KOMISJA
EUROPEJSKA

Bruksela, dnia 29.2.2016 r.
COM(2016) 117 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Transatlantyckie przepływy danych: odbudowa zaufania dzięki ustanowieniu silniejszych gwarancji

1. Wprowadzenie: Rola wymiany danych osobowych w stosunkach między UE a Stanami Zjednoczonymi

Trwałe partnerstwo transatlantyckie między Unią Europejską a Stanami Zjednoczonymi jest obecnie równie ważne, jak w przeszłości. Unia Europejska i Stany Zjednoczone wyznają wspólne wartości, dążą do osiągnięcia tych samych celów politycznych i gospodarczych oraz prowadzą ścisłą współpracę na rzecz zwalczania wspólnych zagrożeń dla naszego bezpieczeństwa. O sile relacji między UE a Stanami Zjednoczonymi świadczy zakres prowadzonej wymiany handlowej i ścisła współpraca w sprawach o zasięgu globalnym.

Transfer i wymiana danych osobowych stanowią zasadniczy element leżący u podstaw silnych związków między Unią Europejską (UE) a Stanami Zjednoczonymi (USA) w obszarze handlu i egzekwowania prawa. Prowadzenie wymiany tego rodzaju danych wymaga zapewnienia wysokiego poziomu ochrony danych oraz ustanowienia odpowiednich gwarancji.

W czerwcu 2013 r. pojawiły się doniesienia o szeroko zakrojonych programach gromadzenia danych przez amerykańskie służby wywiadowcze, które wzbudziły poważne obawy zarówno na szczeblu UE, jak i na szczeblu państw członkowskich dotyczące wpływu tego rodzaju przetwarzania danych osobowych na szeroką skalę przez amerykańskie organy publiczne i przez przedsiębiorstwa prywatne w Stanach Zjednoczonych na prawa podstawowe Europejczyków.

W odpowiedzi na te doniesienia w dniu 27 listopada 2013 r. Komisja wydała komunikat w sprawie odbudowy zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi[1], w którym przedstawiła plan działania na rzecz przywrócenia zaufania do przekazywania danych z korzyścią dla rozwoju gospodarki cyfrowej, ochrony praw Europejczyków oraz wzmocnienia stosunków transatlantyckich. W komunikacie przedstawiono następujące podstawowe działania przyczyniające się do osiągnięcia tego celu:

(i) przyjęcie pakietu dotyczącego reformy ochrony danych zaproponowanego przez Komisję w 2012 r.[2];

[1] Komunikat Komisji do Parlamentu Europejskiego i Rady – Odbudowa zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi, COM(2013) 846 final z 27.11.2013 (zwany dalej „komunikatem z 2013 r." lub „komunikatem"), dostępny pod adresem: http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf

[2] Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych, COM(2012) 10 final z 25.1.2012, oraz wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), COM(2012) 11 final z 25.1.2012, dostępne pod adresem: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

(ii) zwiększenie poziomu bezpieczeństwa zapewnianego dzięki zasadom bezpiecznego transferu danych osobowych zgodnie z 13 zaleceniami przedstawionymi w komunikacie w sprawie zasad bezpiecznego transferu danych osobowych[3]; oraz

(iii) wzmocnienie gwarancji ochrony danych w ramach współpracy w zakresie egzekwowania prawa, w szczególności przez zakończenie negocjacji w sprawie umowy ramowej między UE a Stanami Zjednoczonymi. Jednym z celów tej umowy było również skłonienie Stanów Zjednoczonych do podjęcia zobowiązań w zakresie możliwych do wyegzekwowania na drodze prawnej praw osób fizycznych, w tym ścieżek dochodzenia odszkodowania na drodze sądowej, w szczególności poprzez wdrożenie amerykańskiej ustawy o sądowych środkach odwoławczych, w której rozszerzono na obywateli Unii niektóre prawa wynikające z amerykańskiej ustawy o prywatności z 1974 r., wcześniej przysługujące jedynie obywatelom i stałym rezydentom USA.

Cele te zostały potwierdzone w wytycznych politycznych[4] Komisji Junckera: „Ochrona danych osobowych to jedno z praw podstawowych, mające szczególne znaczenie w erze cyfrowej. Poza szybkim sfinalizowaniem prac legislacyjnych nad wspólnymi dla całej Unii Europejskiej zasadami ochrony danych, musimy także bronić tego prawa w naszych stosunkach zewnętrznych. W świetle niedawnych doniesień o prowadzonym na masową skalę nadzorze, nasi bliscy partnerzy, np. Stany Zjednoczone, muszą przekonać nas, że obecne ustalenia dotyczące bezpiecznego transferu danych są rzeczywiście pewne, jeśli chcą ich kontynuacji. USA muszą także zagwarantować, by wszyscy obywatele UE mogli korzystać z przysługujących im praw do ochrony danych także i w sprawach toczących się przed amerykańskimi sądami, niezależnie od tego, czy zamieszkują na terytorium Stanów Zjednoczonych. Jest to niezbędne dla odbudowy zaufania w relacjach transatlantyckich”.

Od tego czasu Komisja podejmuje działania na rzecz osiągnięcia tych celów. Komisja przyspieszyła negocjacje dotyczące umowy ramowej, którą strony parafowały w dniu 8 września 2015 r. Zwiększono tempo dyskusji międzyinstytucjonalnych w sprawie pakietu dotyczącego reformy ochrony danych, co doprowadziło do zawarcia porozumienia politycznego między Radą a Parlamentem Europejskim w dniu 15 grudnia 2015 r. Jeżeli chodzi o transatlantyckie transfery danych w obszarze handlu, w styczniu 2014 r. Komisja rozpoczęła rozmowy ze Stanami Zjednoczonymi w sprawie wzmocnienia zasad bezpiecznego transferu danych osobowych. Unieważnienie przez Trybunał Sprawiedliwości decyzji w sprawie zasad bezpiecznego transferu danych osobowych w orzeczeniu z dnia 6 października 2015 r. w sprawie Schrems[5] potwierdziło konieczność zaktualizowania istniejących ram oraz przedstawienia dalszych wytycznych w sprawie warunków, jakie ramy te powinny spełniać.

[3] 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 27.11.2013, s. 18–19 (zwany dalej „komunikatem w sprawie zasad bezpiecznego transferu danych osobowych”), dostępny pod adresem: http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

[4] Nowy początek dla Europy: Mój program na rzecz zatrudnienia, wzrostu, sprawiedliwości oraz zmian demokratycznych – Wytyczne polityczne na następną kadencję Komisji Europejskiej.

[5] Wyrok z dnia 6 października 2015 r. w sprawie C-362/14 Maximillian Schrems przeciwko Data Protection Commissioner, EU:C:2015:650.

Po wydaniu orzeczenia Komisja opublikowała w dniu 6 listopada 2015 r. wytyczne dla przedsiębiorstw, w których przedstawiła alternatywne instrumenty umożliwiające dalsze przekazywanie danych osobowych do Stanów Zjednoczonych[6]. W dniu 2 lutego 2016 r. zawarto porozumienie polityczne w sprawie nowych ram dotyczących transatlantyckich przepływów danych, tzw. zasad ochrony prywatności UE–USA[7], które ma zastąpić wcześniej obowiązujące porozumienie w tym zakresie.

Wspomniane osiągnięcia korzystnie wpłyną na stosunki transatlantyckie i powinny przyczynić się do odbudowy zaufania Europejczyków do gospodarki cyfrowej, wzmacniając jednocześnie przysługujące im prawa podstawowe. Zapewnią one również UE i jej państwom członkowskim solidniejsze ramy prawne w zakresie ochrony danych, które doprowadzą do większej integracji na rynku wewnętrznym, w szczególności na jednolitym rynku cyfrowym, a także umożliwią UE zwiększenie wysiłków na rzecz propagowania i rozwijania międzynarodowych standardów w zakresie ochrony prywatności i danych osobowych.

Równolegle przystąpiono również do realizacji ważnych inicjatyw, które doprowadziły do wprowadzenia istotnych zmian w porządku prawnym USA. W dniu 17 stycznia 2014 r. prezydent Obama ogłosił[8] reformę amerykańskich przepisów w zakresie rozpoznania radioelektronicznego, której założenia przedstawiono następnie w rozporządzeniu prezydenckim nr 28 (PPD-28)[9]. Co istotne, we wspomnianych reformach przewidziano rozszerzenie określonych środków ochrony prywatności również na osoby niebędące obywatelami amerykańskimi, a także przeorientowano proces gromadzenia danych, odchodząc od masowego gromadzenia danych na rzecz podejścia zorientowanego przede wszystkim na ukierunkowane gromadzenie danych i ukierunkowany dostęp do danych. Komisja z zadowoleniem przyjęła te zmiany i uznała je za krok we właściwym kierunku[10]. Wspomniana reforma dostarczyła również istotnych informacji na potrzeby prowadzonych ze Stanami Zjednoczonymi rozmów dotyczących zasad ochrony prywatności UE–USA. Od tego czasu wprowadzono również kolejne zmiany. Na przykład w czerwcu 2015 r. w Stanach Zjednoczonych przyjęto ustawę o wolności[11], wprowadzającą zmiany w niektórych amerykańskich programach inwigilacji, wzmacniającą nadzór sądowy nad tymi programami oraz zwiększającą poziom przejrzystości publicznej w zakresie ich wykorzystania. Ponadto w dniu 10 lutego 2016 r. Kongres Stanów Zjednoczonych przyjął ustawę o sądowych środkach

[6] Zob. komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie przekazywania danych osobowych z UE do Stanów Zjednoczonych na mocy dyrektywy 95/46/WE w następstwie wyroku Trybunału Sprawiedliwości w sprawie C-362/14 (Schrems), COM(2015) 566 final z 6.11.2015. Zob. również stanowisko Grupy Roboczej Art. 29 w sprawie skutków wyroku w sprawie Schrems z dnia 3 lutego 2016 r., dostępne pod adresem: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf

[7] Zob. http://europa.eu/rapid/press-release_IP-16-216_pl.htm

[8] https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

[9] https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

[10] http://europa.eu/rapid/press-release_MEMO-14-30_en.htm

[11] Amerykańska ustawa o wolności z 2015 r., Pub. L. nr 114–23, § 401, 129 Stat. 268.

odwoławczych. Ustawa ta została podpisana przez prezydenta Obamę w dniu 24 lutego 2016 r.[12].

Wspomniane powyżej działania stanowią tło dla zawartej w niniejszym komunikacie oceny postępów w osiągnięciu celów wyznaczonych w komunikacie z 2013 r. W komunikacie przedstawione zostaną również obszary, które w dalszym ciągu wymagają podjęcia dodatkowych działań, aby umocnić i w pełni przywrócić zaufanie do transatlantyckich przepływów danych.

2. Reforma systemu ochrony danych w UE

2.1. Kontekst

W celu wykorzystania możliwości stwarzanych przez cyfrowy świat, w którym występuje coraz więcej wzajemnych powiązań, oraz stawienia czoła wyzwaniom związanym z tym światem Komisja Europejska przedstawiła w styczniu 2012 r. pakiet dotyczący reformy ochrony danych („reforma"). Dzięki wzmocnieniu wewnętrznych przepisów unijnych i zapewnieniu osobom fizycznym większej kontroli nad ich danymi osobowymi reforma ma przyczynić się do zwiększenia poziomu zaufania do gospodarki cyfrowej, niezależnie od tego, czy do dane osobowe są przetwarzane w jednym państwie członkowskim, w UE czy w państwach trzecich, np. w Stanach Zjednoczonych.

Pakiet dotyczący reformy obejmuje dwa instrumenty prawne: ogólne rozporządzenie o ochronie danych[13] („rozporządzenie") ustanawiające wspólne unijne ramy w zakresie ochrony danych oraz dyrektywę o ochronie danych w obszarze współpracy policyjnej i sądowej („dyrektywa w sprawie policji")[14]. Przedstawiając wniosek w sprawie rozporządzenia, którego przepisy będą bezpośrednio stosowane w państwach członkowskich, Komisja dąży do stworzenia jednego zbioru norm w zakresie ochrony danych wspólnego dla wszystkich tych państw, a tym samym do wyeliminowania różnic w poziomie ochrony między państwami członkowskimi. Również dyrektywa w sprawie policji będzie stanowiła pierwszy wspólny zbiór przepisów w tym zakresie na szczeblu UE, który zarazem będzie uwzględniał specyfikę poszczególnych państw członkowskich, jeżeli chodzi o tradycje w obszarze sądownictwa i egzekwowania prawa.

W dniu 15 grudnia 2015 r. Parlament Europejski i Rada zawarły porozumienie polityczne w sprawie pakietu dotyczącego reformy, realizując tym samym jedno z podstawowych działań przewidzianych w komunikacie z 2013 r.

2.2. Co się zmieniło?

W rozporządzeniu zaktualizowano, zmodernizowano, a w niektórych przypadkach również wzmocniono zasady ochrony danych ustanowione w dyrektywie o ochronie danych z 1995

[12] H.R. 1428 – ustawa o sądowych środkach odwoławczych z 2015 r. Ustawa ta wejdzie w życie po upływie 90 dni od dnia jej przyjęcia.
[13] COM(2012) 11 final z 25.1.2012: zob. przypis 2.
[14] COM(2012) 10 final z 25.1.2012: zob. przypis 2.

r.[15] w celu zapewnienia poszanowania prawa do prywatności. Celem rozporządzenia jest wzmocnienie praw osób fizycznych, pogłębienie rynku wewnętrznego UE, zapewnienie lepszego egzekwowania przepisów, usprawnienie międzynarodowego przekazywania danych osobowych oraz ustanowienie globalnych norm w zakresie ochrony danych. Z założenia przepisy te mają zapewnić ochronę danych osobowych osób fizycznych z UE – niezależnie od tego, dokąd takie dane są przekazywane ani gdzie są przetwarzane lub przechowywane, nawet poza UE, co może się często zdarzać w cyfrowym świecie. Warto w tym miejscu zwrócić szczególną uwagę na szereg kwestii związanych z przedmiotową reformą.

Po pierwsze, **terytorialny zakres stosowania**: w rozporządzeniu wyraźnie zaznaczono, że jego przepisy mają zastosowanie również do przedsiębiorstw mających siedzibę w państwie trzecim, jeżeli oferują one towary i usługi lub monitorują zachowanie osób fizycznych w UE. Przedsiębiorstwa mające siedzibę poza UE będą musiały stosować te same przepisy co przedsiębiorstwa mające siedzibę w UE. Zagwarantuje to kompleksową ochronę praw osób fizycznych z UE. Zapewni również równe warunki działania przedsiębiorstwom z UE i przedsiębiorstwom z państw trzecich oraz pozwoli uniknąć nierównowagi konkurencyjnej między przedsiębiorstwami z UE a przedsiębiorstwami z państw trzecich prowadzącymi działalność w UE lub podejmującymi działania ukierunkowane na konsumentów w UE.

Po drugie, **skuteczniejsze egzekwowanie** przepisów w zakresie ochrony danych: dzięki zharmonizowaniu uprawnień krajowych nadzorczych organów ochrony danych w rozporządzeniu ustanowiono skuteczny system sankcji. Organy te będą upoważnione do nakładania grzywien w wysokości do 20 mln EUR lub do 4 % łącznych rocznych obrotów uzyskiwanych przez dane przedsiębiorstwo na całym świecie. Tego rodzaju uprawnienie do nakładania odstraszających sankcji z tytułu niezapewnienia zgodności z przepisami w zakresie ochrony danych w połączeniu z poszerzeniem terytorialnego zakresu stosowania, o którym mowa powyżej, przyczyni się do zagwarantowania, że przedsiębiorstwa prowadzące działalność w UE będą miały silną motywację do przestrzegania prawa Unii. W nowych przepisach ustanowiono również przejrzystszy i bardziej rygorystyczny system dla administratorów i podmiotów przetwarzających.

Po trzecie, **harmonizacja przepisów w zakresie współpracy organów ścigania**: w dyrektywie w sprawie policji ustanowione zostaną ogólne zasady i przepisy w zakresie ochrony danych obowiązujące w kontekście przetwarzania danych osobowych przez policję i organy wymiaru sprawiedliwości w państwach członkowskich do celów związanych z egzekwowaniem prawa karnego. Działania w tym obszarze obejmują przyjęcie zharmonizowanych przepisów w zakresie międzynarodowego przekazywania danych osobowych w kontekście współpracy między organami ścigania w sprawach karnych[16]. Nowa

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

[16] W odróżnieniu od decyzji ramowej Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, która odnosi się wyłącznie do kwestii związanych z transgraniczną wymianą danych między właściwymi organami państw członkowskich, zastosowanie takich przepisów na mocy dyrektywy w sprawie policji nie będzie już

dyrektywa zwiększy poziom ochrony osób fizycznych, zapewniając jednocześnie odpowiednią ochronę danych ofiar, świadków i podejrzanych o popełnienie przestępstwa w ramach dochodzeń lub czynności organów ścigania. Niezależne krajowe organy ochrony danych zapewniają właściwy nadzór nad danymi osobowymi, przy czym osobom fizycznym należy zapewnić możliwość skorzystania ze skutecznych środków zaskarżenia. Jednocześnie większy poziom harmonizacji obowiązujących przepisów zapewni policji i organom wymiaru sprawiedliwości możliwość prowadzenia skuteczniejszej współpracy na rzecz walki z przestępczością i terroryzmem, zarówno między poszczególnymi państwami członkowskimi, jak i między państwami członkowskimi a ich międzynarodowymi partnerami. Jest to zasadniczy element Europejskiej agendy bezpieczeństwa[17].

Po czwarte, **wzmocnienie przepisów służących zwiększeniu bezpieczeństwa międzynarodowego przekazywania danych**: zarówno w rozporządzeniu, jak i w dyrektywie w sprawie policji ustanowiono przejrzyste, szczegółowe i kompleksowe przepisy dotyczące przekazywania danych osobowych do państw trzecich. Przepisy te obejmują wszystkie formy międzynarodowego przekazywania danych, zarówno do celów handlowych, jak i do celów związanych z egzekwowaniem prawa, pomiędzy osobami prywatnymi lub organami publicznymi bądź pomiędzy podmiotami prywatnymi a organami publicznymi. Choć struktura przepisów dotyczących międzynarodowego przekazywania danych pozostaje zasadniczo taka sama jak struktura przewidziana w aktualnie obowiązującej dyrektywie o ochronie danych (tj. decyzje w sprawie odpowiedniej ochrony danych osobowych, standardowe klauzule umowne i wiążące reguły korporacyjne, a także pewne odstępstwa od ogólnego zakazu przekazywania danych osobowych podmiotom poza UE), w pakiecie dotyczącym reformy doprecyzowano te przepisy i uproszczono je na szereg różnych sposobów, ograniczają zarazem biurokrację. Reforma obejmuje również pewne nowe narzędzia dotyczące międzynarodowego przekazywania danych.

Ponadto w rozporządzeniu rozszerzono **uprawnienia unijnych organów ochrony danych**, również w zakresie międzynarodowego przekazywania danych. W porównaniu z aktualnie obowiązującą dyrektywą o ochronie danych przepisy rozporządzenia dotyczące niezależności, funkcji i uprawnień unijnych organów ochrony danych są bardziej szczegółowe i znacznie rozbudowane. Zawarto w nich bezpośrednie uprawnienie do zawieszenia przepływów danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej. Dyrektywa w sprawie policji zawiera podobne przepisy w odniesieniu do międzynarodowego przekazywania danych oraz uprawnień organów ochrony danych w sektorze egzekwowania prawa.

Ściślej rzecz biorąc, jeżeli chodzi o przepisy dotyczące podejmowanych przez Komisję **decyzji w sprawie odpowiedniej ochrony danych osobowych**, w rozporządzeniu przewidziano precyzyjny i szczegółowy katalog elementów, które Komisja musi uwzględnić przy ocenie poziomu ochrony prawnej przewidzianej w porządku prawnym państwa trzeciego. W ramach tej procedury Komisja musi przeprowadzić kompleksową ocenę

uzależnione od tego, czy odnośne dane były wcześniej wymieniane między organami ścigania państw członkowskich.

[17] Zob. komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Europejska agenda bezpieczeństwa, COM(2015) 185 final z 28.4.2015.

przepisów regulujących dostęp do danych osobowych przez organy publiczne państwa trzeciego – element ten jest również zgodny z orzeczeniem w sprawie Schrems. Kolejnym kluczowym aspektem tej oceny jest fakt, że osoby fizyczne mogą skutecznie korzystać z możliwych do wyegzekwowania na drodze prawnej praw do ochrony danych osobowych i mogą skutecznie dochodzić odszkodowania na drodze sądowej i administracyjnej.

Ponadto w rozporządzeniu wyraźnie zobowiązano Komisję do przeprowadzania – co najmniej raz na cztery lata – **okresowego przeglądu** wszystkich wydanych przez siebie decyzji w sprawie odpowiedniej ochrony danych osobowych, aby należycie uwzględnić wszelkie istotne zmiany, które zaszły w państwie trzecim i które mogą mieć bezpośredni lub w praktyce niekorzystny wpływ na poziom ochrony przewidziany w porządku prawnym tego państwa. Tego rodzaju stałe monitorowanie odpowiedniości będzie stanowiło bardziej dynamiczny proces, ponieważ będzie wiązało się z koniecznością prowadzenia dialogu z organami danego państwa trzeciego.

Jeżeli chodzi o przekazywanie informacji do państw trzecich, w odniesieniu do których nie wydano decyzji w sprawie odpowiedniej ochrony danych osobowych, w rozporządzeniu określono warunki korzystania z **alternatywnych narzędzi przekazywania danych**, takich jak standardowe klauzule umowne i wiążące reguły korporacyjne. W rozporządzeniu przewidziano również inne instrumenty, np. zatwierdzone kodeksy postępowania i zatwierdzone mechanizmy certyfikacji. Ponadto w rozporządzeniu wyjaśniono, w jakich sytuacjach dopuszcza się możliwość skorzystania z **odstępstw**.

2.3. Dalsze działania

Reforma systemu ochrony danych stanowi istotny krok w kierunku wzmocnienia praw podstawowych obywateli w epoce cyfrowej oraz ułatwienia prowadzenia działalności gospodarczej dzięki uproszczeniu przepisów mających zastosowanie do przedsiębiorstw funkcjonujących na jednolitym rynku cyfrowym. Zaufanie konsumentów do podmiotów w UE i w państwach trzecich będzie stanowiło motor napędowy europejskiej i globalnej gospodarki cyfrowej, a tym samym przyniesie jej korzyści. Będzie ono miało pozytywny wpływ na nasze stosunki handlowe ze Stanami Zjednoczonymi, naszym największym partnerem handlowym. Zaufanie przyniesie przejrzystość i zapewni stabilne środowisko działania dla unijnych i zagranicznych przedsiębiorstw. Z kolei przedsiębiorstwa ze Stanów Zjednoczonych odniosą korzyść dzięki zwiększeniu pewności prawa, wynikającej z prowadzenia działalności gospodarczej w zintegrowanym obszarze gospodarczym, w którym stosuje się jednolity zbiór przepisów w zakresie ochrony danych.

Wspólne przepisy w sektorze egzekwowania prawa zagwarantują lepszą ochronę danych osób fizycznych oraz zapewnią tym osobom prawo do skutecznego korzystania ze środków zaskarżenia. Ułatwienie współpracy transgranicznej między policją a organami wymiaru sprawiedliwości w państwach członkowskich zwiększy efektywność egzekwowania prawa karnego, a tym samym stworzy warunki sprzyjające skuteczniejszemu zapobieganiu przestępczości w UE. Umożliwi to jednocześnie sprawniejszą współpracę z partnerami w państwach trzecich.

Oczekuje się, Parlament Europejski i Rada formalnie przyjmą pakiet dotyczący reformy w pierwszym półroczu 2016 r. Rozporządzenie będzie obowiązywało przez dwa lata od dnia jego przyjęcia, natomiast w odniesieniu do dyrektywy w sprawie policji przewidziano dwuletni okres wdrażania. Wszystkie zainteresowane strony, zarówno z UE, jak i spoza UE, powinny wykorzystać dwuletni okres przejściowy na przygotowanie się do stosowania nowych przepisów. Komisja również odegra pewną rolę w tym procesie. W trakcie okresu przejściowego Komisja będzie ściśle współpracowała z państwami członkowskimi, organami ochrony danych oraz innymi zainteresowanymi stronami na rzecz zapewnienia jednolitego stosowania przepisów i promowania otoczenia sprzyjającego przestrzeganiu obowiązującego prawa.

3. ZASADY OCHRONY PRYWATNOŚCI UE–USA: NOWE TRANSATLANTYCKIE RAMY PRZEPŁYWÓW DANYCH OSOBOWYCH

3.1. Kontekst

Aby usprawnić przepływy danych osobowych między UE a Stanami Zjednoczonymi do celów prowadzenia wymiany handlowej przy jednoczesnym zapewnieniu ochrony danych osobowych, Komisja uznała w 2000 r., że ramy bezpiecznego transferu danych osobowych zapewniają odpowiedni poziom ochrony[18]. W rezultacie, pomimo braku ogólnej ustawy o ochronie danych w Stanach Zjednoczonych, dane osobowe mogły być swobodnie przekazywane z państw członkowskich UE do przedsiębiorstw w Stanach Zjednoczonych, które zobowiązały się do przestrzegania zasad dotyczących prywatności leżących u podstaw tych ram.

W komunikacie w sprawie zasad bezpiecznego transferu danych osobowych z 2013 r.[19] Komisja zwróciła uwagę na szereg niedociągnięć związanych z funkcjonowaniem tego systemu na przestrzeni czasu, w szczególności na brak przejrzystości w kwestii tego, czy poszczególne przedsiębiorstwa przystąpiły do systemu, czy też nie, oraz na fakt, że organy Stanów Zjednoczonych nie podejmowały skutecznych działań służących wyegzekwowaniu przestrzegania przewidzianych w systemie zasad dotyczących prywatności przez przedsiębiorstwa, które przystąpiły do systemu. Co więcej, doniesienia o inwigilacji, które pojawiły się wcześniej w tym samym roku, wzbudziły obawy co do skali i zakresu niektórych programów gromadzenia danych przez amerykańskie organy wywiadowcze oraz co do poziomu dostępu amerykańskich organów publicznych do danych osobowych Europejczyków przekazywanych zgodnie z zasadami bezpiecznego transferu danych osobowych. Po wzięciu

[18] Decyzja Komisji 2000/520/WE z dnia 20 lipca 2000 r. Na mocy tej decyzji, wydanej na podstawie art. 25 ust. 6 dyrektywy o ochronie danych, Komisja uznała zasady bezpiecznego transferu danych osobowych oraz towarzyszące im często zadawane pytania opublikowane przez Departament Handlu Stanów Zjednoczonych za zapewniające odpowiedni poziom ochrony do celów przekazywania danych osobowych z UE. Funkcjonowanie ustaleń w zakresie bezpiecznego transferu danych osobowych opierało się na zobowiązaniach i samocertyfikacji uczestniczących przedsiębiorstw. Zgodnie z prawem Stanów Zjednoczonych wspomniane przepisy były wiążące dla tych podmiotów i można było dochodzić ich przed Federalną Komisją Handlu Stanów Zjednoczonych.

[19] Zob. przypis 3.

tych i innych[20] względów pod uwagę Komisja stwierdziła, że konieczne jest przeprowadzenie przeglądu zasad bezpiecznego transferu danych osobowych. W tym kontekście Komisja sformułowała 13 zaleceń[21] na rzecz wzmocnienia i zaktualizowania gwarancji w zakresie ochrony danych włączonych do tych ram. Zalecenia te dotyczyły przede wszystkim: (i) wzmocnienia konkretnych zasad dotyczących prywatności oraz zwiększenia przejrzystości strategii prywatności stosowanych przez samocertyfikowane przedsiębiorstwa amerykańskie i obejmujących te zasady; (ii) usprawnienia i poprawy nadzoru nad przestrzeganiem tych zasad przez przedsiębiorstwa oraz monitorowania i egzekwowania przestrzegania tych zasad przez organy amerykańskie; (iii) zapewnienia dostępu do przystępnych cenowo mechanizmów rozstrzygania sporów wszczynanych w rezultacie wniesienia skarg przez osoby fizyczne; oraz (iv) potrzeby zapewnienia ograniczenia korzystania z wyjątku dotyczącego bezpieczeństwa narodowego i egzekwowania prawa przewidzianego w decyzji w sprawie zasad bezpiecznego transferu danych osobowych z 2000 r. do działań, których podjęcie jest ściśle konieczne i proporcjonalne.

Na podstawie tych 13 zaleceń w styczniu 2014 r. Komisja przystąpiła do rozmów z władzami Stanów Zjednoczonych. Późniejsze unieważnienie decyzji w sprawie zasad bezpiecznego transferu danych osobowych przez Trybunał Sprawiedliwości w dniu 6 października 2015 r. potwierdziło konieczność ustanowienia nowych, solidniejszych ram regulujących kwestie związane z transatlantyckimi przepływami danych do celów handlowych. Choć w orzeczeniu Trybunału powołano się na zalecenia Komisji z 2013 r., podkreślono w nim również konieczność wprowadzenia ograniczeń, gwarancji oraz mechanizmów kontroli sądowej w celu zapewnienia stałej ochrony danych osobowych osób fizycznych z UE, w tym również w przypadku uzyskiwania dostępu do takich danych i ich stosowania przez organy publiczne do celów związanych z bezpieczeństwem narodowym, interesem publicznym lub egzekwowaniem prawa.

W dniu 2 lutego 2016 r., po dwóch latach intensywnych dyskusji, UE i Stany Zjednoczone osiągnęły porozumienie polityczne w sprawie nowych ram, tj. nowych zasad ochrony prywatności UE–USA. Te nowe ustalenia obejmują istotne nowe gwarancje i zapewnią wysoki poziom ochrony praw podstawowych osób fizycznych z UE. Dzięki nim przedsiębiorstwa po obu stronach Atlantyku, które chcą wspólnie prowadzić interesy, zyskają niezbędną pewność prawa. Ponadto nadadzą one nową dynamikę partnerstwu transatlantyckiemu.

Po zakończeniu negocjacji ze Stanami Zjednoczonymi Komisja przedstawi nowe ustalenia Grupie Roboczej Art. 29 (obejmującej organy ochrony danych w UE) w celu otrzymania od niej opinii na temat poziomu zapewnionej ochrony. Ponadto zanim będzie możliwe przyjęcie decyzji w sprawie odpowiedniej ochrony danych osobowych, zostanie ona poddana

[20] Wspomniane względy obejmowały gwałtowny wzrost natężenia przepływów danych oraz ich podstawowe znaczenie dla gospodarki transatlantyckiej, a także gwałtowny wzrost liczby przedsiębiorstw amerykańskich, które przestrzegają zasad bezpiecznego transferu danych osobowych. Zob. komunikat w sprawie zasad bezpiecznego transferu danych osobowych, s. 37.

[21] Komunikat w sprawie zasad bezpiecznego transferu danych osobowych, s. 18–19.

procedurze komitetowej. Co więcej, przeprowadzone zostaną konsultacje z Europejskim Inspektorem Ochrony Danych,

3.2. Co się zmieniło?

Nowe zasady ochrony prywatności UE–USA zapewniają solidną i skuteczną reakcję zarówno na 13 zaleceń Komisji, jak i na orzeczenie w sprawie Schrems. Zawierają one szereg istotnych ulepszeń, w porównaniu z poprzednimi ramami, w odniesieniu do zobowiązań, które muszą zostać podjęte przez przedsiębiorstwa z USA. Ponadto zawierają one ważne nowe zobowiązania i szczegółowe wyjaśnienia odpowiednich amerykańskich przepisów i praktyk stosowanych przez władze Stanów Zjednoczonych. W przeciwieństwie do wcześniejszych zasad nowe zasady ochrony prywatności obejmują nie tylko zobowiązania w sektorze handlowym, ale także, co jest istotne i co ma po raz pierwszy miejsce w stosunkach między UE a Stanami Zjednoczonymi, w obszarze dostępu organów publicznych do danych osobowych, m.in. do celów bezpieczeństwa narodowego. Jest to bardzo ważny i niezbędny w świetle orzecznictwa Trybunału element umożliwiający przywrócenie zaufania w stosunkach transatlantyckich po doniesieniach o inwigilacji.

Najważniejsze osiągnięcia wynikające z tych nowych ustaleń można podzielić na cztery główne kategorie.

Po pierwsze, **nałożenie rygorystycznych obowiązków na przedsiębiorstwa oraz konsekwentne egzekwowanie przepisów**: nowe zasady będą bardziej przejrzyste i obejmą skuteczne mechanizmy nadzoru w celu zapewnienia, by przedsiębiorstwa przestrzegały zasad, do których przestrzegania prawnie się zobowiązały. Amerykańskie przedsiębiorstwa, które chcą importować dane osobowe z Europy zgodnie z nowymi zasadami ochrony prywatności, będą musiały zaakceptować rygorystyczne obowiązki dotyczące sposobu przetwarzania danych osobowych i gwarantowania poszanowania praw jednostek. Obejmuje to zaostrzone warunki i bardziej rygorystyczne przepisy o odpowiedzialności obowiązujące przedsiębiorstwa stosujące nowe zasady ochrony prywatności, które przekazują unijne dane, np. na potrzeby działalności związanej z podwykonawstwem przetwarzania, osobom trzecim nieobjętym ramami zarówno w Stanach Zjednoczonych, jak i w innych państwach trzecich („wtórne przekazywanie"). Jeżeli chodzi o nadzór, Departament Handlu Stanów Zjednoczonych zobowiązał się do regularnego i rygorystycznego monitorowania sposobu, w jaki przedsiębiorstwa wywiązują się ze swoich zobowiązań, oraz do usunięcia „gapowiczów" tj. przedsiębiorstw, które niezgodnie z prawdą twierdzą, że przestrzegają systemu. Zobowiązania przedsiębiorstw są prawnie wiążące i możliwe do wyegzekwowania zgodnie z prawem Stanów Zjednoczonych przez Federalną Komisję Handlu, a na przedsiębiorstwa, które nie wywiązują się ze swoich zobowiązań, zostaną nałożone poważne sankcje.

Po drugie, **wprowadzenie wyraźnych ograniczeń i gwarancji w odniesieniu do dostępu administracji rządowej Stanów Zjednoczonych**: po raz pierwszy w historii rząd Stanów Zjednoczonych, za pośrednictwem Departamentu Sprawiedliwości i Urzędu Dyrektora Krajowych Służb Wywiadowczych, jako organu nadzorującego wszystkie amerykańskie służby wywiadowcze, przedstawił UE pisemne uwagi i zapewnienia, że dostęp organów publicznych do danych osobowych ze względów egzekwowania prawa, bezpieczeństwa

narodowego i innych interesów publicznych będzie podlegać wyraźnym ograniczeniom, gwarancjom i mechanizmom nadzoru. Stany Zjednoczone ustanowią również nowy mechanizm dochodzenia roszczeń w odniesieniu do osób z UE, których dane dotyczą, w obszarze bezpieczeństwa narodowego za pośrednictwem rzecznika, który będzie działał niezależnie od krajowych organów bezpieczeństwa. Rzecznik będzie odpowiadał za rozpatrywanie skarg i zapytań otrzymanych od osób fizycznych UE w kwestii dostępu do danych do celów bezpieczeństwa narodowego oraz będzie musiał potwierdzić danej osobie, że odpowiednie przepisy są przestrzegane lub że usunięto wszelkie niezgodności. Stanowi to znaczący postęp, który będzie miał zastosowanie nie tylko do transferów prowadzonych zgodnie z nowymi zasadami ochrony prywatności, ale do *wszystkich* danych osobowych przekazywanych do Stanów Zjednoczonych do celów handlowych, niezależnie od zastosowanej podstawy przekazania tych danych.

Po trzecie, **skuteczna ochrona prawa osób fizycznych UE do prywatności, obejmująca różne możliwości dochodzenia roszczeń**: każdy w Europie, kto uważa, że jego dane zostały niewłaściwie wykorzystane na mocy nowych zasad, będzie mógł skorzystać z kilku dostępnych i przystępnych cenowo możliwości indywidualnego dochodzenia roszczeń, w tym bezpłatnych usług organów oferujących alternatywne metody rozwiązywania sporów. Przedsiębiorstwa zobowiązują się do udzielenia odpowiedzi na skargi w ustalonym terminie. Ponadto każde przedsiębiorstwo przetwarzające dane z Europy o zasobach ludzkich musi zobowiązać się do przestrzegania decyzji właściwego unijnego organu ochrony danych, zaś inne przedsiębiorstwa mogą podjąć takie zobowiązanie dobrowolnie. Osoby fizyczne mogą również złożyć skargę do krajowego organu ochrony danych w swoim państwie, który będzie mógł korzystać ze sformalizowanej procedury kierowania skarg do Departamentu Handlu i Federalnej Komisji Handlu w celu ułatwienia dochodzenia i rozpatrzenia danego roszczenia w rozsądnych ramach czasowych. Jeżeli sprawa nie zostanie jednak rozstrzygnięta w ramach jednego z tych trybów, osoby fizyczne będą mogły ostatecznie odwołać się do panelu ds. ochrony prywatności, tj. mechanizmu rozstrzygania sporów, który może podejmować wiążące i możliwe do wyegzekwowania na drodze prawnej decyzje w stosunku do amerykańskich przedsiębiorstw stosujących nowe zasady ochrony prywatności. Ponadto unijne organy ochrony danych będą w stanie zapewnić osobom fizycznym pomoc w zakresie przygotowania sprawy. Jak wspomniano powyżej, na potrzeby rozpatrywania skarg dotyczących możliwego dostępu przez krajowe organy wywiadowcze zostanie utworzony nowy urząd rzecznika, co zapewni dodatkowe możliwości dochodzenia roszczeń.

Wreszcie po czwarte, **mechanizm wspólnego corocznego przeglądu:** umożliwi to Komisji regularne monitorowanie funkcjonowania wszystkich aspektów nowych zasad ochrony prywatności, w tym ograniczeń i gwarancji związanych z dostępem do danych do celów bezpieczeństwa narodowego. Komisja i Departament Handlu Stanów Zjednoczonych przeprowadzą przegląd z udziałem unijnych organów ochrony danych oraz krajowych organów bezpieczeństwa Stanów Zjednoczonych i rzecznika. W ten sposób Stany Zjednoczone będą ponosiły odpowiedzialność za swoje zobowiązania. Komisja nie poprzestanie jednak na tych działaniach: będzie również korzystać ze wszystkich dostępnych źródeł informacji, w tym dobrowolnych sprawozdań przedsiębiorstw z przejrzystości

dotyczących liczby rządowych wniosków o udostępnienie danych[22]. Roczny przegląd wykracza poza nowe rozporządzenie, które wymaga jedynie przeprowadzania takich przeglądów przynajmniej co cztery lata. Świadczy to o determinacji UE i Stanów Zjednoczonych do rygorystycznego zapewnienia pełnej zgodności.

Tego rodzaju przegląd nie będzie formalistycznym działaniem niewywołującym żadnych konsekwencji. W przypadkach, w których amerykańskie przedsiębiorstwa lub organy publiczne nie będą wywiązywać się ze swoich zobowiązań, Komisja uruchomi proces polegający na zawieszeniu nowych zasad ochrony prywatności. Jak podkreślił Trybunał Sprawiedliwości w orzeczeniu w sprawie Schrems, decyzja w sprawie odpowiedniej ochrony danych osobowych nie może być martwą literą prawa; amerykańskie przedsiębiorstwa i organy muszą raczej ożywić ramy i stale je utrzymywać, wywiązując się ze swoich zobowiązań. W przeciwnym razie szczególna korzyść dla przekazywania danych wynikająca z ustalenia dotyczącego adekwatności przestaje być uzasadniona i zostanie wycofana.

3.3. Dalsze działania

Zobowiązania uzgodnione przez Stany Zjednoczone zgodnie z nowymi zasadami ochrony prywatności będą stanowiły podstawę do sporządzenia nowej decyzji Komisji w sprawie odpowiedniej ochrony danych osobowych i zostaną w niej odzwierciedlone. Przedsiębiorstwa zachęca się do niezwłocznego rozpoczęcia przygotowań, tak aby były w stanie jak najszybciej zacząć stosować nowe ramy po ich wprowadzeniu w następstwie przyjęcia decyzji Komisji. Ze swojej strony rząd Stanów Zjednoczonych opublikuje swoje uwagi w amerykańskim rejestrze federalnym, tym samym publicznie poświadczając zamiar wywiązania się z podjętych zobowiązań.

Nowe zasady ochrony prywatności UE–USA wymagają podjęcia działań przez wiele podmiotów:

- uczestniczące przedsiębiorstwa amerykańskie, które muszą wywiązać się ze swoich obowiązków wynikających z ram przy pełnej świadomości, że będą one ściśle egzekwowane oraz że ich nieprzestrzeganie wiąże się z nałożeniem sankcji. W celu wzmocnienia zaufania konsumentów przedsiębiorstwa zachęca się również do wyboru unijnych organów ochrony danych jako docelowych organów rozpatrujących skargi dotyczące nowych zasad ochrony prywatności, ponieważ Europejczycy najprawdopodobniej zwrócą się do tych właśnie organów. Podobnie zakres, w jakim przedsiębiorstwa są przygotowane do skorzystania z przewidzianej w prawie amerykańskim możliwości publikowania sprawozdań z przejrzystości w sprawie wniosków o przyznanie dostępu do otrzymanych danych UE do celów bezpieczeństwa narodowego i egzekwowania prawa, przyczyni się do zachowania pewności, że tego rodzaju dostęp jest ograniczony do tego, co jest konieczne i proporcjonalne[23];

[22] Główne amerykańskie przedsiębiorstwa internetowe sporządzają już takie sprawozdania w celu odzyskania zaufania swoich klientów. Amerykańska ustawa o wolności z 2015 r. zezwala na publikację dobrowolnych sprawozdań dotyczących wniosków o udostępnienie danych, przynajmniej w niektórych branżach, w celu ochrony interesów bezpieczeństwa narodowego.

[23] Tego rodzaju sprawozdania sporządza się zgodnie z przepisami amerykańskiej ustawy o wolności z 2015 r. Zob. przypis 22.

– różne organy Stanów Zjednoczonych, którym powierzono nadzorowanie i egzekwowanie ram z poszanowaniem ograniczeń i gwarancji, jeżeli chodzi o dostęp do danych w celu egzekwowania prawa i bezpieczeństwa narodowego, oraz te, którym powierzono zadanie terminowego i stosownego reagowania na skargi złożone przez osoby fizyczne z UE dotyczące ewentualnego nadużycia ich danych osobowych;

– unijne organy ochrony danych, które mają do odegrania ważną rolę w zapewnianiu, aby osoby fizyczne mogły skutecznie korzystać z przysługujących im praw na mocy nowych zasad ochrony prywatności, m.in. poprzez kierowanie swoich skarg do odpowiednich organów Stanów Zjednoczonych i współpracę z nimi, uruchomienie procedury z udziałem rzecznika, wsparcie skarżących we wniesieniu spraw przed panel ds. ochrony prywatności oraz sprawowanie nadzoru nad przekazywaniem danych o zasobach ludzkich; oraz

– Komisję, która jest odpowiedzialna za ustalenie adekwatności i dokonywanie jej regularnego przeglądu: takie regularne przeglądy oznaczają istotne odejście od poprzedniej statycznej sytuacji poprzez przekształcenie ustalenia dotyczącego adekwatności zasad ochrony prywatności w ściśle monitorowane, żywe ramy.

Wspólny przegląd roczny i opracowane na jego podstawie sprawozdanie Komisji – oraz perspektywa zawieszenia porozumienia w przypadku braku zgodności – odegrają zatem kluczową rolę w zapewnieniu, by nowe zasady ochrony prywatności przetrwały próbę czasu. Naszą wzajemną ambicją transatlantycką powinno być wspólne rozwijanie silnej kultury przestrzegania prywatności i ochrony praw osób fizycznych, która zapewnia przywrócenie i utrzymanie zaufania.

4. UMOWA RAMOWA: WZMOCNIENIE GWARANCJI OCHRONY DANYCH NA POTRZEBY WSPÓŁPRACY ORGANÓW ŚCIGANIA

4.1. Kontekst

Ważnym wymiarem naszych stosunków transatlantyckich jest zdolność UE, państw członkowskich i Stanów Zjednoczonych do skutecznego reagowania na wspólne zagrożenia dla bezpieczeństwa i wyzwania w sposób skoordynowany i oparty na współpracy. Taka wspólna reakcja w znacznym stopniu zależy od naszej zdolności do wymiany danych osobowych w ramach współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych. Aby zrealizować ten cel, na przestrzeni czasu zawarto szereg umów dwustronnych między państwami członkowskimi a Stanami Zjednoczonymi oraz między UE a Stanami Zjednoczonymi[24]. Jednocześnie równie ważne jest, aby wspomniane porozumienia w zakresie egzekwowania prawa zapewniały skuteczne gwarancje ochrony danych. Dwojaki cel

[24] W szczególności umowa między UE a Stanami Zjednoczonymi o danych dotyczących przelotu pasażera oraz Program śledzenia środków finansowych należących do terrorystów (program TFTP) prowadzony przez UE i Stany Zjednoczone.

polegający na skutecznej współpracy z naszymi amerykańskimi partnerami na rzecz zwalczania poważnej przestępczości i terroryzmu przy jednoczesnym podnoszeniu poziomu ochrony Europejczyków zgodnie z ich prawami podstawowymi i unijnymi przepisami o ochronie danych podczas przekazywania danych w tych celach doprowadził do rozpoczęcia w marcu 2011 r. negocjacji, które dotyczyły międzynarodowej umowy w sprawie ochrony danych w obszarze egzekwowania prawa, tj. umowy ramowej między UE a Stanami Zjednoczonymi w sprawie ochrony danych[25].

UE i Stany Zjednoczone zakończyły negocjacje latem 2015 r. Obie strony parafowały umowę ramową w dniu 8 września 2015 r. w Luksemburgu[26] i obecnie oczekuje ona na ratyfikację po obu stronach Atlantyku. Podpisanie umowy ramowej było jednak uzależnione od przyjęcia przez Kongres Stanów Zjednoczonych ustawy o sądowych środkach odwoławczych w celu zapewnienia po raz pierwszy równego traktowania obywateli Unii i obywateli Stanów Zjednoczonych na mocy amerykańskiej ustawy o prywatności z 1974 r.[27]. Projekt ustawy został zatwierdzony przez Kongres w dniu 10 lutego 2016 r. i podpisany w dniu 24 lutego 2016 r.

4.2. Co się zmieniło?

Umowa ramowa po raz pierwszy będzie obejmowała zharmonizowany i kompleksowy zestaw gwarancji ochrony danych, który będzie miał zastosowanie do wszystkich rodzajów transatlantyckich wymian danych pomiędzy odpowiednimi organami w obszarze egzekwowania prawa karnego. Jest to w istocie umowa o prawach podstawowych wyznaczająca wysoki standard ochrony, do którego należy porównywać wszystkie wymiany danych w istniejących i przyszłych umowach.

Po pierwsze, **środki ochrony i gwarancje przewidziane w umowie ramowej będą miały horyzontalnie zastosowanie do wszystkich rodzajów wymian danych odbywających się w kontekście transatlantyckiej współpracy organów ścigania w sprawach karnych**. Obejmuje to przekazywanie danych na podstawie przepisów krajowych, umów między UE a Stanami Zjednoczonymi, umów między państwami członkowskimi a Stanami Zjednoczonymi (np. traktaty o wzajemnej pomocy prawnej) oraz określonych umów przewidujących przekazywanie danych osobowych przez podmioty prywatne do celów egzekwowania prawa. Uzgodnione przepisy natychmiast podniosą zatem poziom ochrony gwarantowany osobom z UE, których dane dotyczą, przy przekazywaniu danych do Stanów Zjednoczonych. Zwiększą

[25] Umowa między UE a Stanami Zjednoczonymi w sprawie ochrony danych osobowych przekazywanych i przetwarzanych do celów działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych, w tym terroryzmu, w ramach współpracy policyjnej i sądowej w sprawach karnych.

[26] http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm

[27] W ustawie o sądowych środkach odwoławczych przyznaje się prawa obywatelom „państw objętych" tą ustawą, wyznaczonych przez rząd Stanów Zjednoczonych. To z kolei jest uzależnione od następujących kryteriów: a) państwo [lub organizacja regionalna] zawarło umowę ze Stanami Zjednoczonymi o środkach ochrony prywatności informacji udostępnianych do celów zapobiegania, prowadzenia dochodzenia, wykrywania lub ścigania przestępstw; b) państwo lub [organizacja regionalna] zezwoliło na przekazywanie danych osobowych między nim a Stanami Zjednoczonymi do celów handlowych; oraz c) polityka dotycząca przekazywania danych osobowych do celów handlowych oraz powiązane działania państwa lub organizacji regionalnej nie mają istotnego wpływu na interesy Stanów Zjednoczonych w zakresie bezpieczeństwa narodowego.

one również pewność prawa w odniesieniu do transatlantyckiej współpracy organów ścigania przez zapewnienie, aby istniejące umowy zawierały wszystkie niezbędne środki ochrony i mogły tym samym obronić się w przypadku ewentualnych zastrzeżeń prawnych.

Po drugie, przepisy obejmują wszystkie podstawowe unijne przepisy o ochronie danych w zakresie **norm przetwarzania** (np. jakość i integralność danych, bezpieczeństwo danych, odpowiedzialność i nadzór), **gwarancji i ograniczeń** (np. ograniczenia dotyczące celów i wykorzystania, zatrzymywanie danych, wtórne przekazywanie, przetwarzanie danych szczególnie chronionych) oraz **praw osób fizycznych** (dostęp, poprawianie, dochodzenie odszkodowania na drodze administracyjnej i sądowej).

Po trzecie, umowa zapewni dostępność **prawa do dochodzenia odszkodowania na drodze sądowej w przypadku odmowy dostępu, odmowy poprawienia i bezprawnego ujawnienia**. Jest to istotna poprawa, która znacząco przyczyni się do przywrócenia zaufania do transatlantyckiej wymiany danych. Ten kluczowy postulat UE, który od wielu lat pozostawał bez odpowiedzi, został już odzwierciedlony w ustawie o sądowych środkach odwoławczych przedstawionej Kongresowi Stanów Zjednoczonych w marcu 2015 r. i przyjętej w dniu 10 lutego 2016 r. Ustawa ta rozszerzy na obywateli Unii[28] trzy podstawowe możliwości dochodzenia odszkodowania na drodze sądowej na mocy amerykańskiej ustawy o prywatności z 1974 r., które obecnie są zarezerwowane tylko dla amerykańskich obywateli i stałych rezydentów. Tym samym po raz pierwszy obywatele Unii będą mogli skorzystać z praw do ogólnego zastosowania w odniesieniu do dowolnego transferu danych w sektorze egzekwowania prawa karnego. Usuwa to krytyczną różnicę w traktowaniu obywateli Unii i Stanów Zjednoczonych.

Po czwarte, umowa ramowa uogólnia i rozszerza na cały sektor egzekwowania prawa zasadę **niezależnego nadzoru**, która stanowi podstawowy wymóg ochrony danych, a nie został uwzględniony w wielu istniejących umowach dwustronnych. Obejmuje to faktyczne uprawnienia do badania i rozpatrywania skarg osób fizycznych dotyczących zgodności z umową.

Po piąte, skuteczne wdrażanie umowy ramowej będzie podlegało **okresowym wspólnym przeglądom**. W ramach tych przeglądów szczególna uwaga zostanie poświęcona przepisom dotyczącym praw osób fizycznych (prawa do dostępu, poprawiania, dochodzenia odszkodowania na drodze administracyjnej i sądowej).

Umowa ramowa sama w sobie nie zezwala na przekazywanie danych ani nie stanowi decyzji w sprawie odpowiedniej ochrony danych osobowych.

4.3. Dalsze działania

Wejście w życie ustawy o sądowych środkach odwoławczych[29] utoruje drogę do podpisania umowy ramowej. Komisja wkrótce przedstawi Radzie wniosek w sprawie decyzji

[28] Zgodnie z ustawą o sądowych środkach odwoławczych inne państwa niebędące członkami UE lub „regionalne organizacje integracji gospodarczej" można w równym stopniu uznać za „państwa objęte tą ustawą", skutkiem czego ich obywatele będą mogli korzystać z prawa do dochodzenia odszkodowania na drodze sądowej.

[29] Ustawa o sądowych środkach odwoławczych wejdzie w życie po upływie 90 dni od dnia jej przyjęcia.

zezwalającej na podpisanie umowy ramowej. Po podpisaniu umowy i uzyskaniu zgody Parlamentu Europejskiego Rada będzie musiała przyjąć decyzję w sprawie zawarcia umowy. Umowa ramowa znacząco poprawi obecną sytuację, która charakteryzuje się fragmentarycznymi, niezharmonizowanymi i często nieskutecznymi przepisami o ochronie danych stosowanymi w ramach mozaiki wielostronnych, dwustronnych, krajowych i sektorowych instrumentów. Umowa ramowa ma moc wsteczną w tym sensie, że uzupełni gwarancje ochrony danych w obecnych umowach wówczas i w takim zakresie, w jakim nie posiadają one odpowiedniego poziomu gwarancji. W związku z tym umowa zapewni znaczącą wartość dodaną, przede wszystkim uzupełniając braki w istniejących umowach, które oferują niższe standardy ochrony danych niż standardy występujące w umowie ramowej. Umożliwi to ciągłość współpracy organów ścigania, zapewniając jednocześnie większą pewność prawa przy przekazywaniu danych. Jeżeli chodzi o przyszłe umowy, umowa ramowa będzie reprezentować siatkę bezpieczeństwa, poniżej której nie może spaść poziom ochrony. Jest to bardzo ważna gwarancja na przyszłość i zdecydowane przejście od sytuacji obecnej, w której gwarancje, środki ochrony i prawa muszą być negocjowane od nowa w przypadku każdej nowej umowy. Umowa ramowa stanowi zatem szablon zawierający standardowe gwarancje, których nie można obniżyć w toku negocjacji. Jest to bardzo ważny precedens nie tylko w odniesieniu do stosunków między UE a Stanami Zjednoczonymi, ale bardziej ogólnie do wszelkich przyszłych ustaleń dotyczących ochrony lub wymiany danych na szczeblu międzynarodowym.

Negocjowana równolegle z reformą umowa ramowa jest zgodna z dorobkiem UE w zakresie ochrony danych. Interakcja między umową ramową a dyrektywą w sprawie policji jest szczególnie istotna ze względu na znaczenie posiadania wysokiego i jednakowego poziomu ochrony danych, niezależnie od tego, czy dane osobowe są przetwarzane na szczeblu krajowym, czy wymieniane ponad granicami w UE lub z państwami trzecimi. W tym zakresie umowa ramowa pomoże uzasadnić ogólne wymogi reformy w kontekście transatlantyckim.

Zakończenie negocjacji w sprawie umowy ramowej, która ustanawia wspólne standardy w złożonej dziedzinie prawa i polityki, stanowi znaczące osiągnięcie. Przyszła umowa ramowa przywróci i wzmocni zaufanie, zapewni gwarancje legalności przekazywania danych i ułatwi współpracę między UE a Stanami Zjednoczonymi w tej dziedzinie.

W przyszłości będzie istniała potrzeba wspólnego zmierzenia się z wyzwaniami w dziedzinie współpracy policji i wymiaru sprawiedliwości. Jedną z istotnych otwartych kwestii jest bezpośredni dostęp organów ścigania do danych osobowych przechowywanych przez prywatne przedsiębiorstwa za granicą. Co do zasady taki dostęp powinien być umożliwiony w ramach formalnych kanałów współpracy, takich jak umowy o wzajemnej pomocy prawnej lub inne umowy sektorowe. Przedsiębiorstwa prywatne są obecnie narażone na brak pewności prawa, który może wpłynąć na ich zdolność do prowadzenia działalności w różnych jurysdykcjach, gdy są proszone o udzielenie dostępu, na mocy przepisów prawa jednego państwa, do dowodów elektronicznych dotyczących danych osobowych podlegających prawu innego państwa. Równolegle ze zbliżającym się przeglądem umowy o wzajemnej pomocy

prawnej między UE a Stanami Zjednoczonymi[30] UE z zadowoleniem przyjęłaby dalszą wymianę informacji ze Stanami Zjednoczonymi w tej sprawie, w tym poruszenie kwestii opracowania wspólnych i skuteczniejszych przepisów dotyczących gromadzenia dowodów elektronicznych.

5. Wnioski

Pomyślne zakończenie podstawowych działań przewidzianych w komunikacie z 2013 r. świadczy o zdolności UE do rozwiązywania problemów w sposób pragmatyczny i skoncentrowany, bez poświęcania jej ugruntowanych wartości i tradycji w zakresie praw podstawowych. Świadczy to również o tym, że UE i Stany Zjednoczone są w stanie pokonać istniejące między nimi różnice i podjąć trudne decyzje w celu utrzymania strategicznych stosunków, które przetrwały próbę czasu. Jednocześnie, chociaż rozpoczynamy nowy rozdział w naszych stosunkach dwustronnych, nie zakończył się jeszcze okres czujności, ponieważ nadal stawiamy czoła wspólnym zagrożeniom i wyzwaniom w niepewnym świecie.

Gdy nowe zasady ochrony prywatności i umowa ramowej zaczną obowiązywać, na obu stronach będzie spoczywał obowiązek zapewnienia, aby te dwa istotne instrumenty regulujące przekazywanie danych funkcjonowały w sposób skuteczny i trwały. Ich sukces zależy w dużej mierze od skutecznego egzekwowania prawa i poszanowania praw przyznanych osobom fizycznym. Zależy on również od ciągłej oceny ich funkcjonowania; wymaga to zmiany nastawienia i przejścia z procesu statycznego na bardziej dynamiczny.

W tym kontekście ważny element tego procesu odnosi się do trwającej reformy amerykańskich programów wywiadowczych. W związku z powyższym Komisja będzie uważnie śledzić zapowiadane sprawozdania przygotowywane przez amerykańską Radę ds. Prywatności i Wolności Obywatelskich (ang. Privacy and Civil Liberties Oversight Board – PCLOB) oraz przegląd sekcji 702 programu FISA dotyczącej inwigilacji zagranicznej zaplanowany na 2017 r. Przedmiotem ścisłego monitorowania będą w szczególności dalsze reformy dotyczące przejrzystości, nadzoru oraz rozszerzenia gwarancji na osoby niebędące obywatelami ani rezydentami Stanów Zjednoczonych.

Ogólniej rzecz biorąc, z uwagi na znaczenie transgranicznych przepływów danych w handlu transatlantyckim UE będzie uważnie śledzić dalsze postępy legislacyjne po stronie Stanów Zjednoczonych w dziedzinie prywatności. Teraz, gdy Europa wypracowała jeden spójny i solidny zbiór przepisów, można mieć nadzieję, że Stany Zjednoczone również będą kontynuowały wysiłki na rzecz kompleksowego systemu ochrony prywatności i danych. Dzięki takiemu właśnie kompleksowemu podejściu można osiągnąć zbieżność między obydwoma systemami w dłuższej perspektywie. W tym zakresie Komisja przeprowadzi doroczny szczyt poświęcony prywatności z udziałem zainteresowanych organizacji pozarządowych i innych zainteresowanych stron po obu stronach Atlantyku.

[30] Decyzja Rady 2009/820/WPZiB z dnia 23 października 2009 r. w sprawie zawarcia w imieniu Unii Europejskiej Umowy o ekstradycji między Unią Europejską a Stanami Zjednoczonymi Ameryki oraz Umowy o wzajemnej pomocy prawnej między Unią Europejską a Stanami Zjednoczonymi Ameryki, Dz.U. L 291 z 7.11.2009, s. 40–41.

Partnerstwo pomiędzy UE a Stanami Zjednoczonymi może stymulować opracowywanie i promowanie międzynarodowych norm prawnych w zakresie ochrony prywatności i danych osobowych. Inicjatywy podejmowane na szczeblu ONZ, w tym prace specjalnego sprawozdawcy ds. prawa do prywatności, również mogą odegrać ważną rolę w tym zakresie. W nadchodzących latach, z uwagi na rosnące znaczenie tych kwestii na arenie międzynarodowej, UE i Stany Zjednoczone powinny wykorzystać tę szansę, aby wzmocnić swoje wspólne wartości w zakresie wolności i praw osobistych w zglobalizowanym świecie cyfrowym.