramach kontroli:

— Wspólnota Wywiadowcza zatrudnia setki pracowników odpowiedzialnych za nadzór. W samej Agencji Bezpieczeństwa Narodowego za zgodność z zasadami jest odpowiedzialnych ponad 300 pracowników; w innych agencjach również funkcjonują biura zajmujące się nadzorem. Ponadto Departament Sprawiedliwości zapewnia szeroki nadzór nad działaniami służb wywiadowczych; nadzór sprawuje również Departament Obrony.

— Każda z agencji Wspólnoty Wywiadowczej ma swoje własne Biuro Inspektora Generalnego odpowiedzialne, między innymi, za nadzór nad działaniami służb wywiadowczych. Inspektorzy Generalni są niezależni ustawowo; mają szerokie uprawnienia w kwestii przeprowadzania dochodzeń, audytów oraz kontroli programów, w tym oszustw i nadużyć lub naruszeń prawa; mogą również zalecić działania naprawcze. Podczas gdy zalecenia inspektora generalnego nie są wiążące, jego sprawozdania są często upubliczniane oraz w każdym przypadku przedkładane Kongresowi; dotyczy to sprawozdań uzupełniających w przypadku, gdy działania naprawcze zalecone w poprzednich sprawozdaniach nie zostały jeszcze zakończone. Kongres jest zatem informowany o wszelkich przypadkach nieprzestrzegania zasad i może wywierać presję, w tym poprzez środki budżetowe, aby doprowadzić do podjęcia działań naprawczych. Szereg sprawozdań Inspektora Generalnego w sprawie programów służb wywiadowczych został udostępniony do wglądu publicznego ([1]).

— Biuro Wolności Obywatelskich i Ochrony Prywatności Urzędu Dyrektora Krajowych Służb Wywiadowczych (ang. ODNI's Civil Liberties and Privacy Office; CLPO) jest zobowiązane do zapewnienia, by działania Wspólnoty Wywiadowczej prowadziły do zwiększenia bezpieczeństwa narodowego, a wolności obywatelskie oraz prawo do prywatności były jednocześnie chronione ([2]). Inne agencje Wspólnoty Wywiadowczej mają własnych urzędników ds. ochrony prywatności.

— Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi (ang. The Privacy and Civil Liberties Oversight Board), niezależny organ ustawowy, jest zobowiązany do analizy i oceny programów i polityki w ramach walki z terroryzmem, w tym stosowania rozpoznania radioelektronicznego w celu zapewnienia w nich odpowiedniej ochrony prywatności i wolności obywatelskich. Zarząd wydał szereg publicznych sprawozdań dotyczących działań wywiadu.

— Jak opisano bardziej szczegółowo poniżej, Sąd ds. Nadzoru nad Obcym Wywiadem, w którego skład wchodzą niezależni sędziowie federalni, jest odpowiedzialny za zapewnienie zgodności wszelkich działań związanych z gromadzeniem danych poprzez rozpoznanie radioelektroniczne z ustawą o kontroli wywiadu oraz nadzór nad tymi działaniami.

— Dodatkowo Kongres Stanów Zjednoczonych, szczególnie Komisje ds. Wywiadu oraz Komisje Sprawiedliwości Izby i Senatu, ponosi dużą odpowiedzialność za nadzór nad wszelkimi działaniami amerykańskich służb wywiadowczych, w tym rozpoznanie radioelektroniczne Stanów Zjednoczonych.

Poza tymi formalnymi mechanizmami nadzoru, Wspólnota Wywiadowcza stosuje szereg mechanizmów, aby zapewnić zgodność z ograniczeniami dotyczącymi gromadzenia danych. Na przykład:

— Urzędnicy gabinetu mają obowiązek co roku potwierdzać potrzeby związane z rozpoznaniem radioelektronicznym.

— Agencja Bezpieczeństwa Narodowego kontroluje cele rozpoznania radioelektronicznego w procesie gromadzenia danych, aby ustalić, czy faktycznie przyczyniają się one do realizacji priorytetów służb wywiadowczych; agencja ta zaprzestanie gromadzenia danych dotyczących celów, które nie spełniają tego warunku. Dodatkowe procedury zapewniają okresową weryfikację terminów umożliwiających selekcję.

([1]) Zob. np. sprawozdanie Departamentu Sprawiedliwości Stanów Zjednoczonych Inspektora Generalnego „Kontrola działań Federalnego Biura Śledczego zgodnie z sekcją 702 ustawy o kontroli wywiadu z 2008 r." (wrzesień 2012), dokument dostępny pod adresem https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) Zob. www.dni.gov/clpo.

— Na podstawie zalecenia niezależnej grupy ds. kontroli powołanej przez prezydenta Obamę, Dyrektor Krajowych Służb Wywiadowczych wprowadził nowy mechanizm monitorowania gromadzenia danych pozyskanych w ramach rozpoznania radioelektronicznego oraz ich rozpowszechniania, gdy dane charakteryzują się szczególną wrażliwością ze względu na charakter celu lub sposób gromadzenia danych, aby zapewnić, że działania te są zgodne z postanowieniami decydentów.

— Urząd Dyrektora Krajowych Służb Wywiadowczych dokonuje także corocznej kontroli przydziału środków Wspólnoty Wywiadowczej pod względem priorytetów określonych w ramach amerykańskich priorytetów wywiadowczych oraz ogólnej misji służb wywiadowczych. Kontrola obejmuje ocenę jakości wszystkich sposobów gromadzenia informacji, w tym rozpoznania radioelektronicznego, i dotyczy zakończonych działań (w jakim stopniu działania Wspólnoty Wywiadowczej służące realizacji jej celów zakończyły się powodzeniem?) oraz przyszłych potrzeb (jakie będą potrzeby Wspólnoty Wywiadowczej w przyszłości?). Zapewnia to stosowanie środków rozpoznania radioelektronicznego do najważniejszych krajowych priorytetach.

Jak udowodniono w tym wyczerpującym opisie, Wspólnota Wywiadowcza nie decyduje samodzielnie, którym rozmowom się przysłuchiwać ani nie próbuje gromadzić wszystkich możliwych danych, a jej działalność jest nadzorowana. Działania Wspólnoty Wywiadowczej skoncentrowane są na priorytetach wyznaczonych przez decydentów w procesie, w którym zaangażowany jest cały rząd, przy czym proces ten podlega nadzorowi zarówno w obrębie Agencji Bezpieczeństwa Narodowego, jak i przez Urząd Dyrektora Krajowych Służb Wywiadowczych, Departament Sprawiedliwości oraz Departament Obrony.

Dyrektywa zawiera także szereg innych przepisów, aby zapewnić ochronę danych osobowych zgromadzonych w ramach rozpoznania radioelektronicznego, bez względu na narodowość osoby, której dane dotyczą. Na przykład dyrektywa polityczna Prezydenta nr 28 przewiduje procedury w zakresie bezpieczeństwa danych, dostępu oraz jakości służące ochronie danych osobowych zgromadzonych za pośrednictwem rozpoznania radioelektronicznego, jak również obowiązkowe szkolenia mające zagwarantować, że pracownicy rozumieją obowiązek ochrony danych osobowych, niezależnie od narodowości osoby, której te dane dotyczą. W dyrektywie przewiduje się również dodatkowe mechanizmy nadzoru i przestrzegania zasad. Obejmują one okresowe kontrole i przeglądy praktyk związanych z ochroną danych osobowych zgromadzonych w wyniku rozpoznania radioelektronicznego przeprowadzane przez odpowiednich urzędników ds. nadzoru i zgodności. Przegląd obejmuje również ocenę przestrzeganie procedur ochrony tego typu danych przez agencje.

Dodatkowo zgodnie z dyrektywą polityczną Prezydenta nr 28, kwestie związane z osobami, które nie są obywatelami lub rezydentami Stanów Zjednoczonych, będą rozstrzygane na wyższych szczeblach rządu. W przypadku wystąpienia istotnego problemu z przestrzeganiem zasad związanego z danymi osobistymi jakiejkolwiek osoby, które zostały zgromadzone na skutek działań w ramach rozpoznania radioelektronicznego, poza spełnieniem wszelkich innych istniejących wymogów dotyczących zgłaszania, kwestia ta musi dodatkowo zostać bezzwłocznie zgłoszona Dyrektorowi Krajowemu Służb Wywiadowczych. Jeśli problem związany jest z danymi osobowymi dotyczącymi osoby nieposiadającej amerykańskiego obywatelstwa Dyrektor Krajowy Służb Wywiadowczych, podczas konsultacji z Sekretarzem Stanu oraz kierownikiem odpowiedniej agencji Wspólnoty Wywiadowczej, ustali, czy powinny zostać podjęte działania mające na celu poinformowanie odpowiedniego rządu zagranicznego, zgodnie z ochroną źródeł i metod oraz personelu Stanów Zjednoczonych. Co więcej, zgodnie z dyrektywą polityczną Prezydenta nr 28, Sekretarz Stanu wyznaczył urzędnika wysokiego szczebla, podsekretarz stanu Catherine Novelli, na osobę odpowiedzialną za kontakty z rządami zagranicznymi, które pragną zgłosić swoje obawy dotyczące działań z zakresu rozpoznania radioelektronicznego prowadzonych przez Stany Zjednoczone. Ten wysoki stopień zaangażowania jest przykładem starań, jakich rząd Stanów Zjednoczonych podejmuje przez ostatnie kilka lat, aby zwiększyć zaufanie do licznych pokrywających się gwarancji dotyczących danych osobowych, które obecnie obowiązują i dotyczą zarówno danych obywateli i rezydentów Stanów Zjednoczonych, jak i osób niebędących obywatelami i rezydentami Stanów Zjednoczonych.

e. **Streszczenie**

Procedury Stanów Zjednoczonych dotyczące gromadzenia, zatrzymywania oraz rozpowszechniania danych zapewniają istotne zabezpieczenia dla danych osobowych wszystkich osób, bez względu na ich narodowość. Procedury te gwarantują w szczególności, że Wspólnota Wywiadowcza skupia się na swojej misji bezpieczeństwa narodowego zgodnie z obowiązującym prawem, rozporządzeniami wykonawczymi oraz dyrektywami prezydenckimi; chroni dane przed nieuprawnionym dostępem, wykorzystaniem i ujawnieniem; oraz prowadzi działania, które poddawane są wielopoziomowym kontrolom i nadzorowi, w tym komisji nadzorczych Kongresu. Dyrektywa polityczna Prezydenta nr 28 oraz wdrażające ją procedury są odzwierciedleniem naszych starań, aby rozszerzyć określoną minimalizację oraz inne istotne zasady ochrony danych na dane osobowe dotyczące wszystkich osób bez względu na ich narodowość. Dane osobowe zgromadzone w wyniku rozpoznania radioelektronicznego Stanów Zjednoczonych podlegają zasadom i wymaganiom amerykańskiego prawa oraz kierownictwu prezydenta, w tym zabezpieczeniom określonym w dyrektywie politycznej Prezydenta nr 28. Zasady i wymagania te gwarantują, że wszystkie osoby są traktowane z godnością i szacunkiem, niezależnie od ich narodowości lub miejsca zamieszkania; uznają one również, że wszystkie osoby mają uzasadnione prawo do ochrony prywatności przy przetwarzaniu ich danych osobowych.

II. USTAWA O KONTROLI WYWIADU – SEKCJA 702

Gromadzenie danych zgodnie z sekcją 702 ustawy o kontroli wywiadu ([1]) nie jest „masowe i bezkrytyczne", lecz skupia się ściśle na danych dotyczących indywidualnie określonych i zasadnych celów; jest wyraźnie dozwolone przez określony organ ustawowy; oraz podlega zarówno niezależnej kontroli sądowej, jak i dokładnym przeglądom i nadzorowi władzy wykonawczej oraz Kongresu. Dane pozyskane zgodnie z sekcją 702 uznaje się za dane zgromadzone w wyniku rozpoznania radioelektronicznego z zastrzeżeniem wymogów dyrektywy politycznej Prezydenta nr 28 ([2]).

Gromadzenie danych zgodnie z sekcją 702 jest jednym z najcenniejszych źródeł danych chroniącym zarówno Stany Zjednoczone, jak i naszych europejskich partnerów. Kompleksowe informacje na temat działania i nadzoru na podstawie sekcji 702 są dostępne do wglądu publicznego. Liczne oświadczenia złożone w sądzie, orzeczenia sądowe oraz sprawozdania dotyczące nadzoru związane z programem zostały odtajnione i zamieszczone na ogólnodostępnej stronie internetowej Urzędu Dyrektora Krajowych Służb www.icontherecord.tumblr.com. Co więcej, sekcja 702 została poddana kompleksowej analizie przez Radę Nadzoru nad Prywatnością i Wolnościami Obywatelskimi w sprawozdaniu dostępnym na stronie https://www.pclob.gov/library/702-Report.pdf ([3]).

Sekcja 702 została uchwalona jako część ustawy z 2008 r. ([4]) zmieniającej ustawę o kontroli wywiadu po szeroko zakrojonej debacie publicznej w Kongresie. Zezwala się w niej na pozyskiwanie danych wywiadowczych poprzez skoncentrowanie działań na osobach niebędących obywatelami i rezydentami Stanów Zjednoczonych znajdujących się poza terytorium Stanów Zjednoczonych przy obowiązkowej pomocy ze strony amerykańskich dostawców usług łączności elektronicznej. W sekcji 702 upoważnia się Prokuratora Generalnego oraz Dyrektora Krajowych Służb Wywiadowczych – dwóch urzędników na szczeblu gabinetu powoływanych przez prezydenta i zatwierdzanych przez Senat – do przedkładania corocznych certyfikacji do Sądu ds. Nadzoru nad Wywiadem Zagranicznym ([5]). Certyfikacje te określają szczególne kategorie danych wywiadowczych, które mają być gromadzone, takie jak dane wywiadowcze związane z walką z terroryzmem lub bronią masowego rażenia, i które muszą być klasyfikowane zgodnie z kategoriami danych wywiadowczych określonymi w ustawie o kontroli wywiadu ([6]). Jak zauważył Zarząd Nadzoru nad Prywatnością i Wolnościami Obywatelskimi, „ograniczenia te nie pozwalają na nieograniczone gromadzenie danych o cudzoziemcach" ([7]).

Certyfikacje muszą również zawierać procedury „ukierunkowywania" oraz „minimalizacji", zbadane i zatwierdzone przez Sąd ds. Nadzoru nad Wywiadem Zagranicznym ([8]). Procedury ukierunkowywania są opracowane w sposób, który gwarantuje, że gromadzenie danych ma miejsce jedynie wtedy, gdy jest dozwolone ustawowo oraz mieści się w zakresie certyfikacji; procedury minimalizacji mają na celu ograniczenie pozyskiwania, rozpowszechniania i zatrzymywania danych dotyczących obywateli i rezydentów Stanów Zjednoczonych oraz zawierają przepisy zapewniające istotną ochronę danych dotyczących również tych osób, które nie są obywatelami i rezydentami Stanów Zjednoczonych, jak opisano poniżej. Co więcej, zgodnie z powyższym, w dyrektywie politycznej Prezydenta nr 28 nakazano, aby Wspólnota Wywiadowcza zapewniła dodatkową ochronę danych osobowych osób niebędących obywatelami i rezydentami Stanów Zjednoczonych i ochrona ta ma zastosowanie do informacji zgromadzonych na mocy sekcji 702.

Gdy sąd zatwierdzi procedury ukierunkowywania oraz minimalizacji, gromadzenie danych zgodnie z sekcją 702 nie będzie polegało na hurtowym lub bezkrytycznym gromadzeniu danych, ale „na skupieniu się na określonych osobach, w przypadku których przeprowadzono zindywidualizowane rozpoznanie", jak twierdzi Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi ([9]). Gromadzenie danych prowadzone jest przy wykorzystaniu indywidualnych selektorów, takich jak adresy e-mail lub numery telefonów, które według pracowników amerykańskiego wywiadu, są prawdopodobnie wykorzystywane do przekazywania danych wywiadowczych, których rodzaj został uwzględniony

([1]) Tytuł 50 § 1881a.

([2]) Stany Zjednoczone mogą również uzyskać, zgodnie z innymi przepisami ustawy o kontroli wywiadu nakazy sądowe w sprawie tworzenia danych, w tym danych przekazywanych zgodnie z Tarczą Prywatności. Zob. tytuł 50 § 1801 i nast. U.S.C. Zgodnie z tytułem I i III ustawy o kontroli wywiadu, które zezwalają odpowiednio na obserwację elektroniczną oraz przeszukania, wymagany jest nakaz sądowy (poza nagłymi przypadkami); zawsze należy określić również prawdopodobną przyczynę podejrzeń, że dana osoba działa na korzyść innego kraju lub jest jego agentem. Tytuł IV ustawy o kontroli wywiadu zezwala na stosowanie urządzeń rejestrujących wybierane numery (ang. pen register) oraz urządzeń śledzących (ang. trap and trace) na mocy nakazu sądowego (poza nagłymi przypadkami) w autoryzowanych dochodzeniach służb wywiadowczych i dochodzeniach związanych z kontrwywiadem lub walką z terroryzmem. Tytuł V ustawy o kontroli wywiadu zezwala, na mocy nakazu sądowego (poza nagłymi przypadkami), na uzyskanie rejestrów handlowych istotnych dla autoryzowanych dochodzeń służb wywiadowczych oraz dochodzeń związanych z kontrwywiadem lub walką z terroryzmem. Jak omówiono poniżej, w amerykańskiej ustawie o wolności wyraźnie zakazuje się stosowania nakazów rejestrowania wybieranych numerów lub nakazów w sprawie uzyskania dokumentacji przedsiębiorstwa przewidzianych w ustawie o kontroli wywiadu dla celów hurtowego gromadzenia danych i nakłada się wymóg „konkretnych terminów umożliwiających selekcję", aby zapewnić wykorzystywanie środków w ukierunkowany sposób.

([3]) Przygotowane przez Radę Nadzoru nad Prywatnością i Wolnościami Obywatelskimi „Sprawozdanie z programu kontroli funkcjonującego zgodnie z art. 702 ustawy o kontroli wywiadu" (z 2 lipca 2014 r.) („sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi").

([4]) Zob. Zbiór Ustaw Prawa Publicznego, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

([5]) Zob. tytuł 50 § 1881a lit. a) i b) U.S.C.

([6]) Zob. tamże § 1801 lit. e).

([7]) Zob. sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi, s. 99.

([8]) Zob. tytuł 50 § 1881a lit. d) i e) U.S.C.

([9]) Zob. sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi, s. 111.

w certyfikacji złożonej w sądzie ([1]). Podstawa wyboru docelowych informacji musi zostać udokumentowana, a dokumentacja każdego selektora musi zostać następnie przejrzana przez Departament Sprawiedliwości ([2]). Rząd Stanów Zjednoczonych upublicznił informacje, z których wynika, że w 2014 r. około 90 000 osób fizycznych zostało objętych sekcją 702, co stanowi niewielki ułamek społeczności internetowej składającej się z ponad 3 mld użytkowników na całym świecie ([3]).

Informacje zgromadzone na podstawie sekcji 702 podlegają zatwierdzonym przez sąd procedurom minimalizacji, które zapewniają ochronę osób niebędących obywatelami i rezydentami Stanów Zjednoczonych, jak i osób będących obywatelami i rezydentami Stanów Zjednoczonych, które to procedury zostały upublicznione ([4]). Na przykład komunikaty obywateli i rezydentów Stanów Zjednoczonych lub osób niebędących obywatelami i rezydentami Stanów Zjednoczonych, zebrane na podstawie sekcji 702, przechowuje się w bazach danych o ścisłej kontroli dostępu. Komunikacja może być przeglądana jedynie przez pracowników służb wywiadowczych, którzy przeszli szkolenie w zakresie procedur minimalizacji ukierunkowanych na ochronę prywatności oraz którym wydano specjalną zgodę na dostęp na potrzeby wykonywania ich zatwierdzonych zadań ([5]). Wykorzystanie danych ogranicza się do identyfikacji danych wywiadowczych lub dowodów przestępstw ([6]). Zgodnie z dyrektywą polityczną Prezydenta nr 28 informacje te można upowszechniać jedynie do celów wywiadu zagranicznego lub egzekwowania prawa; nie ma znaczenia fakt, że jedna ze stron wiadomości nie jest ani obywatelem, ani rezydentem Stanów Zjednoczonych ([7]). Procedury minimalizacji oraz dyrektywa polityczna Prezydenta nr 28 określają również maksymalny okres zatrzymywania danych zgromadzonych na podstawie sekcji 702 ([8]).

Nadzór nad stosowaniem sekcji 702 jest kompleksowy i prowadzony przez wszystkie trzy gałęzie naszego rządu. Agencje wykonujące ustawę prowadzą wewnętrzny przegląd na wielu szczeblach, w tym na szczeblu niezależnych Inspektorów Generalnych, oraz kontrole dostępu do danych pod kątem technologii. Departament Sprawiedliwości i Urząd Dyrektora Krajowych Służb Wywiadowczych dokonują dokładnego przeglądu sekcji 702 oraz analizują jej stosowanie w celu sprawdzenia, czy jest zgodna z przepisami prawa; na agencjach spoczywa również niezależny obowiązek zgłaszania potencjalnych przypadków niezgodności. Przypadki te są badane, przy czym wszystkie przypadki dotyczące zgodności są zgłaszane Sądowi ds. Nadzoru nad Wywiadem Zagranicznym, prezesowi Rady Nadzoru nad Służbami Wywiadowczymi i Kongresowi, a następnie podejmowane są odpowiednie kroki. ([9]). Do tej pory nie odnotowano żadnych przypadków umyślnego usiłowania naruszenia przepisów lub ominięcia wymogów prawnych ([10]).

Sąd ds. Nadzoru nad Wywiadem Zagranicznym odgrywa istotną rolę w wykonywaniu sekcji 702. W sądzie zasiadają niezależni sędziwie federalni, ich kadencja trwa siedem lat, niemniej jednak jak wszyscy sędziowie federalni są zatrudnieni dożywotnio. Jak wspomniano powyżej sąd dokonuje przeglądu rocznych certyfikatów oraz procedur ukierunkowywania i minimalizacji pod względem zgodności z prawem. Ponadto, jak wspomniano powyżej, rząd ma obowiązek niezwłocznie powiadomić sąd o kwestiach zgodności ([11]), przy czym kilka opinii sądu zostało odtajnionych i upublicznionych, ukazując wyjątkowy stopień kontroli sądowej i niezależności, jaka przysługuje temu sądowi podczas badania tych przypadków.

Wymagające procedury sądowe zostały opisane przez poprzedniego prezesa sądu w piśmie skierowanym do Kongresu, które zostało podane do wiadomości publicznej ([12]). W wyniku amerykańskiej ustawy o wolności, opisanej poniżej, sądowi przysługuje wyraźne uprawnienie do wyznaczenia adwokata z zewnątrz jako niezależnego adwokata występującego w imieniu ochrony prywatności w przypadkach, które dotyczą nowych lub istotnych zagadnień prawnych ([13]). Stopień zaangażowania niezależnego sądownictwa krajowego w działania wywiadowcze ukierunkowane na osoby, które nie są ani obywatelami danego kraju ani nie znajdują się na jego terytorium, jest niezwykły, a nawet niespotykany oraz pomaga zapewnić gromadzenie danych na podstawie sekcji 702 w określonych granicach prawnych.

([1]) Tamże.

([2]) Tamże s. 8; tytuł 50 § 1881a lit. l); zob. także sprawozdanie Dyrektora ds. Wolności Obywatelskich i Prywatności Agencji Bezpieczeństwa Narodowego, „Wykonanie przepisów sekcji 702 ustawy o kontroli wywiadu przez Agencję Bezpieczeństwa Narodowego" (zwane dalej „sprawozdaniem Agencji Bezpieczeństwa Narodowego") s. 4, dokument dostępny pod adresem: http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) Sprawozdanie na temat przejrzystości Dyrektora Krajowych Służb Wywiadowczych z 2014 r. dostępne pod adresem: http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

([4]) Procedury minimalizacji dostępne pod adresem: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf („NSA Minimization Procedures"); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; i http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) Zob. sprawozdanie Agencji Bezpieczeństwa Narodowego, s. 4.

([6]) Zob. np. procedury minimalizacji Agencji Bezpieczeństwa Narodowego, s. 6.

([7]) Procedury Agencji Wywiadowczej określone w dyrektywie politycznej Prezydenta nr 28 dostępne pod adresem: http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) Zob. procedury minimalizacji Agencji Bezpieczeństwa Narodowego; sekcja 4 dyrektywy politycznej Prezydenta nr 28.

([9]) Zob. tytuł 50 § 1881 lit. l) U.S.C.; zob. także sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi, s. 66–76.

([10]) 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 s. 2–3, dokument dostępny pod adresem: http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf

([11]) Reguła nr 13 regulaminu Sądu ds. Nadzoru nad Wywiadem Zagranicznym; dokument dostępny pod adresem: http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf

([12]) Pismo od Pana Reggiego B. Waltona do Pana Patricka J. Leahy'ego z dnia 29 lipca 2013 r.; dokument dostępne pod adresem: http://fas.org/irp/news/2013/07/fisc-leahy.pdf

([13]) Zob. sekcja 401 amerykańskiej ustawy o wolności, Zbiór Ustaw Prawa Publicznego nr 114-23.

Kongres sprawuje nadzór poprzez ustawowe składanie sprawozdań Komisji ds. Wywiadu i Komisji Sprawiedliwości oraz częste briefingi i przesłuchania. Należą do nich półroczne sprawozdanie Prokuratora Generalnego dokumentujące stosowanie sekcji 702 i wszelkie przypadki niezgodności ([1]); odrębna ocena półroczna przeprowadzona przez Prokuratora Generalnego i Dyrektora Krajowych Służb Wywiadowczych dokumentująca zgodność z procedurami ukierunkowywania i minimalizacji, w tym zgodność z procedurami służącymi zapewnieniu, aby dane gromadzono dla ważnych celów wywiadowczych ([2]); oraz roczne sprawozdanie sporządzone przez szefów agencji wywiadowczych, które obejmuje certyfikację potwierdzającą, że dane gromadzone na podstawie sekcji 702 w dalszym ciągu zawierają dane wywiadowcze ([3]).

Krótko mówiąc, gromadzenie danych zgodnie z sekcją 702 jest dozwolone przez prawo; podlega wielu etapom przeglądu, kontroli sądowej i nadzorowi sądowemu; oraz, jak stwierdził Sąd ds. Nadzoru nad Wywiadem Zagranicznym w odtajnionej niedawno opinii, nie jest „prowadzone w sposób hurtowy lub bezkrytyczny", ale „poprzez […]decyzje wyraźnie skoncentrowane na konkretnych urządzeniach służących [komunikacji]" ([4]).

III. AMERYKAŃSKA USTAWA O WOLNOŚCI

Amerykańska ustawa o wolności, podpisana w czerwcu 2015 r. znacząco zmieniła akty stanowiące podstawę prawną uprawnień amerykańskich organów nadzoru i bezpieczeństwa narodowego oraz zwiększyła przejrzystość publiczną w zakresie korzystania z tych aktów oraz orzeczeń Sądu ds. Nadzoru nad Wywiadem Zagranicznym, jak określono poniżej. ([5]). Ustawa gwarantuje uprawnienia potrzebne personelowi organów wywiadowczych i organów do ochrony narodu, przy jednoczesnym zapewnieniu, aby prywatność osób fizycznych była właściwie chroniona podczas korzystania z takich uprawnień. Ustawa rozszerza ochronę prywatności i wolności obywatelskich oraz zwiększa przejrzystość.

W ustawie wprowadza się zakaz hurtowego gromadzenia wszelkich rejestrów, w tym zarówno dotyczących obywateli i rezydentów Stanów Zjednoczonych, jak i osób niebędących obywatelami i rezydentami Stanów Zjednoczonych, na podstawie różnych przepisów ustawy o kontroli wywiadu lub poprzez wykorzystanie wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego w formie ustawowo zatwierdzonych wezwań administracyjnych ([6]). Zakaz ten obejmuje w szczególności metadane telefoniczne dotyczące połączeń między osobami na terytorium Stanów Zjednoczonych oraz osobami poza terytorium Stanów Zjednoczonych, a także będzie obejmował gromadzenie informacji w ramach Tarczy Prywatności na podstawie aktów stanowiących podstawę prawną tych uprawnień. W ustawie tej nakłada się zobowiązanie, aby rząd opierał każdy wniosek o przekazanie danych na podstawie tych aktów na „konkretnym terminie umożliwiającym selekcję" – terminie, który pozwala zidentyfikować określoną osobę, konto, adres lub urządzenie osobiste w sposób, który maksymalnie ogranicza zakres poszukiwanych informacji ([7]). Przepis ten dodatkowo zapewnia, aby gromadzenie informacji dla celów wywiadowczych było właściwie skoncentrowane i ukierunkowane.

Na mocy ustawy znacząco zmodyfikowano postępowania prowadzone przed Sądem ds. Nadzoru nad Wywiadem Zagranicznym, w wyniku czego zwiększono przejrzystość i zapewniono dodatkowe gwarancje ochrony prywatności. Jak wspomniano powyżej, ustawa umożliwiła utworzenie stałego zespołu prawników, którzy otrzymali poświadczenie bezpieczeństwa, mających doświadczenie w zakresie ochrony prywatności i wolności obywatelskich, gromadzenia danych wywiadowczych, technologii komunikacji lub innych istotnych dziedzinach, którzy mogą zostać powołani do występowania przed sądem jako *amicus curiae* w sprawach, które wymagają znaczącej lub nowatorskiej interpretacji prawa. Wspomniani prawnicy są uprawnieni do przytaczania argumentów prawnych, które zwiększają ochronę prywatności i wolności obywatelskich osób fizycznych oraz będą mieli dostęp do wszelkich informacji, w tym informacji niejawnych, które sąd uzna za niezbędne do pełnienia przez nich obowiązków ([8]).

Ustawa opiera się również na niespotykanej dotąd przejrzystości działań wywiadowczych rządu Stanów Zjednoczonych, zobowiązując Dyrektora Krajowych Służb Wywiadowczych, w porozumieniu z Prokuratorem Głównym, do odtajnienia lub opublikowania jawnego podsumowania każdego orzeczenia, decyzji lub opinii wydanej przez Sąd ds. Nadzoru nad Wywiadem Zagranicznym lub Sąd Apelacyjny ds. Kontroli Wywiadu, które zawiera ważną konstrukcję prawną lub interpretację jakiegokolwiek przepisu prawa.

([1]) Zob. tytuł 50 § 1881f U.S.C.
([2]) Zob. tamże § 1881a lit. l) ppkt 1.
([3]) Zob. tamże § 1881a lit. l) ppkt 3. Niektóre z tych sprawozdań zostały utajnione.
([4]) Mem. opinia i zarządzenie, s. 26 (FISC 2014); dokument dostępny pod adresem: http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf
([5]) Amerykańska ustawa o wolności z 2015 r., Pub. L. nr 114–23, § 401, 129 Stat. 268.
([6]) Zob. tamże §§ 103, 201, 501. Wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego są zatwierdzone na mocy różnych ustaw i umożliwiają FBI uzyskanie informacji zawartych w sprawozdaniach kredytowych, dokumentacji finansowej i dokumentacji abonenta elektronicznego i dokumentacji dotyczącej transakcji od niektórych rodzajów przedsiębiorstw, wyłącznie w celu ochrony przed terroryzmem międzynarodowym lub tajnymi działaniami wywiadowczymi. Zob. tytuł 12 § 3414 U.S.C.; tytuł 15 §§ 1681u-1681v U.S.C.; Tytuł 18 § 2709 U.S.C. FBI korzysta zwykle z wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego w celu gromadzenia krytycznych informacji nieobejmujących treści na wczesnych etapach walki z terroryzmem i dochodzeń kontrwywiadu – takich jak informacje na temat tożsamości abonenta rachunku, który mógł komunikować się z przedstawicielami grupy terrorystycznej, np. ISIL. Odbiorcy wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego mają prawo zakwestionować je przed sądem. Zob. tytuł 18 § 3511 U.S.C.
([7]) Zob. tamże.
([8]) Zob. tamże, w § 401.

Ponadto ustawa przewiduje ujawnianie licznych informacji na temat gromadzenia danych na podstawie ustawy o kontroli wywiadu i wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego. Stany Zjednoczone muszą co roku ujawniać Kongresowi i społeczeństwu liczbę nakazów i certyfikatów wydawanych na podstawie ustawy o kontroli wywiadu, o które się ubiegano i które otrzymano; szacunki dotyczące liczby obywateli i rezydentów Stanów Zjednoczonych oraz osób niebędących obywatelami i rezydentami Stanów Zjednoczonych objętych obserwacją; oraz, wśród innych informacji, liczbę powołanych *amici curiae* ([1]). W ustawie nakłada się również na rząd obowiązek dodatkowego publicznego zgłaszania liczby wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego dotyczących obywateli i rezydentów Stanów Zjednoczonych oraz osób niebędących obywatelami i rezydentami Stanów Zjednoczonych ([2]).

Jeżeli chodzi o przejrzystość działalności przedsiębiorstw, w ustawie zapewniono przedsiębiorstwom szereg wariantów publicznego zgłaszania łącznej liczby nakazów i dyrektyw na mocy ustawy o kontroli wywiadu lub wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego, które otrzymują od rządu, oraz liczby kont klientów będących przedmiotem tych nakazów ([3]). Kilka przedsiębiorstw dokonało już takich ujawnień, wyjawiając ograniczoną liczbę klientów, których rejestry były przedmiotem dochodzenia.

Ze wspomnianych sprawozdań dotyczących przejrzystości działalności przedsiębiorstw wynika, że wnioski o udostępnienie amerykańskich danych wywiadowczych dotyczą tylko niewielkiej części danych. Na przykład z jednego z ostatnich sprawozdań z przejrzystości sporządzonego przez duże przedsiębiorstwo wynika, że otrzymało ono wnioski o przedstawienie informacji ze względów bezpieczeństwa narodowego (zgodnie z ustawą o kontroli wywiadu lub wezwaniami do przedstawienia informacji do celów bezpieczeństwa narodowego) dotyczące mniej niż 20 000 jego kont, w okresie gdy miało co najmniej 400 mln abonentów. Innymi słowy wszystkie wnioski w sprawie amerykańskiego bezpieczeństwa narodowego zgłoszone przez to przedsiębiorstwo dotyczyły mniej niż 0,005 % jego abonentów. Nawet jeżeli każdy z tych wniosków odnosił się do danych objętych programem „bezpieczna przystań", a tak nie jest, oczywiste jest, że wnioski są ukierunkowane i odpowiednie pod względem skali, oraz nie obejmują hurtowego i bezkrytycznego gromadzenia danych.

Ponadto, o ile już w ustawach, w których zatwierdzono wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego, ograniczono okoliczności, w jakich można zabronić odbiorcy takich wezwań ich ujawnienia, o tyle przedmiotowa ustawa stanowi dodatkowo, że takie wymogi dotyczące nieujawniania muszą być okresowo weryfikowane; zawiera wymóg powiadamiania odbiorców wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego, gdy fakty nie uzasadniają już wymogu nieujawniania; oraz ujednolica się w niej procedury zaskarżania wymogów nieujawniania ([4]).

Podsumowując, istotne zmiany wprowadzone amerykańską ustawą o wolności w zakresie uprawnień amerykańskich organów wywiadowczych stanowią wyraźny dowód na szeroko zakrojone wysiłki podejmowane przez Stany Zjednoczone w celu nadania priorytetu ochronie danych osobowych, prywatności i wolności obywatelskich oraz przejrzystości we wszystkich amerykańskich praktykach wywiadowczych.

IV. PRZEJRZYSTOŚĆ

Oprócz przejrzystości wprowadzonej amerykańską ustawą o wolności, amerykańska Wspólnota Wywiadowcza przekazuje społeczeństwu wiele dodatkowych informacji, dając dobry przykład w odniesieniu do przejrzystości prowadzonych przez nich działań wywiadowczych. Wspólnota Wywiadowcza opublikowała wiele swoich strategii politycznych, procedur, orzeczeń Sądu ds. Nadzoru nad Wywiadem Zagranicznym oraz inne odtajnione materiały, zapewniając wyjątkowo wysoki stopień przejrzystości. Ponadto Wspólnota Wywiadowcza znacząca zwiększyła ilość ujawnianych danych statystycznych na temat korzystania przez rząd z aktów stanowiących podstawę prawną do gromadzenia danych do celów bezpieczeństwa narodowego. W dniu 22 kwietnia 2015 r. Wspólnota Wywiadowcza opublikowała swoje drugie coroczne sprawozdanie przedstawiające dane statystyczne dotyczące częstotliwości korzystania z tych istotnych aktów przez rząd. Urząd Dyrektora Krajowych Służb Wywiadowczych także opublikował na swoich stronach internetowych oraz na stronie internetowej „IC On the Record" – zbiór konkretnych zasad dotyczących przejrzystości ([5]) – i plan realizacji, który przekłada te zasady na konkretne, wymierne inicjatywy ([6]). W październiku 2015 r. Dyrektor Krajowych Służb Wywiadowczych zarządził, aby każda agencja wywiadowcza wyznaczała urzędnika ds. przejrzystości danych wywiadowczych wśród swoich kierowników w celu zwiększenia przejrzystości i prowadzenia inicjatyw w zakresie przejrzystości ([7]). Urzędnik ds. przejrzystości będzie ściśle współpracował z każdym urzędnikiem ds. ochrony prywatności i wolności obywatelskich z agencji wywiadowczej w celu zapewnienia, aby przejrzystość, prywatność i wolności obywatelskie nadal pozostawały głównymi priorytetami.

([1]) Zob. tamże, w § 602.
([2]) Zob. tamże.
([3]) Zob. tamże, w § 603.
([4]) Zob. tamże §§ 502 lit.f) – 503.
([5]) Dostępny pod adresem: http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) Dokument dostępny pod adresem: http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) Zob. tamże.

Dla zilustrowania tych starań w ciągu kilku ostatnich lat główny urzędnik ds. ochrony prywatności i wolności obywatelskich Agencji Bezpieczeństwa Narodowego opublikował kilka jawnych sprawozdań, w tym sprawozdania na temat działań prowadzonych na podstawie sekcji 702, rozporządzenia wykonawczego nr 12333 i amerykańskiej ustawy o wolności ([1]). Ponadto Wspólnota Wywiadowcza ściśle współpracuje z Radą Nadzoru nad Prywatnością i Wolnościami Obywatelskimi, Kongresem i amerykańską społecznością adwokacką zajmującą się ochroną prywatności w celu zapewnienia większej przejrzystości działań amerykańskich służb wywiadowczych, o ile to możliwe i zgodne z ochroną wrażliwych źródeł i metod wywiadowczych. Jako całość działania amerykańskich służb wywiadowczych są przejrzyste jak działania prowadzone przez jakiekolwiek inne państwo na świecie a nawet bardziej przejrzyste oraz są na tyle przejrzyste na ile to możliwe, aby odpowiadać potrzebie zapewnienia ochrony wrażliwych źródeł i metod.

Podsumowując znaczną przejrzystość, jaką odznaczają się działania amerykańskich służb wywiadowczych, należy wspomnieć o poniższych działaniach.

— Wspólnota Wywiadowcza wydała i umieściła w internecie tysiące stron orzeczeń sądowych i procedury stosowane przez agencje, opisujące określone procedury i wymogi dotyczące naszych działań wywiadowczych. Opublikowaliśmy także sprawozdania dotyczące przestrzegania przez agencje wywiadowcze obowiązujących ograniczeń,

— urzędnicy wysokiego szczebla z agencji wywiadu regularnie wypowiadają się publicznie na temat ról i działań swoich organizacji, w tym opisują systemy zgodności i gwarancje, które regulują ich pracę,

— Wspólnota Wywiadowcza wydała szereg dodatkowych dokumentów dotyczących działań wywiadowczych zgodnie z naszą ustawą o dostępie do informacji publicznej,

— prezydent przyjął dyrektywę polityczną nr 28, publicznie określającą dodatkowe ograniczenia dotyczące naszych działań wywiadowczych, a Urząd Dyrektora Krajowych Służb Wywiadowczych opublikował dwa sprawozdania publiczne dotyczące wykonania tych ograniczeń,

— Wspólnota Wywiadowcza ma ustawowy obowiązek publikowania znaczących opinii prawnych wydanych przez Sąd ds. Nadzoru nad Wywiadem Zagranicznym lub podsumowań tych opinii,

— rząd jest zobowiązany do przedstawiania corocznych sprawozdań na temat zakresu wykorzystania określonych aktów stanowiących podstawę prawną do celów bezpieczeństwa narodowego; także przedsiębiorstwa są do tego upoważnione,

— Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi opublikowała kilka szczegółowych sprawozdań publicznych dotyczących działań wywiadowczych i nadal będzie to robić,

— Wspólnota Wywiadowcza przekazuje komisjom nadzorczym Kongresu obszerne informacje niejawne,

— Dyrektor Krajowych Służb Wywiadowczych opublikował zasady przejrzystości regulujące działania Wspólnoty Wywiadowczej.

Ta rozszerzona przejrzystość w dalszym ciągu będzie zwiększana. Wszelkie informacje podawane do wiadomości publicznej zostaną oczywiście udostępnione Departamentowi Handlu i Komisji Europejskiej. Roczny przegląd prowadzony przez Komisję Handlu i Komisję Europejską dotyczący wdrożenia Tarczy Prywatności będzie stanowił okazję dla Komisji Europejskiej do omówienia kwestii poruszonych w związku z upublicznieniem jakichkolwiek nowych informacji oraz wszelkich innych kwestii dotyczących Tarczy Prywatności i jej działania; zdajemy sobie sprawę, że Departament może, według własnego uznania, zaprosić przedstawicieli innych agencji, w tym Wspólnoty Wywiadowczej, do wzięcia udziału w tym przeglądzie. Należy oczywiście pamiętać o mechanizmie przewidzianym dla państw członkowskich UE w dyrektywie politycznej Prezydenta nr 28, który służy do przekazywania obaw związanych z nadzorem wyznaczonemu urzędnikowi Departamentu Stanu.

V. DOCHODZENIE ROSZCZEŃ

W prawie Stanów Zjednoczonych przewiduje się szereg środków prawnych dla osób fizycznych, które objęte są bezprawną obserwacją elektroniczną dla celów bezpieczeństwa narodowego. Na mocy ustawy o kontroli wywiadu prawo do dochodzenia odszkodowania w sądzie amerykańskim nie jest ograniczone wyłącznie do obywateli i rezydentów Stanów Zjednoczonych. Osobie fizycznej, która może wykazać legitymację procesową, przysługiwałyby środki ochrony prawnej umożliwiające zaskarżenie bezprawnej obserwacji elektronicznej na mocy ustawy o kontroli wywiadu. Na przykład na mocy ustawy o kontroli wywiadu osoby objęte bezprawną obserwacją elektroniczną mogą bezpośrednio dochodzić odszkodowania od amerykańskich urzędników państwowych, w tym odszkodowania sankcyjnego i kosztów zastępstwa procesowego. Zob. tytuł 50 § 1810 U.S.C. Osoby fizyczne, które mają legitymację

([1]) Dokument dostępny pod adresem: https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

procesową, mogą także wytoczyć powództwo cywilne o odszkodowanie, w tym koszty postępowania sądowego, przeciwko Stanom Zjednoczonym, w przypadku gdy informacje na ich temat uzyskane w ramach obserwacji elektronicznej na mocy ustawy o kontroli wywiadu zostały bezprawnie i umyślnie wykorzystane lub ujawnione. Zob. tytuł 18 § 2712 U.S.C. Jeżeli rząd zamierza wykorzystać lub ujawnić jakiekolwiek informacje na temat dowolnej osoby poszkodowanej otrzymane lub pozyskane za pomocą obserwacji elektronicznej na mocy ustawy o kontroli wywiadu przeciwko tej osobie w postępowaniu sądowym lub administracyjnym w Stanach Zjednoczonych, musi z wyprzedzeniem powiadomić o swoim zamiarze sąd i daną osobę, które mogą następnie podważyć zgodność nadzoru z prawem i wnieść o zaprzestanie rozpowszechniania informacji. Zob. tytuł 50 § 1806 U.S.C. Ponadto ustawa o kontroli wywiadu przewiduje również sankcje karne dla osób fizycznych, które umyślnie angażują się w bezprawną obserwację elektroniczną na mocy prawa lub które umyślnie korzystają z informacji uzyskanych w ramach bezprawnego dozoru lub ujawniają takie informacje. Zob. tytuł 50 § 1809 U.S.C.

Obywatele Unii mają inne możliwości wystąpienia na drogę sądową przeciwko amerykańskim urzędnikom państwowym za bezprawne wykorzystanie danych lub uzyskanie dostępu do tych danych, w tym przeciwko urzędnikom rządowym, którzy dopuszczają się naruszenia prawa w trakcie bezprawnego dostępu do informacji lub korzystania z informacji do rzekomych celów bezpieczeństwa narodowego. W ustawie o oszustwach i nadużyciach komputerowych ustanowiono zakaz umyślnego uzyskiwania nieuprawnionego dostępu (lub przekraczania granic uprawnionego dostępu) w celu pozyskania informacji z instytucji finansowej, systemu komputerowego rządu Stanów Zjednoczonych lub komputera, do których uzyskano dostęp za pośrednictwem internetu, a także zakaz formułowania gróźb uszkodzenia chronionych komputerów do celów związanych z wyłudzeniem lub popełnieniem oszustwa. Zob. tytuł 18 § 1030 U.S.C. Każda osoba, niezależnie od jej narodowości, która dozna szkody lub poniesie stratę w następstwie naruszenia przepisów tej ustawy, może wytoczyć powództwo przeciwko sprawcy naruszenia (w tym także urzędnikowi państwowemu) o odszkodowanie wyrównawcze oraz o orzeczenie zakazu lub innego słusznego środka zgodnie z sekcją 1030 lit. g), niezależnie od tego, czy w odniesieniu do sprawcy wszczęto postępowanie karne, pod warunkiem że naruszenie wypełnia znamiona przynajmniej jednego rodzaju czynu zabronionego opisanego w ustawie. Ustawa o ochronie danych w łączności elektronicznej reguluje kwestie związane z dostępem rządu do przechowywanych danych przekazywanych drogą elektroniczną oraz do informacji gromadzonych przez dostawców usług komunikacyjnych będących osobami trzecimi na temat abonentów. Zob. tytuł 18 § 2701–2712 U.S.C. Zgodnie z przepisami ustawy o ochronie danych w łączności elektronicznej osoba poszkodowana jest uprawniona do wytoczenia powództwa przeciwko urzędnikom państwowym w związku z umyślnym bezprawnym dostępem do przechowywanych danych. Ustawa ma zastosowanie do wszystkich osób niezależnie od ich obywatelstwa, a sąd może zasądzić wypłatę odszkodowania i pokrycie kosztów zastępstwa procesowego z tytułu naruszenia jej przepisów. Ustawa o prawie do poufności informacji finansowych ogranicza możliwość uzyskania dostępu do przechowywanych w rejestrach bankowych i brokerskich informacji dotyczących klientów indywidualnych przez organy rządu Stanów Zjednoczonych. Zob. tytuł 12 § 3401-3422 U.S.C. Zgodnie z przepisami ustawy o poufności informacji finansowych klient banku lub domu maklerskiego może pozwać rząd Stanów Zjednoczonych, dochodząc odszkodowania ustawowego, faktycznego lub odszkodowania mającego charakter kary z tytułu bezprawnego uzyskania dostępu do rejestrów zawierających dane tego klienta, przy czym w przypadku potwierdzenia, że takiego bezprawnego uzyskania dostępu dopuszczono się umyślnie, przeciwko stosownym urzędnikom rządowym automatycznie wszczęte zostanie postępowanie, które może zakończyć się wyciągnięciem konsekwencji dyscyplinarnych wobec sprawców naruszenia. Zob. tytuł 12 § 3417 U.S.C.

Zgodnie z przepisami ustawy o dostępie do informacji publicznej każda osoba jest uprawniona do uzyskania dostępu do aktualnej wersji prowadzonego przez agencję federalną rejestru zawierającego informacje na dowolny temat – istnieją jednak pewne wyjątki od tego prawa. Zob. tytuł 5 § 552 lit. b) U.S.C. Wśród tych wyjątków należy wymienić ograniczenia w dostępie do informacji niejawnych istotnych dla bezpieczeństwa narodowego, danych osobowych innych osób fizycznych oraz informacji dotyczących dochodzeń prowadzonych przez organy egzekwowania prawa – ograniczenia te są porównywalne z ograniczeniami nakładanymi przez organy krajowe zgodnie z krajowymi przepisami w zakresie dostępu do informacji. Ograniczenia te odnoszą się zarówno do Amerykanów, jak i osób innej narodowości. Sporne decyzje dotyczące udostępniania rejestrów będących przedmiotem wniosku zgodnie z ustawą o dostępie do informacji publicznej można zaskarżyć administracyjnie, a następnie w sądzie federalnym. Sąd jest zobowiązany na nowo ustalić, czy udostępnienie rejestrów zostały wstrzymane zasadnie, tytuł 5 § 552(a)(4)(B) U.S.C., oraz może nakazać rządowi zapewnienie dostępu do rejestrów. W niektórych sprawach sąd obalił stanowisko rządu, zgodnie z którym nie należało dopuścić do ujawnienia informacji z uwagi na ich niejawny charakter ([1]). Mimo że nie ma możliwości zasądzenia odszkodowania pieniężnego, sąd może zarządzić wypłatę honorariów pełnomocnikom procesowym.

VI. WNIOSEK

Stany Zjednoczone zgadzają się, że przy podejmowaniu przez nas działań w obszarze rozpoznania radioelektronicznego i prowadzeniu innego rodzaju działalności wywiadowczej należy wziąć pod uwagę fakt, że wszystkie osoby powinny być traktowane z godnością i szacunkiem, niezależnie od ich narodowości lub miejsca zamieszkania, oraz że wszystkie osoby mają uzasadniony interes w dążeniu do zapewnienia poszanowania ich prywatności przy przetwarzaniu dotyczących ich danych osobowych. Stany Zjednoczone podejmują działania w obszarze rozpoznania radioelektronicznego w celu realizacji swoich interesów w obszarze bezpieczeństwa narodowego i polityki zagranicznej oraz w celu

([1]) Zob. np. wyrok w sprawie New York Times przeciwko Departamentowi Sprawiedliwości, 756 F.3d 100 (2d Cir. 2014) i wyrok w sprawie Amerykańska Unia Wolności Obywatelskich przeciwko CIA, 710 F.3d 422 (D.C. Cir. 2014).

zapewnienia ochrony swoim obywatelom i obywatelom państw sojuszniczych i partnerskich. Krótko mówiąc, Wspólnota Wywiadowcza nie prowadzi żadnego rodzaju masowej inwigilacji jakichkolwiek podmiotów, uwzględniając zwykłych obywateli Unii. Gromadzenie informacji w ramach rozpoznania radioelektronicznego odbywa się wyłącznie po uzyskaniu odpowiedniego upoważnienia i zgodnie z ustanowionymi ograniczeniami, wyłącznie po rozważeniu możliwości skorzystania z innych źródeł informacji, w tym źródeł dyplomatycznych i publicznych, oraz w sposób uwzględniający odpowiednie i możliwe do zastosowania rozwiązania alternatywne. W przypadkach, w których jest to możliwe, w ramach działań w obszarze rozpoznania radioelektronicznego należy gromadzić wyłącznie informacje skoncentrowane na osobie namierzanej lub dotyczące określonych zagadnień związanych z wywiadem zagranicznym, każdorazowo stosując wyróżniki.

Polityka Stanów Zjednoczonych w tym obszarze została zatwierdzona w dyrektywie politycznej Prezydenta nr 28. W tym kontekście agencje wywiadowcze Stanów Zjednoczonych nie posiadają kompetencji prawnych, zasobów i zdolności technicznej pozwalających im przechwytywać informacje wymieniane na całym świecie ani woli przechwytywania takich informacji. Wspomniane agencje nie zajmują się czytaniem wiadomości e-mail wszystkich osób w Stanów Zjednoczonych ani – tym bardziej – wszystkich osób na świecie. Zgodnie z dyrektywą polityczną Prezydenta nr 28 Stany Zjednoczone kompleksową ochroną obejmuje się dane osobowe osób niebędących obywatelami i rezydentami Stanów Zjednoczonych, które są gromadzone w ramach działań w obszarze rozpoznania radioelektronicznego. W stopniu, w jakim jest to możliwe, biorąc pod uwagę kwestie związane z bezpieczeństwem narodowym, wspomniana ochrona obejmuje strategie i procedury służące ograniczaniu do minimum przypadków zatrzymywania danych oraz rozpowszechniania danych osobowych dotyczących osób niebędących obywatelami i rezydentami Stanów Zjednoczonych na poziomie porównywalnym z poziomem ochrony, jaki przysługuje obywatelom i rezydentom Stanów Zjednoczonych. Ponadto, jak wskazano powyżej, kompleksowy system nadzoru ustanowiony przez organ powołany zgodnie z sekcją 702 ustawy o kontroli wywiadu jest najlepszym tego rodzaju systemem na świecie. Ponadto istotne zmiany do ustawy o służbie wywiadowczej Stanów Zjednoczonych przewidziane w amerykańskiej ustawie o wolności oraz w inicjatywach Urzędu Dyrektora Krajowych Służb Wywiadowczych na rzecz promowania przejrzystości w ramach Wspólnoty Wywiadowczej w znacznym stopniu przyczynią się do ochrony prywatności i wolności obywatelskich wszystkich osób fizycznych niezależnie od ich przynależności państwowej.

Z poważaniem

Robert S. Litt

Dnia 21 czerwca 2016 r.

Pan Justin S. Antonipillai
Doradca
Departamentu Handlu Stanów Zjednoczonych
1401 Constitution Ave., NW
Waszyngton, DC 20230

Pan Ted Dean
Zastępca Wicesekretarza
Urząd ds. Handlu Międzynarodowego
1401 Constitution Ave., NW
Waszyngton, DC 20230

Szanowni Państwo!

W niniejszym piśmie pragnę przekazać Państwu dalsze informacje o tym, w jaki sposób Stany Zjednoczone hurtowo gromadzą dane w wyniku rozpoznania radioelektronicznego. Jak wyjaśniono w przypisie 5 w dyrektywie politycznej Prezydenta nr 28 (zwanej dalej „PPD-28"), „hurtowe" gromadzenie danych dotyczy pozyskiwania względnie dużego wolumenu informacji lub danych gromadzonych w wyniku rozpoznania radioelektronicznego w sytuacji, gdy Wspólnota Wywiadowcza nie może stosować identyfikatora związanego z namierzaną osobą (np. adresu e-mail lub numeru telefonu celu), by skupić gromadzenie danych na konkretnych celach. Nie oznacza to jednak, że tego rodzaju gromadzenie danych jest „masowe" lub „bezkrytyczne". PPD-28 nakłada także wymóg, zgodnie z którym „[d]ziałania w ramach rozpoznania radioelektronicznego muszą być dostosowane do danych potrzeb". W celu wypełnienia tego wymogu Wspólnota Wywiadowcza podejmuje działania mające zagwarantować, że nawet gdy nie możemy zastosować konkretnych identyfikatorów, by skupić gromadzenie danych na konkretnych celach, dane, które mają zostać zgromadzone, prawdopodobnie będą zawierać dane wywiadowcze, które będą odpowiadać wymogom sformułowanym przez decydentów w Stanach Zjednoczonych zgodnie z procesem, który objaśniłem w moim poprzednim piśmie; Wspólnota Wywiadowcza minimalizuje także ilość nieistotnych informacji, które są gromadzone.

Przykładowo, Wspólnota Wywiadowcza może zostać poproszona o pozyskanie danych w wyniku rozpoznania radioelektronicznego o działaniach grupy terrorystycznej aktywnej w regionie jednego z państw na Bliskim Wschodzie, która przypuszczalnie szykuje ataki przeciwko państwom w Europie Zachodniej, lecz Wspólnota Wywiadowcza może nie znać imion i nazwisk, numerów telefonów, adresów e-mail lub innych konkretnych identyfikatorów osób fizycznych związanych z taką grupą terrorystyczną. Możemy skoncentrować się na takiej grupie poprzez gromadzenie komunikatów przekazywanych z i do takiego regionu na potrzeby dalszego badania i analizy, by zidentyfikować takie komunikaty dotyczące danej grupy. W ten sposób Wspólnota Wywiadowcza dążyłaby do tego, by możliwie jak najbardziej zawęzić gromadzenie danych. Takie gromadzenie danych byłoby uznane za „hurtowe", gdyż wykorzystanie wyróżników nie jest wykonalne, lecz takie gromadzenie danych nie ma charakteru „masowego" ani „bezkrytycznego"; raczej jest skoncentrowane na celu w możliwie największy sposób.

Stąd nawet jeśli ukierunkowanie gromadzenia danych poprzez wykorzystanie konkretnych selektorów nie jest możliwe, Stany Zjednoczone nie gromadzą wszystkich komunikatów ze wszystkich narzędzi komunikacyjnych w każdym miejscu na świecie, lecz stosują filtry i inne narzędzia techniczne, by skoncentrować gromadzenie danych na takich narzędziach, które mogą zawierać komunikaty o wartości wywiadowczej. W ten sposób działania Stanów Zjednoczonych w zakresie rozpoznania radioelektronicznego dotyczą jedynie ułamka komunikacji odbywającej się za pośrednictwem internetu.

Ponadto, jak zauważyłem w moim poprzednim piśmie, ponieważ „hurtowe" gromadzenie danych wiąże się z większym ryzykiem gromadzenia nieistotnych komunikatów, PPD-28 ogranicza możliwości korzystania przez Wspólnotę Wywiadowczą z danych gromadzonych masowo w wyniku rozpoznania radioelektronicznego do sześciu konkretnych celów. PPD-28 i polityki agencji wdrażające PPD-28 również nakładają ograniczenia dotyczące zatrzymywania i rozpowszechniania danych osobowych pozyskanych w wyniku rozpoznania radioelektronicznego, niezależnie od tego, czy takie informacje zostały zgromadzone w hurtowy czy w ukierunkowany sposób, a także niezależnie od obywatelstwa danej osoby fizycznej.

„Hurtowe" gromadzenie danych przez Wspólnotę Wywiadowczą nie jest zatem „masowe" ani „bezkrytyczne", lecz wiąże się ze stosowaniem metod i narzędzi służących do filtrowania gromadzonych danych, tak by skoncentrować gromadzenie danych na materiale, który będzie odpowiadał wymogom wywiadu sformułowanym przez decydentów, jednocześnie minimalizując gromadzenie nieistotnych danych, i opiera się na rygorystycznych przepisach chroniących nieistotne informacje, które można pozyskać. Polityki i procedury opisane w niniejszym piśmie mają zastosowanie do

wszystkich danych gromadzonych hurtowo w wyniku rozpoznania radioelektronicznego, w tym wszelkich gromadzonych hurtowo komunikatów przekazywanych z i do Europy, bez potwierdzenia ani zaprzeczenia, że takie gromadzenie danych ma miejsce.

Zwrócili się Państwo również o dodatkowe informacje na temat Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi („PCLOB") i generalnych inspektorów, i ich organów. PCLOB jest niezależną agencją w strukturze władzy wykonawczej. Członków pięcioosobowej Rady reprezentującej obie partie mianuje Prezydent i zatwierdza Senat ([1]). Każdy członek Rady powoływany jest na sześcioletnią kadencję. Członkowie Rady i jej personel uzyskują stosowne poświadczenia bezpieczeństwa, tak by mogli wywiązywać się ze wszystkich swoich ustawowych zadań i obowiązków ([2]).

Zadaniem PCLOB jest zapewnienie, by działania rządu federalnego mające zapobiegać terroryzmowi w sposób wyważony uwzględniały potrzebę ochrony prywatności i wolności obywatelskich. Rada pełni dwie zasadnicze funkcje: nadzorczą i doradczą. PCLOB sama określa swój program i ustala, jakie działania związane z nadzorem lub doradztwem chce realizować.

Jeśli chodzi o funkcję *nadzorczą*, PCLOB dokonuje przeglądu i analizy działań, jakie władza wykonawcza podejmuje w celu ochrony swojego społeczeństwa przed terroryzmem, i zapewnia, by potrzeba takich działań w sposób wyważony uwzględniała potrzebę ochrony prywatności i wolności obywatelskich ([3]). W swoim ostatnim zakończonym przeglądzie nadzoru PCLOB skoncentrowała się na programach kontroli realizowanych zgodnie z sekcją 702 FISA ([4]). Obecnie prowadzi przegląd działań wywiadowczych realizowanych na podstawie dekretu 12333 ([5]).

Jeśli chodzi o funkcję *doradczą*, PCLOB zapewnia, by kwestie dotyczące wolności były odpowiednio uwzględniane w trakcie opracowywania i wdrażania przepisów, regulacji i polityk związanych z działaniami na rzecz ochrony społeczeństwa przed terroryzmem ([6]).

Aby zrealizować swoje zadania, Rada ma przyznane ustawowo prawo dostępu do wszystkich odnośnych rejestrów, sprawozdań, audytów, przeglądów, dokumentów, opracowań, zaleceń i wszelkich innych odnośnych materiałów agencji, uwzględniając informacje niejawne, zgodnie z prawem ([7]). Ponadto Rada może prowadzić przesłuchania, pobierać oświadczenia lub zeznania publiczne od wszystkich urzędników lub pracowników władzy wykonawczej ([8]). Rada może także wystąpić na piśmie, by prokurator generalny, w jej imieniu, wydał wezwania zmuszające strony poza strukturą władzy wykonawczej do przekazania istotnych informacji ([9]).

Wreszcie PCLOB musi przestrzegać ustawowych wymogów w zakresie przejrzystości publicznej. Oznacza to m.in. informowanie opinii publicznej o swoich działaniach poprzez organizowanie posiedzeń jawnych i publiczne udostępnianie swoich sprawozdań, w możliwie jak największym zakresie zgodnie z ochroną informacji niejawnych ([10]). Ponadto PCLOB jest zobowiązana zgłaszać przypadki, gdy agencja władzy wykonawczej odmówi stosowania się do jej rad.

Generalni inspektorzy we Wspólnocie Wywiadowczej prowadzą audyty, kontrole i przeglądy programów i działań we Wspólnocie Wywiadowczej, by rozpoznać i usunąć zagrożenia systemowe, luki w zabezpieczeniach i niedociągnięcia. Ponadto generalni inspektorzy prowadzą dochodzenia w sprawie skarg lub informacji o zarzutach łamania prawa, przepisów lub regulacji bądź o niewłaściwym zarządzaniu; rażącym marnotrawstwie funduszy; nadużywaniu władzy lub znaczącym i szczególnym zagrożeniu dla zdrowia i bezpieczeństwa publicznego w programach i działaniach Wspólnoty Wywiadowczej. Niezależność generalnych inspektorów stanowi bardzo ważny element obiektywizmu i integralności wszystkich sprawozdań, ustaleń i zaleceń, wydawanych przez inspektorów generalnych. Niektóre z najważniejszych

([1]) Tytuł 42 § 2000ee lit. a) i h) U.S.C.
([2]) Tytuł 42 § 2000ee lit. k) U.S.C.
([3]) Tytuł 42 § 2000ee lit. d) ppkt 2 U.S.C.
([4]) *Zob. pod kątem ogólnym* https://www.pclob.gov/library.html#oversightreports.
([5]) *Zob. pod kątem ogólnym* https://www.pclob.gov/events/2015/may13.html.
([6]) Tytuł 42 § 2000ee lit. d) ppkt 1 U.S.C; *Zob. także* PCLOB Advisory Function Policy and Procedure, Policy 2015-004 [Polityka i procedura dotycząca funkcji doradczej PCLOB, Polityka na lata 2015-004], *dostępne na stronie* https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
([7]) Tytuł 42 § 2000ee lit. g) ppkt 1 pkt A U.S.C.
([8]) Tytuł 42 § 2000ee lit. g) ppkt 1 pkt B U.S.C.
([9]) Tytuł 42 § 2000ee lit. g) ppkt 1 pkt D U.S.C.
([10]) Tytuł 42 § 2000ee lit. f) U.S.C.

elementów dla zachowania niezależności generalnych inspektorów obejmują proces ich mianowania i usuwania; odrębne organy operacyjne, budżetowe i kadrowe; oraz wymogi dotyczące podwójnej sprawozdawczości względem kierowników agencji władzy wykonawczej i Kongresu.

Kongres ustanowił niezależny urząd generalnego inspektora w każdej agencji władzy wykonawczej, w tym w każdej jednostce Wspólnoty Wywiadowczej ([1]). Wraz z uchwaleniem ustawy o zatwierdzeniu działań wywiadowczych na rok budżetowy 2015 prawie wszyscy generalni inspektorzy pełniący nadzór nad jednostką Wspólnoty Wywiadowczej są mianowani przez Prezydenta i zatwierdzani przez Senat, w tym Departament Sprawiedliwości USA, Centralną Agencję Wywiadowczą, Agencję Bezpieczeństwa Narodowego i Wspólnotę Wywiadowczą ([2]). Ponadto tacy generalni inspektorzy są bezstronnymi urzędnikami zatrudnianymi na stałe i mogą zostać usunięci z urzędu tylko przez Prezydenta. Wprawdzie Konstytucja Stanów Zjednoczonych wymaga, by Prezydent był uprawniony do usuwania generalnych inspektorów, z uprawnienia tego rzadko korzysta; Prezydent ma obowiązek przedstawić Kongresowi pisemne uzasadnienie w terminie 30 dni przed usunięciem generalnego inspektora ([3]). Taki proces mianowania generalnych inspektorów gwarantuje, że urzędnicy władzy wykonawczej nie wywierają nadmiernego wpływu w procesie wyboru, mianowania lub usuwania generalnych inspektorów.

Po drugie, generalni inspektorzy posiadają istotne uprawnienia ustawowe do prowadzenia audytów, dochodzeń i przeglądów programów i operacji władzy wykonawczej. Poza dochodzeniami i przeglądami z zakresu nadzoru wymaganymi w świetle prawa generalni inspektorzy dysponują dużą swobodą uznania co do sprawowania nadzoru w zakresie dokonywania przeglądów wybranych przez siebie programów i działań ([4]). W trakcie sprawowania takiego nadzoru prawo zapewnia, by generalni inspektorzy posiadali niezależne zasoby w celu wykonywania swoich obowiązków, w tym by byli upoważnieni do zatrudniania własnego personelu i osobnego dokumentowania swoich wniosków budżetowych składanych w Kongresie ([5]). Prawo zapewnia, by generalni inspektorzy mieli dostęp do informacji niezbędnych do pełnienia swoich obowiązków. Obejmuje to uprawnienie do bezpośredniego dostępu do wszystkich rejestrów i informacji agencji wyszczególniających programy i operacje agencji niezależnie od klasyfikacji; upoważnienie do wezwania do przekazania informacji i dokumentów; oraz upoważnienie do przyjmowania przysiąg ([6]). W ograniczonych przypadkach kierownik agencji władzy wykonawczej może zabronić wykonywania działań przez generalnego inspektora, jeżeli na przykład audyt lub dochodzenie prowadzone przez generalnego inspektora istotnie zakłóciłyby interesy bezpieczeństwa narodowego Stanów Zjednoczonych. Kierownik korzysta z takiego uprawnienia niezwykle rzadko i – podobnie jak Prezydent w przykładzie podanym powyżej – ma obowiązek przedstawić Kongresowi uzasadnienie zamiaru skorzystania z takiego uprawnienia w terminie 30 dni ([7]). Dyrektor Krajowych Służb Wywiadowczych nigdy nie skorzystał z takiego uprawnienia w odniesieniu do jakichkolwiek działań generalnych inspektorów.

Po trzecie, generalni inspektorzy mają za zadanie na bieżąco składać kierownikom agencji władzy wykonawczej i Kongresowi wyczerpujące sprawozdania na temat oszustw i innych poważnych problemów, nadużyć i niedociągnięć dotyczących programów i działań władzy wykonawczej ([8]). Podwójna sprawozdawczość wzmacnia niezależność generalnych inspektorów, gdyż zapewnia przejrzystość procesu nadzoru sprawowanego przez generalnych inspektorów i daje kierownikom agencji możliwość wykonania zaleceń generalnych inspektorów, zanim Kongres podejmie działania ustawodawcze. Dla przykładu, generalni inspektorzy są zobowiązani w świetle prawa do sporządzania półrocznych sprawozdań opisujących takie problemy i podjęte dotychczas działania naprawcze ([9]). Agencje władzy wykonawczej poważnie traktują ustalenia i zalecenia generalnych inspektorów, a ci ostatni mogą często zawrzeć fakt przyjęcia i wykonania przez agencje zaleceń inspektorów generalnych w takich i innych sprawozdaniach przedstawianych

([1]) Sekcje 2 i 4 ustawy o generalnym inspektorze z 1978 r. wraz z późniejszymi zmianami; sekcja 103H(b) i (e) ustawy o bezpieczeństwie narodowym z 1947 r. wraz z późniejszymi zmianami.; sekcja 17(a) ustawy o Centralnej Agencji Wywiadowczej (zwanej dalej „ustawą o CIA").

([2]) Zob. Zbiór Ustaw Prawa Publicznego, Pub. L. No. 113-293, 128 Stat. 3990, (19 grudnia 2014 r.). Tylko generalni inspektorzy w Agencji Wywiadu Wojskowego i Państwowej Agencji ds. Wywiadu Geoprzestrzennego nie są mianowani przez Prezydenta; jednakże generalni inspektorzy w Departamencie Obrony Stanów Zjednoczonych i Wspólnocie Wywiadowczej równolegle sprawują właściwość nad tymi agencjami.

([3]) Sekcja 3 ustawy o generalnym inspektorze z 1978 r. wraz z późniejszymi zmianami; sekcja 103H(c) ustawy o bezpieczeństwie narodowym; i sekcja 17(b) ustawy o CIA.

([4]) Zob. sekcje 4(a) i 6(a)(2) ustawy o generalnym inspektorze z 1947 r.; sekcja 103H(e) i (g)(2)(A) ustawy o bezpieczeństwie narodowym; sekcja 17(a) i (c) ustawy o CIA.

([5]) Sekcje 3(d), 6(a)(7) i 6(f) ustawy o generalnym inspektorze; sekcje 103H(d), (i), (j) i (m) ustawy o bezpieczeństwie narodowym; sekcje 17 (e)(7) i (f) ustawy o CIA.

([6]) Sekcja 6(a)(1), (3), (4), (5) i (6) ustawy o generalnym inspektorze; sekcje 103H(g)(2) ustawy o bezpieczeństwie narodowym; sekcja 17(e) (1), (2), (4) i (5) ustawy o CIA.

([7]) Zob. np. sekcje 8(b) i 8E(a) ustawy o generalnym inspektorze; sekcja 103H(f) ustawy o bezpieczeństwie narodowym; sekcja 17(b) ustawy o CIA.

([8]) Sekcja 4(e)(5) ustawy o CIA; sekcja 103H(a)(b)(3) i (4) ustawy o bezpieczeństwie narodowym; sekcja 17(a)(2) i (4) ustawy o CIA.

([9]) Sekcja 2(3), 4(a) i 5 ustawy o generalnym inspektorze; sekcja 103H(k) ustawy o bezpieczeństwie narodowym; sekcja 17(d) ustawy o CIA. Generalny inspektor w Departamencie Sprawiedliwości USA udostępnia swoje sprawozdania podawane do wiadomości publicznej na stronie http://oig.justice.gov/reports/all.htm. Podobnie generalny inspektor dla Wspólnoty Wywiadowczej udostępnia swoje półroczne sprawozdania pod adresem: https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

Kongresowi, a w niektórych przypadkach podawanych do wiadomości publicznej ([1]). Poza podwójną sprawozdawczością generalni inspektorzy odpowiadają również za kierowanie osób we władzy wykonawczej zgłaszających przypadki naruszenia (ang. *whistleblowers*) do stosownych komisji nadzorczych Kongresu, by ujawniły rzekome oszustwa, przypadki marnotrawstwa lub nadużyć w programach i działaniach władzy wykonawczej. Tożsamość takich osób jest chroniona przed ujawnieniem władzy wykonawczej, która chroni osoby zgłaszające przypadki naruszenia przed ewentualnymi zakazanymi decyzjami personalnymi lub postępowaniami sprawdzającymi, podejmowanymi w odwecie za dokonanie zgłoszenia do generalnego inspektora ([2]). Ponieważ osoby zgłaszające przypadki naruszenia są często źródłem informacji w dochodzeniach prowadzonych przez generalnych inspektorów, możliwość zgłaszania ich obaw Kongresowi bez wywierania przez władzę wykonawczą wpływu zwiększa skuteczność nadzoru sprawowanego przez generalnych inspektorów. Z uwagi na taką niezależność generalni inspektorzy mogą promować gospodarność, wydajność i odpowiedzialność w agencjach władzy wykonawczej, zachowując obiektywizm i integralność.

Wreszcie Kongres ustanowił Radę generalnych inspektorów ds. integralności i wydajności. Rada zajmuje się m.in. opracowywaniem standardów generalnych inspektorów do celów audytów, dochodzeń i przeglądów; promuje szkolenia; i jest upoważniona do prowadzenia dochodzeń w sprawie zarzutów dotyczących wykroczeń popełnionych przez generalnych inspektorów, co służy temu, by dokładnie przyglądać się generalnym inspektorom, którym powierzono zadanie obserwowania wszystkich pozostałych ([3]).

Mam nadzieję, że udzielone przeze mnie informacje okażą się pomocne.

Z poważaniem
Robert S. Litt
Główny Doradca

([1]) Sekcja 2(3), 4(a) i 5 ustawy o generalnym inspektorze; sekcja 103H(k) ustawy o bezpieczeństwie narodowym; sekcja 17(d) ustawy o CIA. Generalny inspektor w Departamencie Sprawiedliwości USA udostępnia swoje sprawozdania podawane do wiadomości publicznej na stronie http://oig.justice.gov/reports/all.htm. Podobnie generalny inspektor dla Wspólnoty Wywiadowczej udostępnia swoje półroczne sprawozdania pod adresem: https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) Sekcja 7 ustawy o generalnym inspektorze; sekcja 103H(g)(3) ustawy o bezpieczeństwie narodowym; sekcja 17(e)(3) ustawy o CIA.

([3]) Sekcja 11 ustawy o generalnym inspektorze.

ZAŁĄCZNIK VII

Pismo zastępcy asystenta prokuratora generalnego i doradcy do spraw międzynarodowych Bruce'a Swartza, Departament Sprawiedliwości Stanów Zjednoczonych

Dnia 19 lutego 2016 r.

Justin S. Antonipillai
Doradca
Departamentu Handlu Stanów Zjednoczonych
1401 Constitution Ave., NW
Waszyngton, DC 20230

Ted Dean
Zastępca Wicesekretarza
Urząd ds. Handlu Międzynarodowego
1401 Constitution Ave., NW
Waszyngton, DC 20230

Szanowni Państwo!

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 ze ściganiem 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]). Omawiane pisma sądowe nie mają dyskryminacyjnego charakteru, ponieważ służą do pozyskiwania informacji od korporacji w Stanach Zjednoczonych, w tym od spółek, które dokonały samocertyfikacji w ramach Tarczy Prywatności UE-USA, niezależnie od narodowości 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 Zjednoczonym, 389 U.S. 347, 357 (1967). Jeżeli obowiązek uzyskania nakazu nie ma zastosowania w danym przypadku, 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.

Uprawnienia organów egzekwowania prawa w sprawach karnych:

Prokuratorzy federalni, którzy są urzędnikami Departamentu Sprawiedliwości, oraz federalni agenci śledczy, w tym agenci Federalnego Biura Śledczego (FBI), agencji egzekwowania prawa w ramach Departamentu Sprawiedliwości, mają

([1]) W niniejszym przeglądzie nie opisano narzędzi dochodzeniowych w obszarze bezpieczeństwa narodowego wykorzystywanych przez organy egzekwowania prawa w dochodzeniach dotyczących terroryzmu lub dochodzeniach dotyczących 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 – zob. tytuł 12 § 3414 U.S.C.; tytuł 15 § 1681u U.S.C.; tytuł 15 § 1681v U.S.C.; tytuł 18 § 2709 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, zob. tytuł 50 § 1801 i nast. U.S.C.

([2]) W niniejszym piśmie omówiono federalne organy egzekwowania prawa i organy regulacyjne; w przypadkach naruszenia prawa stanowego dochodzenie prowadzą stany, 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.

prawo nakazać osobom prawnym w Stanach Zjednoczonych przedstawienie dokumentów lub 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 połączenia przychodzące 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. 17. 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:: akty stanowiące podstawę prawną wezwań administracyjnych 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 przedsiębiorstwa telekomunikacyjne pełniące funkcję dostawców usług internetowych 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 internetowych innych niż dane określone w prawie konstytucyjnym. W ustawie o przechowywanych danych przekazywanych za pomocą łączności elektronicznej 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.

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 § 2510-2522 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 również możliwość pociągnięcia odpowiednich osób do odpowiedzialności cywilnej i karnej z tytułu naruszenia przepisów dotyczących podsłuchów.

Nakaz przeszukania – zasada 41: 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. Zob. czwarta poprawka do konstytucji Stanów Zjednoczonych (omówiona bardziej szczegółowo powyżej), zasada 41 federalnego kodeksu postępowania karnego. Podmiot, w odniesieniu do którego wydano nakaz przeszukania, może wystąpić o jego uchylenie z uwagi na fakt, że ma on zbyt szeroki zakres, jest nadmiernie uciążliwy lub został uzyskany w nieprawidłowy sposób, a strony poszkodowane posiadające legitymację procesową mogą wystąpić o wyłączenie wszelkich dowodów uzyskanych w rezultacie bezprawnego przeszukania z postępowania. Zob. wyrok w sprawie Mapp przeciwko Ohio, 367 U.S. 643 (1961).

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". Zob. 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(DIOG); 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 dla prokuratorów Stanów Zjednoczonych** (USAM), który jest również dostępny pod adresem http://www.justice.gov/usam/united-states-attorneys-manual.

Organy administracji cywilnej lub regulacyjne (interes publiczny):

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 cywilnego. 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 § 3401–3422 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 administracyjnym 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.

Z poważaniem

Bruce C. Swartz

Zastępca asystenta prokuratora generalnego i doradca
do spraw międzynarodowych