KOMISJA
EUROPEJSKA

Bruksela, dnia 6.11.2015 r.
COM(2015) 566 final

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)

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Przekazywanie danych osobowych z UE do Stanów Zjednoczonych na mocy dyrektywy 95/46/WE w następstwie wyroku Trybunału Sprawiedliwości w sprawie C-362/14 (Schrems)

1. WPROWADZENIE: UCHYLENIE DECYZJI W SPRAWIE BEZPIECZNEGO PRZEKAZYWANIA DANYCH

W swoim wyroku z dnia 6 października 2015 r. w sprawie C-362/14 (Schrems)[1] Trybunał Sprawiedliwości Unii Europejskiej (zwany dalej: „Trybunałem Sprawiedliwości" lub „Trybunałem") potwierdził znaczenie praw podstawowych w kontekście ochrony danych osobowych, zgodnie z zapisem w Karcie praw podstawowych UE, również w sytuacjach przekazywania takich danych poza UE.

Przekazywanie danych osobowych jest zasadniczym elementem stosunków transatlantyckich. UE i USA są dla siebie wzajemnie najważniejszymi partnerami handlowymi, a przekazywanie danych w coraz większym stopniu stanowi integralną część wymiany handlowej.

Aby ułatwić przepływ danych przy jednoczesnym zapewnieniu wysokiego poziomu ochrony danych osobowych, Komisja uznała adekwatność ram prawnych „bezpiecznej przystani", przyjmując decyzję Komisji 2000/520/WE z dnia 20 lipca 2000 r. (zwaną dalej „decyzją w sprawie bezpiecznego przekazywania danych"). W decyzji tej, opartej na art. 25 ust. 6 dyrektywy 95/46/WE[2], Komisja uznała, że zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz odnoszące się do nich najczęściej zadawane pytania (NZP) wydane przez Departament Handlu USA zapewniają adekwatny poziom ochrony do celów przekazywania danych osobowych z UE[3]. W rezultacie dane osobowe mogą być swobodnie przekazywane z państw członkowskich UE do tych przedsiębiorstw w Stanach Zjednoczonych, które zobowiązały się do przestrzegania wspomnianych zasad, pomimo braku ogólnego prawa dotyczącego ochrony danych osobowych w Stanach Zjednoczonych. Funkcjonowanie ustaleń w zakresie „bezpiecznej przystani" opierało się na zobowiązaniach i samocertyfikacji uczestniczących przedsiębiorstw. Zobowiązanie się do przestrzegania zasad ochrony prywatności w ramach „bezpiecznej przystani" oraz NZP jest dobrowolne, jednak przepisy te są wiążące na mocy prawa USA dla tych podmiotów, które zobowiązały się do ich przestrzegania, a Federalna Komisja Handlu USA jest uprawniona do ich wyegzekwowania[4].

---

1 Wyrok z dnia 6 października 2015 r. w sprawie C-362/14 Maximilian Schrems przeciwko Data Protection Commissioner, EU:C:2015:650 (zwany dalej również „wyrokiem" lub „wyrokiem Schrems").

2 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 (zwana dalej „dyrektywą 95/46/WE" lub „dyrektywą").

3 Na potrzeby niniejszego komunikatu termin „UE" obejmuje również EOG. W związku z tym odniesienia do „państw członkowskich" rozumie się jako obejmujące również państwa członkowskie EOG.

4 Bardziej szczegółowy przegląd ustaleń w zakresie „bezpiecznej przystani" można znaleźć w komunikacie Komisji do Parlamentu Europejskiego i Rady w sprawie funkcjonowania zasad bezpiecznego transferu

W swoim wyroku z dnia 6 października 2015 r. Trybunał stwierdził nieważność decyzji w sprawie bezpiecznego przekazywania danych. W tym właśnie kontekście niniejszy komunikat ma na celu przedstawienie przeglądu narzędzi alternatywnych do celów transatlantyckiego przekazywania danych na mocy dyrektywy 95/46/WE w sytuacji braku decyzji w sprawie odpowiedniej ochrony danych osobowych. Opisano w nim również krótko konsekwencje wyroku dla innych wydanych przez Komisję decyzji w sprawie odpowiedniej ochrony danych osobowych. W swoim wyroku Trybunał wyjaśnił, że decyzja w sprawie odpowiedniej ochrony danych osobowych na mocy art. 25 ust. 6 dyrektywy 95/46/WE jest uzależniona od ustalenia przez Komisję, że w danym kraju trzecim poziom ochrony danych osobowych jest, jeśli nawet niekoniecznie identyczny, „merytorycznie równoważny" poziomowi gwarantowanemu na terytorium UE na mocy tej dyrektywy interpretowanej w świetle Karty praw podstawowych. W odniesieniu do decyzji w sprawie bezpiecznego przekazywania danych Trybunał orzekł, że nie zawierała ona wystarczających ustaleń Komisji dotyczących ograniczeń w zakresie dostępu amerykańskich organów publicznych do danych przekazywanych na mocy tej decyzji oraz dotyczących istnienia skutecznej ochrony prawnej przed taką ingerencją. W szczególności Trybunał wyjaśnił, że uregulowanie umożliwiające organom publicznym uzyskanie powszechnego dostępu do treści wiadomości elektronicznych należy uznać za naruszenie zasadniczej istoty prawa podstawowego do poszanowania życia prywatnego. Trybunał potwierdził ponadto, że nawet jeśli wydano decyzję w sprawie odpowiedniej ochrony danych osobowych na mocy art. 25 ust. 6 dyrektywy 95/46/WE, organy ochrony danych państw członkowskich nadal są uprawnione i zobowiązane do zbadania, w sposób całkowicie niezależny, czy przekazywanie danych do państwa trzeciego spełnia wymogi ustanowione w dyrektywie 95/46/WE, interpretowanej w świetle art. 7, 8 i 47 Karty praw podstawowych. Trybunał potwierdził jednak również, że jedynie Trybunał Sprawiedliwości może stwierdzić nieważność unijnego aktu prawnego, takiego jak decyzja Komisji w sprawie odpowiedniej ochrony danych osobowych.

Wyrok Trybunału opiera się na komunikacie Komisji z 2013 r. w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE[5], w którym Komisja wskazała szereg niedociągnięć i określiła 13 zaleceń. Na podstawie tych zaleceń od stycznia 2014 r. Komisja prowadziła rozmowy z organami USA w celu wprowadzenia w życie nowych, poprawionych uzgodnień dotyczących transatlantyckiej wymiany danych.

Po wyroku Trybunału Komisja jest nadal zaangażowana w realizację celu, jakim są odnowione i odpowiednie ramy prawne dla transatlantyckiego przekazywania danych

danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE, COM/2013/847 final.

[5] 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. Zob. również 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 oraz powiązane z nim memorandum „Odbudowa zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi – odpowiedzi na najczęściej zadawane pytania", MEMO/13/1059 z 27.11.2013.

osobowych. W związku z tym niezwłocznie wznowiła i zintensyfikowała ona rozmowy z rządem Stanów Zjednoczonych, aby zagwarantować, że wszelkie nowe uzgodnienia dotyczące transatlantyckiego przekazywania danych osobowych będą całkowicie spełniać normy ustanowione przez Trybunał. Wszelkie tego typu ramy prawne muszą zatem zawierać odpowiednie ograniczenia, zabezpieczenia i mechanizmy kontroli sądowej w celu zapewnienia stałej ochrony danych osobowych obywateli UE, także w odniesieniu do ewentualnego dostępu organów publicznych do celów egzekwowania prawa i do celów bezpieczeństwa narodowego. W międzyczasie przedstawiciele branży wyrazili obawy dotyczące możliwości dalszego przekazywania danych[6]. Konieczne jest zatem sprecyzowanie warunków dalszego przekazywania danych. Skłoniło to Grupę Roboczą Art. 29 – niezależny organ doradczy, w którym zasiadają przedstawiciele wszystkich organów ochrony danych z państw członkowskich, jak również Europejski Inspektor Ochrony Danych – do wydania w dniu 16 października oświadczenia[7] dotyczącego pierwszych wniosków z wyroku. Oprócz innych punktów oświadczenie zawierało następujące wskazówki dotyczące przekazywania danych:

- przekazywanie danych nie może już opierać się na unieważnionej decyzji Komisji w sprawie bezpiecznego przekazywania danych;

- w międzyczasie jako podstawę przekazywania danych można stosować standardowe klauzule umowne i wiążące reguły korporacyjne, choć Grupa Robocza Art. 29 stwierdziła także, że będzie nadal analizować wpływ wyroku na te alternatywne narzędzia.

W oświadczeniu wezwano państwa członkowskie i instytucje UE do podjęcia rozmów z władzami Stanów Zjednoczonych w celu znalezienia rozwiązań prawnych i technicznych dla przekazywania danych; negocjacje dotyczące nowego bezpiecznego przekazywania danych mogłyby, w opinii Grupy Roboczej Art. 29, być częścią tego rozwiązania.

Grupa Robocza Art. 29 ogłosiła, że jeżeli do końca stycznia 2016 r. wraz z władzami Stanów Zjednoczonych nie uda się znaleźć właściwego rozwiązania, i w zależności od oceny alternatywnych narzędzi służących do przekazywania danych, organy ochrony danych podejmą wszelkie niezbędne i odpowiednie działania, w tym skoordynowane działania w zakresie egzekwowania przepisów.

---

[6] Przedstawiciele stowarzyszeń branżowych wyrazili te obawy m.in. na posiedzeniu zorganizowanym przez wiceprzewodniczącego Andrusa Ansipa oraz komisarzy Günthera Oettingera i Věrę Jourovą tuż po wydaniu wyroku Schrems w dniu 14 października. Zob. Daily News z 14.10.2015 (MEX/15/5840). Zob. też: „List otwarty w sprawie wykonania wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-362/14 Maximillian Schrems przeciwko Data Protection Commissioner" z dnia 13 października 2015 r., skierowany do przewodniczącego Komisji Jeana-Claude'a Junckera i podpisany przez unijne i amerykańskie stowarzyszenia branżowe i przedsiębiorstwa: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1045&PortalId=0&TabId=353

[7] Oświadczenie Grupy Roboczej Art. 29 jest dostępne pod adresem: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

Ponadto Grupa Robocza Art. 29 podkreśliła współodpowiedzialność organów ochrony danych, instytucji UE, państw członkowskich i przedsiębiorstw za znalezienie trwałych rozwiązań służących wykonaniu wyroku Trybunału. W szczególności Grupa Robocza wezwała przedsiębiorstwa, aby rozważyły wprowadzenie wszelkich prawnych i technicznych rozwiązań ograniczających potencjalne ryzyko, jakie towarzyszy przekazywaniu przez nie danych.

Niniejszy komunikat jest bez uszczerbku dla całkowicie niezależnych uprawnień i obowiązków organów ochrony danych w zakresie badania legalności takiego przekazywania danych[8]. Nie ustanawia się w nim żadnych wiążących zasad i w pełni szanuje się uprawnienia sądów krajowych do interpretowania prawa właściwego oraz, w razie konieczności, do przedkładania Trybunałowi Sprawiedliwości wniosków o wydanie orzeczenia w trybie prejudycjalnym. Niniejszy komunikat nie może również stanowić podstawy dla żadnych indywidualnych lub zbiorowych uprawnień ani roszczeń.

2. ALTERNATYWNE PODSTAWY PRZEKAZYWANIA DANYCH OSOBOWYCH DO USA

Przepisy dotyczące międzynarodowego przekazywania danych określone w dyrektywie 95/46/WE opierają się na wyraźnym rozróżnieniu między, z jednej strony, przekazywaniem danych państwom trzecim zapewniającym odpowiedni stopień ochrony (art. 25 dyrektywy) oraz, z drugiej strony, przekazywaniem danych państwom trzecim, które uznano za niezapewniające odpowiedniego stopnia ochrony (art. 26 dyrektywy).

Wyrok Schrems odnosi się do warunków, na jakich, zgodnie z art. 25 ust. 6 dyrektywy 95/46/WE, Komisja może stwierdzić, że państwo trzecie zapewnia odpowiedni stopień ochrony.

W sytuacjach gdy państwo trzecie, do którego mają zostać przekazane dane osobowe z UE, uznano za niezapewniające odpowiedniego stopnia ochrony, art. 26 dyrektywy 95/46/WE przewiduje liczne alternatywne podstawy, w oparciu o które przekazanie danych może jednak nastąpić. W szczególności przekazanie można wykonać, gdy podmiot odpowiedzialny za określanie celów i sposobów przetwarzania danych osobowych („administrator danych")

- zaleci odpowiednie zabezpieczenia, w rozumieniu art. 26 ust. 2 dyrektywy 95/46/WE, odnośnie do ochrony prywatności oraz podstawowych praw i wolności osoby oraz odnośnie do wykonywania odpowiednich praw. Takie środki zabezpieczające mogą w szczególności wynikać z odpowiednich klauzul umownych wiążących podmiot przekazujący dane i podmiot odbierający dane (zob. sekcja 2.1 i 2.2 poniżej). Obejmują one standardowe klauzule umowne wydane przez Komisję oraz, w odniesieniu do przekazywania danych między poszczególnymi podmiotami wchodzącymi w skład wielonarodowej grupy przedsiębiorstw, wiążące reguły korporacyjne dopuszczone przez organy ochrony danych; lub

[8] Zob. art. 8 ust. 3 Karty praw podstawowych oraz art. 16 ust. 2 TFUE. Niezależność ta została również podkreślona przez Trybunał w wyroku Schrems.

– powołują się na jedno z odstępstw wyraźnie wymienionych w art. 26 ust. 1 lit. a) – f) dyrektywy 95/46/WE (zob. sekcja 2.3 poniżej).

W porównaniu z decyzjami w sprawie odpowiedniej ochrony danych osobowych, które wynikają z ogólnej oceny systemu danego państwa trzeciego i mogą zasadniczo obejmować wszelkie przekazywanie danych do tego systemu, takie alternatywne podstawy przekazywania danych mają bardziej ograniczony zakres (dotyczą one wyłącznie konkretnych kategorii przepływów danych) oraz szerszy zasięg (nie zawsze są one ograniczone do danego kraju). Alternatywne podstawy przekazywania danych mają zastosowanie do przepływów danych wkonywanych przez poszczególne podmioty, które postanowiły skorzystać z jednej z możliwości przewidzianych w art. 26 dyrektywy 95/46/WE. Ponadto w przypadku gdy podmioty przekazujące dane i podmioty odbierające dane opierają przekazywanie danych na takich podstawach, oraz ponieważ nie mogą one polegać na zawartym w decyzji Komisji stwierdzeniu, że państwo trzecie zapewnia odpowiedni stopień ochrony, ponoszą one odpowiedzialność za zapewnienie, aby przekazywanie danych było zgodne z wymogami dyrektywy.

2.1. Rozwiązania umowne

Jak podkreślono na forum Grupy Roboczej Art. 29, klauzule umowne – aby mogły stanowić wystarczające zabezpieczenia dla celów art. 26 ust. 2 dyrektywy 95/46/WE – „muszą zadowalająco rekompensować brak ogólnego poziomu odpowiedniej ochrony, poprzez włączenie istotnych elementów ochrony, których brakuje w danej konkretnej sytuacji”[9]. W celu ułatwienia stosowania tych instrumentów w międzynarodowym przekazywaniu danych Komisja zatwierdziła, zgodnie z art. 26 ust. 4 dyrektywy, cztery zestawy standardowych klauzul umownych, które uważa się za spełniające wymagania określone w art. 26 ust. 2 dyrektywy. Dwa zestawy klauzul wzorcowych odnoszą się do przekazywania danych między administratorami danych[10], natomiast pozostałe dwa zestawy dotyczą przekazywania danych między administratorem danych a przetwarzającym działającym na jego polecenie[11]. W każdym z tych zestawów klauzul wzorcowych ustanowiono odnośne obowiązki podmiotów przekazujących dane i podmiotów odbierających dane. Obejmują one obowiązki w zakresie, między innymi, środków bezpieczeństwa, informacji przekazywanych osobie, której dane

[9] Zob. dokument roboczy WP 12 „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych”, przyjęty przez Grupę Roboczą Art. 29 dnia 24 lipca 1998 r., s. 16.

[10] Decyzja Komisji 2001/497/WE z dnia 15 czerwca 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, na mocy dyrektywy 95/46/WE, Dz.U. L 181 z 4.7.2001, s. 19 oraz decyzja Komisji 2004/915/WE z dnia 27 grudnia 2004 r. zmieniająca decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, Dz.U. L 385 z 29.12.2004, s. 74.

[11] Decyzja Komisji 2002/16/WE z dnia 27 grudnia 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych przetwarzającym dane mającym siedzibę w państwach trzecich, na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, Dz.U. L 6 z 10.1.2002, s. 52 oraz decyzja Komisji z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, Dz.U. L 39 z 12.2.2010, s. 5. Wcześniejsza decyzja, uchylona przez późniejszą, ma zastosowanie jedynie do umów zawartych przed dniem 15 maja 2010 r.

dotyczą, w przypadku przekazywania danych szczególnie chronionych, powiadomienia podmiotu przekazującego dane o wnioskach o umożliwienie dostępu składanych przez organy ścigania państw trzecich lub o wszelkim przypadkowym lub nieuprawnionym dostępie, oraz w zakresie praw osób, których dane dotyczą, do dostępu do swoich danych osobowych, ich sprostowania lub usunięcia, jak również zasad odszkodowania dla osoby, której dane dotyczą, w przypadku szkody wynikającej z naruszenia przez którąkolwiek ze stron standardowych klauzul umownych. Klauzule wzorcowe zawierają również wymóg, aby obywatel UE, którego dane dotyczą, miał możliwość dochodzenia przed organem ochrony danych lub sądem państwa członkowskiego, w którym ma swoją siedzibę podmiot przekazujący dane, praw przysługujących im na mocy klauzul umownych jako beneficjentowi będącemu osobą trzecią[12]. Te prawa i obowiązki są koniecznym elementem klauzul umownych, ponieważ - w przeciwieństwie do sytuacji, w której Komisja ustaliła, że stopień ochrony danych jest odpowiedni - nie można zakładać, że podmiot odbierający dane w państwie trzecim jest objęty odpowiednim systemem nadzoru i egzekwowania przepisów o ochronie danych.

Ponieważ w państwach członkowskich decyzje Komisji wiążą w całości, włączenie do umowy standardowych klauzul umownych oznacza, że organy krajowe są co do zasady zobowiązane do zaakceptowania tych klauzul. W konsekwencji nie mogą one odmówić przekazania danych państwu trzeciemu tylko na tej podstawie, że wspomniane standardowe klauzule umowne nie oferują wystarczających zabezpieczeń. Pozostaje to bez uszczerbku dla prawa państw członkowskich do zbadania tych klauzul w świetle wymogów określonych przez Trybunał w wyroku Schrems. W przypadku wątpliwości powinny one wnieść sprawę do sądu krajowego, który z kolei może zwrócić się z wnioskiem do Trybunału Sprawiedliwości o wydanie orzeczenia w trybie prejudycjalnym. W większości przepisów państw członkowskich transponujących dyrektywę 95/45/WE nie istnieje wymóg uzyskania uprzedniego zezwolenia krajowego na przekazanie danych, jednak niektóre państwa członkowskie stosują system powiadamiania lub wcześniejszej zgody na wykorzystanie standardowych klauzul umownych. W takim przypadku krajowy organ ochrony danych musi porównać klauzule faktycznie zawarte w spornej umowie ze standardowymi klauzulami umownymi i sprawdzić, czy nie wprowadzono żadnych zmian[13]. Jeśli klauzule zastosowano bez poprawek[14], zezwolenie jest zasadniczo[15] udzielane automatycznie[16]. Jak wyjaśniono

[12] Zob. np. motyw 6 decyzji Komisji 2004/915/WE i pkt V załącznika; klauzula 7 załącznika do decyzji Komisji 2010/87/UE.

[13] Należy zauważyć, że wniosek dotyczący ogólnego rozporządzenia o ochronie danych (COM(2012) 11 final) przewiduje, że przekazywanie danych dokonywane w oparciu o standardowe klauzule umowne lub wiążące reguły korporacyjne w zakresie, w jakim zostały one przyjęte przez Komisję lub zgodnie z przewidzianym mechanizmem zgodności, nie wymaga dodatkowych zezwoleń.

[14] Stosowanie standardowych klauzul umownych nie uniemożliwia jednak stronom prowadzenia uzgodnień w sprawie dodania innych klauzul, pod warunkiem że nie będą one bezpośrednio lub pośrednio sprzeczne z klauzulami zatwierdzonymi przez Komisję i nie będą naruszały podstawowych praw lub wolności osób, których dane dotyczą. Zob. dokument Komisji Europejskiej „Często zadawane pytania na temat przekazywania danych osobowych z UE/EOG do państw trzecich" (pytanie B.1.9), s. 28 (dokument dostępny w internecie pod adresem: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf).

[15] Jeśli organ ochrony danych ma wątpliwości dotyczące zgodności standardowych klauzul umownych z wymaganiami dyrektywy, powinien on skierować zapytanie do sądu krajowego, który z kolei może zwrócić się z wnioskiem do Trybunału Sprawiedliwości o wydanie orzeczenia w trybie prejudycjalnym (por. pkt 51, 52, 64 i 65 wyroku Schrems).

poniżej (zob. sekcja 2.4), pozostaje to bez uszczerbku dla dodatkowych środków, jakie podmiot przekazujący dane może być zmuszony podjąć, w szczególności w następstwie informacji otrzymanych od podmiotu odbierającego dane na temat zmian w systemie prawnym danego państwa trzeciego, które mogą uniemożliwiać podmiotowi odbierającemu dane wypełnienie jego zobowiązań umownych. W przypadku stosowania standardowych klauzul umownych nadzorem organów ochrony danych objęte są zarówno podmioty przekazujące dane, jak i - w wyniku zobowiązania się do przestrzegania postanowień umowy - podmioty otrzymujące dane.

Przyjęcie standardowych klauzul umownych nie uniemożliwia przedsiębiorstwom stosowania innych instrumentów, takich jak ustalenia umowne *ad hoc*, aby wykazać, że przekazują one dane z zastosowaniem wystarczających zabezpieczeń w rozumieniu art. 26 ust. 2 dyrektywy 95/46/WE. Zgodnie z art. 26 ust. 2 dyrektywy muszą one być każdorazowo zatwierdzane przez organy krajowe. Niektóre organy ochrony danych opracowały wytyczne w tej dziedzinie, w tym w formie standardowych umów lub szczegółowych zasad, jakimi należy się kierować przy sporządzaniu klauzul dotyczących przekazywania danych. Większość umów stosowanych obecnie przez przedsiębiorstwa do celów międzynarodowego przekazywania danych oparta jest jednak na zatwierdzonych przez Komisję standardowych klauzulach umownych[17].

2.2. Wewnątrzgrupowe przekazywanie danych

Aby przekazać dane osobowe z UE do oddziałów zlokalizowanych poza UE zgodnie z wymogami określonymi w art. 26 ust. 2 dyrektywy 95/46/WE, przedsiębiorstwo wielonarodowe może przyjąć wiążące reguły korporacyjne. Tego rodzaju kodeks postępowania można stosować wyłącznie w odniesieniu do przekazywania danych w obrębie grupy przedsiębiorstw.

Zastosowanie wiążących reguł korporacyjnych umożliwia swobodny przepływ danych osobowych między poszczególnymi podmiotami grupy przedsiębiorstw na całym świecie, bez konieczności ustaleń umownych między każdym podmiotem z osobna, przy jednoczesnym zapewnieniu przestrzegania przez całą grupę tego samego wysokiego poziomu ochrony danych osobowych za pomocą jednego zestawu wiążących i dających się egzekwować zasad. Jednolity zestaw zasad zapewnia prostszy i bardziej skuteczny system, który pracownicy mogą łatwiej wdrożyć, a osoby, których dane dotyczą, lepiej zrozumieć. W celu wsparcia przedsiębiorstw w opracowywaniu wiążących reguł korporacyjnych Grupa Robocza Art. 29 objaśniła wymogi merytoryczne (np. zasadę celowości, bezpieczeństwo przetwarzania,

---

[16] Grupa Robocza Art. 29 ustanowiła specjalną procedurę współpracy między organami ochrony danych w kwestii zatwierdzania klauzul umownych, które przedsiębiorstwo zamierza stosować w różnych państwach członkowskich. Zob. dokument roboczy WP 226 określający procedurę współpracy na rzecz wydawania wspólnych opinii dotyczących klauzul umownych uznanych za zgodne ze wspólnotową klauzulą wzorcową, przyjęty przez Grupę Roboczą Art. 29 w dniu 26 listopada 2014 r. Zob. również pkt VII załącznika do decyzji Komisji 2004/915/WE oraz klauzulę 10 załącznika do decyzji Komisji 2010/87/UE.

[17] Zob. dokument roboczy WP 226 określający procedurę współpracy na rzecz wydawania wspólnych opinii dotyczących klauzul umownych uznanych za zgodne ze wspólnotową klauzulą wzorcową, przyjęty przez Grupę Roboczą Art. 29 dnia 26 listopada 2014 r., s. 2.

przejrzyste informowanie osób, których dane dotyczą, ograniczenia w zakresie dalszego przekazywania danych poza grupę, indywidualne prawa dostępu, sprostowania i sprzeciwu) oraz proceduralne (np. audyty, kontrolę zgodności, rozpatrywanie skarg, współpracę z organami ochrony danych, odpowiedzialność oraz jurysdykcję) dotyczące wiążących reguł korporacyjnych, oparte na unijnych standardach ochrony danych[18]. Zasady te nie tylko wiążą wszystkich członków grupy przedsiębiorstw, lecz, podobnie jak standardowe klauzule umowne, są także możliwe do wyegzekwowania na drodze prawnej w UE. Osoby, których dane osobowe są przetwarzane przez dany podmiot grupy, są uprawnione, jako beneficjenci będący osobami trzecimi, do wyegzekwowania przestrzegania wiążących reguł korporacyjnych poprzez złożenie skargi do organu ochrony danych i wniesienie sprawy przed sądem danego państwa członkowskiego. Oprócz tego w wiążących regułach korporacyjnych należy wyznaczyć podmiot na terenie UE, który przyjmuje odpowiedzialność za naruszenie zasad przez któregokolwiek członka grupy spoza UE, związanego tymi zasadami.

W większości państw członkowskich przepisy krajowe przyjęte w celu transpozycji dyrektywy przewidują, że przekazywanie danych na podstawie wiążących reguł korporacyjnych musi być zatwierdzone przez organ ochrony danych w każdym państwie członkowskim, z którego przedsiębiorstwo wielonarodowe zamierza przekazać dane. W celu ułatwienia i przyspieszenia tego procesu, a także aby zmniejszyć obciążenie dla wnioskodawców, Grupa Robocza Art. 29 określiła standardowy formularz wniosku[19] oraz szczegółową procedurę współpracy pomiędzy zainteresowanymi organami ochrony danych[20], która obejmuje wyznaczenie jednego „głównego organu" odpowiedzialnego za przeprowadzenie procedury zatwierdzenia.

2.3. Odstępstwa

Dane osobowe można przekazywać podmiotom mającym siedzibę w kraju trzecim nawet w sytuacji braku decyzji w sprawie odpowiedniej ochrony danych osobowych na mocy art. 25 ust. 6 dyrektywy 95/46/WE i niezależnie od zastosowania standardowych klauzul umownych lub wiążących reguł korporacyjnych, o ile ma zastosowanie jedno z odstępstw określonych w art. 26 ust. 1 dyrektywy 95/46/WE[21]:

---

[18] Zob. dokument roboczy WP 153 ustanawiający tabelę zawierającą elementy i zasady, które mają być uwzględnione w wiążących regułach korporacyjnych, przyjęty przez Grupę Roboczą Art. 29 dnia 24 czerwca 2008 r.; dokument roboczy WP 154 w sprawie określenia ram dla struktury wiążących reguł korporacyjnych, przyjęty dnia 24 czerwca 2008 r.; oraz dokument roboczy WP 155 w sprawie często zadawanych pytań (FAQs) dotyczących wiążących reguł korporacyjnych, przyjęty przez Grupę Roboczą Art. 29 dnia 24 czerwca 2008 r.

[19] Dokument roboczy WP 133 „Standardowy wniosek o zatwierdzenie wiążących reguł korporacyjnych dla przekazywania danych osobowych", przyjęty przez Grupę Roboczą Art. 29 dnia 10 stycznia 2007 r.

[20] Dokument roboczy WP 107 ustanawiający procedurę współpracy na rzecz wydawania wspólnych opinii dotyczących odpowiednich środków zabezpieczających wynikających z wiążących reguł korporacyjnych, przyjęty przez Grupę Roboczą Art. 29 dnia 14 kwietnia 2005 r.

[21] Jak podkreśliła Grupa Robocza Art. 29, konieczne jest przestrzeganie dodatkowych wymogów mających znaczenie dla stosowania tych odstępstw, zawartych w innych przepisach dyrektywy 95/46/WE (np. ograniczenia zawarte w art. 8 dotyczące przetwarzania danych szczególnie chronionych). Zob. dokument roboczy WP 114 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty przez Grupę Roboczą Art. 29 w dniu 25 listopada 2005 r., s. 8. Zob. także dokument

- osoba, której dane dotyczą, udzieliła jednoznacznej zgody na proponowane przekazanie danych;

- przekazanie danych jest konieczne dla realizacji umowy między osobą, której dane dotyczą, i administratorem danych lub dla wprowadzenia w życie ustaleń poprzedzających zawarcie umowy, przyjętych na wniosek osoby, której dane dotyczą;

- przekazanie danych jest konieczne dla zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą, między administratorem danych i osobą trzecią;

- przekazanie danych jest konieczne lub wymagane przez prawo z ważnych względów publicznych[22] lub w celu ustanowienia, wykonania lub obrony tytułu prawnego;

- przekazanie jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą;

- przekazanie danych następuje z rejestru, który ma służyć, zgodnie z obowiązującymi przepisami ustawowymi lub wykonawczymi, za źródło informacji dla ogółu społeczeństwa, udostępnionego do konsultacji obywateli i każdej osoby wykazującej uzasadniony interes, o ile warunki określone przez prawo odnośnie do wglądu do takiego rejestru zostały w danym przypadku spełnione.

Względy te stanowią odstępstwo od ogólnego zakazu przekazywania danych osobowych podmiotom mającym siedzibę w państwie trzecim niezapewniającym odpowiedniego stopnia ochrony. Podmiot przekazujący dane nie musi gwarantować zapewnienia odpowiedniej ochrony przez podmiot odbierający dane, i zazwyczaj nie będzie potrzebował uprzedniego zezwolenia na przekazanie danych od właściwych organów krajowych. Niemniej jednak, zdaniem Grupy Roboczej Art. 29, odstępstwa te muszą podlegać wykładni zawężającej ze względu na ich szczególny charakter[23].

Grupa Robocza Art. 29 wydała kilka niewiążących wytycznych w sprawie stosowania art. 26 ust. 1 dyrektywy 95/46/WE[24]. Obejmują one szereg „najlepszych praktyk" opracowanych w

---

Komisji Europejskiej „Często zadawane pytania na temat przekazywania danych osobowych z UE/EOG do państw trzecich" (pytanie D.2), s. 50.

22 Może to obejmować na przykład przekazywanie danych między organami podatkowymi lub służbami celnymi, lub między służbami odpowiedzialnymi za kwestie ubezpieczeń społecznych (zob. motyw 58 dyrektywy 95/46/WE). Odstępstwo to może również dotyczyć przekazywania danych między organami nadzoru w sektorze usług finansowych. Zob. dokument roboczy WP 12 „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych", przyjęty przez Grupę Roboczą Art. 29 dnia 24 lipca 1998 r., s. 25;

23 Dokument roboczy WP 114 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty przez Grupę Roboczą Art. 29 w dniu 25 listopada 2005 r., s. 7, 17

24 Dokument roboczy WP 12 „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych", przyjęty przez Grupę Roboczą Art. 29 dnia 24 lipca 1998 r.; dokument roboczy WP 114 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty przez Grupę Roboczą Art. 29 w dniu 25 listopada 2005 r. Zob. także dokument Komisji

celu ukierunkowania działań w zakresie egzekwowania przepisów prowadzonych przez organy ochrony danych[25]. W szczególności Grupa Robocza zaleca, aby przekazywanie danych osobowych, które można zaliczyć do kategorii powtarzających się, masowych lub strukturalnych, odbywało się z zastosowaniem wystarczających zabezpieczeń i, w miarę możliwości, w określonych ramach prawnych, takich jak standardowe klauzule umowne lub wiążące reguły korporacyjne[26].

W następstwie stwierdzenia nieważności decyzji w sprawie bezpiecznego przekazywania danych w niniejszym komunikacie Komisja będzie odwoływać się jedynie do tych odstępstw, które wydają się szczególnie istotne dla przekazywania danych w kontekście handlowym.

2.3.1. Przekazywanie danych konieczne dla realizacji umowy lub dla wprowadzenia w życie ustaleń poprzedzających zawarcie umowy na wniosek osoby, której dane dotyczą (art. 26 ust. 1 lit. b))

Odstępstwo to może być stosowane na przykład w kontekście rezerwacji hotelowej lub przekazywania informacji o płatnościach do państwa trzeciego w celu dokonania przelewu bankowego. Grupa Robocza Art. 29 uważa jednak, że we wszystkich tych przypadkach musi istnieć „ścisłe i zasadnicze powiązanie", „bezpośredni i obiektywny związek" między osobą, której dane dotyczą, i celem umowy lub ustaleń poprzedzających zawarcie umowy (test konieczności)[27]. Ponadto odstępstwo nie może być stosowane do przekazywania dodatkowych informacji, które nie są konieczne do celów przekazania danych, ani do przekazywania danych w celu innym niż wykonanie umowy (na przykład w celach prowadzenia działań marketingowych po wykonaniu umowy)[28]. Co się tyczy ustaleń poprzedzających zawarcie umowy, Grupa Robocza Art. 29 wyraziła pogląd, że obejmują one jedynie kontakty zainicjowane przez osobę, której dane dotyczą (na przykład pytanie o informacje na temat o danej usługi), ale nie kontakty wynikające z działań marketingowych podjętych przez administratora danych[29].

Europejskiej „Często zadawane pytania na temat przekazywania danych osobowych z UE/EOG do państw trzecich" (pytania D.1-D.9), s. 48-54.

[25] Dokument roboczy WP 114 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty przez Grupę Roboczą Art. 29 w dniu 25 listopada 2005 r., s. 8-10.

[26] Dokument roboczy WP 114 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty przez Grupę Roboczą Art. 29 w dniu 25 listopada 2005 r., s. 9. Według Grupy Roboczej przekazywanie danych zaliczane do kategorii masowych lub powtarzających się może odbywać się jedynie na podstawie odstępstwa, w przypadku gdy zastosowanie standardowych klauzul umownych lub wiążących reguł korporacyjnych jest w praktyce niemożliwe i gdy ryzyko dla osoby, której dane dotyczą, jest niewielkie (np. międzynarodowe przekazy pieniężne). Zob. także dokument Komisji Europejskiej „Często zadawane pytania na temat przekazywania danych osobowych z UE/EOG do państw trzecich" (pytanie D.1), s. 49.

[27] Dokument roboczy WP 114 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty przez Grupę Roboczą Art. 29 w dniu 25 listopada 2005 r., s. 13. Zob. również dokument roboczy WP 66 „Opinia 6/2002 w sprawie przekazywania informacji na temat listy pasażerów i innych danych przez linie lotnicze Stanom Zjednoczonym", przyjęty dnia 24 października 2002 r.

[28] Dokument roboczy WP 12 „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych", przyjęty przez Grupę Roboczą Art. 29 dnia 24 lipca 1998 r., s. 24; dokument roboczy WP 114 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty przez Grupę Roboczą Art. 29 w dniu 25 listopada 2005 r., s. 13.

[29] Dokument roboczy WP 12 „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych", przyjęty przez Grupę Roboczą Art. 29 dnia 24 lipca 1998 r., s. 24.

2.3.2. Przekazywanie danych konieczne dla zawarcia lub wykonania umowy zawartej między administratorem danych i osobą trzecią, w interesie osoby, której dane dotyczą (art. 26 ust. 1 lit. c))

Odstępstwo to może być stosowane na przykład gdy osoba, której dane dotyczą, jest beneficjentem międzynarodowego przelewu bankowego, lub gdy biuro podróży przekazuje przewoźnikowi lotniczemu szczegóły dotyczące rezerwacji lotu. Zastosowanie ma ponownie test konieczności, który w tym przypadku wymaga istnienia ścisłego i zasadniczego związku między interesem osoby, której dane dotyczą, i celem umowy.

2.3.3. Przekazywanie danych konieczne lub wymagane przez prawo z ważnych względów publicznych lub w celu ustanowienia, wykonania lub obrony tytułu prawnego (art. 26 ust. 1 lit. d))

Odstępstwo to może być stosowane na przykład gdy przedsiębiorstwo musi przekazać dane w ramach swojej linii obrony przed roszczeniem prawnym lub w kontekście dochodzenia roszczeń na drodze sądowej lub przed organem publicznym. Podobnie jak w przypadku dwóch poprzednich odstępstw, również to podlega testowi konieczności[30]: konieczne jest istnienie ścisłego powiązania z postępowaniem sądowym lub postępowaniem prawnym (w tym administracyjnym).

Zdaniem Grupy Roboczej Art. 29 odstępstwo to może zostać zastosowane tylko w przypadku zgodności z jakimikolwiek przepisami międzynarodowymi dotyczącymi współpracy w postępowaniach karnych lub cywilnych dotyczących kategorii przekazywania danych, zwłaszcza jeśli wynikają one z przepisów konwencji haskiej z dnia 18 marca 1970 r. („konwencja o przeprowadzaniu dowodów")[31].

2.3.4. Jednoznaczna wcześniejsza zgoda osoby, której dane dotyczą, na proponowane przekazanie danych (art. 26 ust. 1 lit. a))

Zgoda może stanowić podstawę przekazywania danych, należy jednak wziąć pod uwagę szereg okoliczności. Ponieważ zgoda musi być udzielona na „proponowane" przekazanie danych, wymaga to udzielenia wcześniejszej zgody na konkretne przekazanie (lub konkretną kategorię przekazania). W przypadku wyrażania zgody przez internet, Grupa Robocza Art. 29 zaleciła stosowanie pól do samodzielnego zaznaczania (zamiast domyślnie zaznaczonych

[30] Dokument roboczy WP 114 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty przez Grupę Roboczą Art. 29 w dniu 25 listopada 2005 r., s. 15. Na przykład w kontekście zatrudnienia odstępstwo to nie może być wykorzystane do przekazania wszystkich akt danego pracownika spółce dominującej grupy, mającej siedzibę w państwie trzecim, na potrzeby ewentualnych przyszłych postępowań prawnych.

[31] Konwencja haska o przeprowadzaniu dowodów za granicą w sprawach cywilnych i handlowych, otwarta do podpisu dnia 18 marca 1970 r., 23 U.S.T. 2555, 847 U.N.T.S. 241. Konwencja ta obejmuje m.in. wgląd do dokumentów przed wszczęciem postępowania lub wnioski składane przez organ sądowy jednego państwa do właściwego organu innego państwa w celu uzyskania dowodu przeznaczonego do wykorzystania w postępowaniu sądowym w państwie składającym wniosek.

pól)[32]. Ponieważ zgoda musi być jednoznaczna, jakiekolwiek wątpliwości co do tego, czy faktycznie została ona udzielona sprawiłyby, że odstępstwo nie miałoby zastosowania. Będzie to prawdopodobnie oznaczało, że liczne sytuacje, w których zgoda jest co najwyżej dorozumiana (na przykład kiedy dana osoba została poinformowana o przekazaniu danych i nie zgłosiła zastrzeżeń) nie kwalifikowałyby się do objęcia tym odstępstwem. Można by je jednak zastosować w przypadku, gdy podmiot przekazujący jest w bezpośrednim kontakcie z osobą, której dane dotyczą, gdy możliwe jest dostarczenie niezbędnych informacji i uzyskanie jednoznacznej zgody[33].

Ponadto, zgodnie z art. 2 lit. h) dyrektywy 95/46/WE, zgoda musi być dobrowolna, konkretna i świadoma. Zdaniem Grupy Roboczej Art. 29 pierwszy wymóg oznacza, że wszelka „presja" może unieważnić zgodę. Jest to szczególnie istotne w kontekście zatrudnienia, gdzie stosunek podporządkowania i wpisana w zatrudnienie zależność pracownika z reguły podważa możliwość powoływania się na zgodę[34]. Ogólnie rzecz biorąc, nie można uznać za ważną zgody wyrażonej przez osobę, której dane dotyczą, która nie miała sposobności dokonać faktycznego wyboru lub która została postawiona przed faktem dokonanym[35].

Niezwykle istotne jest, aby osoby, których dane dotyczą, były właściwie informowane z wyprzedzeniem o tym, że dane mogą zostać przekazane poza UE, do którego państwa trzeciego i na jakich warunkach (cel przekazania, tożsamość i szczegóły dotyczące odbiorcy(-ów) itd.). W informacjach tych należy uwzględnić konkretne ryzyko, że dane tych osób zostaną przekazane do państwa trzeciego niezapewniającego odpowiedniego stopnia ochrony[36]. Ponadto, jak zauważa Grupa Robocza Art. 29, wycofanie zgody przez osobę, której dane dotyczą, nie ma co prawda mocy wstecznej, ale co do zasady powinno uniemożliwić dalsze przetwarzanie danych osobowych[37]. W świetle tych ograniczeń Grupa Robocza Art. 29 uważa, że zgoda najprawdopodobniej nie zapewni odpowiednich

---

[32] Dokument roboczy WP 114 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty przez Grupę Roboczą Art. 29 dnia 25 listopada 2005 r., s. 10, z odniesieniem do dokumentu roboczego WP 90 „Opinia 5/2004 w sprawie niezamówionych materiałów do celów marketingu bezpośredniego zgodnie z art. 13 dyrektywy 2002/58/WE", przyjętego dnia 27 lutego 2004 r., pkt 3.2.

[33] Dokument roboczy WP 12 „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych", przyjęty przez Grupę Roboczą Art. 29 dnia 24 lipca 1998 r., s. 24.

[34] Dokument roboczy WP 48 „Opinia 8/2001 na temat przetwarzania danych osobowych w kontekście zatrudnienia", przyjęty przez Grupę Roboczą Art. 29 dnia 13 września 2001 r., s. 3, 23 i 26. Według Grupy Roboczej Art. 29 powoływanie się na zgodę powinno ograniczać się do przypadków, w których pracownik ma rzeczywiście wolny wybór i jest później w stanie wycofać zgodę bez poniesienia szkody. Zob. również dokument roboczy WP 114 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty przez Grupę Roboczą Art. 29 w dniu 25 listopada 2005 r., s. 11.

[35] Dokument roboczy WP 114 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty przez Grupę Roboczą Art. 29 w dniu 25 listopada 2005 r., s. 11. Zob. również dokument roboczy WP 66 „Opinia 6/2002 w sprawie przekazywania informacji na temat listy pasażerów i innych danych przez linie lotnicze Stanom Zjednoczonym", przyjęta dnia 24 października 2002 r.

[36] Dokument roboczy WP 12 „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych", przyjęty przez Grupę Roboczą Art. 29 dnia 24 lipca 1998 r., s. 24.

[37] Dokument roboczy WP 187 „Opinia 15/2011 na temat definicji zgody", przyjęty przez Grupę Roboczą Art. 29 dnia 13 lipca 2011 r., s. 9.

długoterminowych ram dla administratorów danych w przypadku przekazywania o charakterze strukturalnym[38].

2.4. Podsumowanie alternatywnych podstaw przekazywania danych osobowych

Jak wynika z powyższego, przedsiębiorstwa mają do dyspozycji szereg różnych alternatywnych narzędzi służących międzynarodowemu przekazywaniu danych do państw trzecich, które uznano za niezapewniające odpowiedniego stopnia ochrony w rozumieniu art. 25 ust. 2 dyrektywy 95/46/WE. W następstwie wyroku Schrems Grupa Robocza Art. 29 w szczególności sprecyzowała, że standardowe klauzule umowne lub wiążące reguły korporacyjne mogą być stosowane do przekazywania danych do USA, przy równoczesnej ocenie sytuacji przeprowadzanej przez Grupę oraz bez uszczerbku dla uprawnień organów ochrony danych do badania poszczególnych przypadków[39]. Branża zareagowała na ten wyrok na różne sposoby, między innymi decydując się na wykorzystywanie do przekazywania danych omawianych narzędzi alternatywnych[40].

Należy jednak zwrócić uwagę na dwa ważne czynniki. Po pierwsze należy przypomnieć, że niezależnie od konkretnej podstawy prawnej, przekazywanie danych do państwa trzeciego może być wykonane zgodnie z prawem wyłącznie jeśli dane zostały pierwotnie zebrane i przetworzone przez administratora danych mającego siedzibę w UE zgodnie z mającymi zastosowanie przepisami prawa krajowego transponującymi dyrektywę 95/46/WE. W dyrektywie wyraźnie stwierdza się, że przetwarzanie danych dokonywane przed ich przekazaniem, podobnie jak samo przekazywanie, musi odbywać się z pełnym poszanowaniem przepisów przyjętych przez państwa członkowskie zgodnie z innymi przepisami dyrektywy[41]. Po drugie, w przypadku braku decyzji Komisji w sprawie odpowiedniej ochrony danych osobowych odpowiedzialność za zapewnienie przekazywania danych z zastosowaniem wystarczających zabezpieczeń zgodnie z art. 26 ust. 2 dyrektywy spoczywa na administratorach danych. Ocenę taką należy przeprowadzić w świetle wszystkich okoliczności dotyczących danego przekazania danych. W szczególności zarówno standardowe klauzule umowne, jak i wiążące reguły korporacyjne stanowią, że jeżeli podmiot odbierający dane ma podstawy sądzić, że prawodawstwo mające zastosowanie w kraju odbiorcy może przeszkodzić mu w wypełnieniu swoich obowiązków, niezwłocznie informuje o tym podmiot przekazujący dane w UE. W takiej sytuacji to podmiot przekazujący dane odpowiada za rozważenie podjęcia stosownych środków niezbędnych do zapewnienia

---

[38] Dokument roboczy WP 114 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty przez Grupę Roboczą Art. 29 w dniu 25 listopada 2005 r., s. 11.

[39] Zob. oświadczenie Grupy Roboczej Art. 29 z dnia 16 października 2015 r. (przypis 8 powyżej).

[40] Wiele przedsiębiorstw wielonarodowych zadeklarowało, że do przekazywania danych do USA stosuje narzędzia alternatywne. Zob. np. oświadczenie Microsoftu (http://blogs.microsoft.com/on-the-issues/2015/10/06/a-message-to-our-customers-about-eu-us-safe-harbor/) lub Salesforce (http://www.salesforce.com/company/privacy/data-processing-addendum-faq.jsp). Inne firmy amerykańskie takie jak Oracle oświadczyły, że oferują klientom korzystającym z chmury możliwość przechowywania danych w Europie, nie są więc one przesyłane do przechowywania w innym miejscu: http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot

[41] Zob. motyw 60 i art. 25 ust. 1 dyrektywy 95/46/WE.

ochrony danych osobowych[42]. Mogą one obejmować szereg opcji, począwszy od środków technicznych, organizacyjnych, związanych z modelem biznesowym lub środków prawnych[43], aż po możliwość zawieszenia przekazywania danych lub rozwiązania umowy. Aby dane przekazanie spełniało wymogi art. 26 ust. 2 dyrektywy, podmioty przekazujące dane mogą więc być zmuszone, uwzględniając wszystkie okoliczności przekazywania danych, do stosowania dodatkowych zabezpieczeń w celu uzupełnienia tych wprowadzonych na mocy obowiązującej podstawy prawnej.

Ostateczną ocenę przestrzegania tych wymogów przeprowadzają każdorazowo organy ochrony danych w ramach wykonywania swoich funkcji nadzoru i egzekwowania prawa, w tym w kontekście zatwierdzania ustaleń umownych i wiążących reguł korporacyjnych lub na podstawie indywidualnych skarg. Niektóre organy ochrony danych wyraziły wątpliwości co do możliwości stosowania instrumentów takich jak standardowe klauzule umowne i wiążące reguły korporacyjne do transatlantyckich przepływów danych[44]. W swoim oświadczeniu wydanym w następstwie wyroku Schrems Grupa Robocza Art. 29 oświadczyła, że będzie kontynuować analizę wpływu wyroku na inne narzędzia do przekazywania danych[45]. Pozostaje to bez uszczerbku dla uprawnień organów ochrony danych do badania poszczególnych przypadków oraz do wykonywania ich uprawnień w celu ochrony osób fizycznych.

3. WPŁYW WYROKU SCHREMS NA DECYZJE W SPRAWIE ODPOWIEDNIEJ OCHRONY DANYCH OSOBOWYCH

W swoim wyroku Trybunał Sprawiedliwości nie kwestionuje kompetencji Komisji do stwierdzania, na mocy art. 25 ust. 6 dyrektywy 95/46/WE, czy państwo trzecie zapewnia odpowiedni stopień ochrony, o ile spełnione zostały wymogi określone przez Trybunał. Zgodnie z tymi wymogami wniosek z 2012 r. dotyczący ogólnego rozporządzenia o ochronie

[42] Zob. np. klauzula 5 załącznika do decyzji Komisji 2010/87/UE oraz dokument roboczy WP 154 w sprawie określenia ram dla struktury wiążących reguł korporacyjnych, przyjęty przez Grupę Roboczą Art. 29 dnia 24 czerwca 2008 r., s. 8.

[43] Zob. np. wytyczne wydane przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA): https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf.

[44] Zob. np. dokument konferencji ochrony danych przedstawiający stanowisko niemieckich organów ochrony danych na szczeblu federalnym i krajów związkowych, wydany dnia 26.10.2015 r.: https://www.datenschutz.hessen.de/ft-europa.htm#entry4521. W dokumencie tym podkreślono, że wyrok Schrems obejmuje „surowe wymogi merytoryczne", które muszą być przestrzegane zarówno przez Komisję, jak i krajowe organy ochrony danych, a także wskazano, że niemieckie organy ochrony danych będą oceniać legalność przekazywania danych na podstawie alternatywnych rozwiązań (standardowych klauzul umownych, wiążących reguł korporacyjnych) i nie będą udzielać nowych upoważnień do korzystania z tych narzędzi. Jednocześnie poszczególne niemieckie organy ochrony danych wydały jasne ostrzeżenia, że alternatywne narzędzia przekazywania danych są przedmiotem analizy prawnej. Zob. np. stanowiska wydane przez organy ds. ochrony danych kraju związkowego Schleswig-Hol:https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html i Nadrenii-Palatynatu: https://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf.

[45] Zob. oświadczenie Grupy Roboczej Art. 29 z dnia 16 października 2015 r. (przypis 8 powyżej).

danych osobowych[46], które ma zastąpić dyrektywę 95/46/WE, doprecyzowuje i wyszczególnia warunki, na jakich można przyjmować decyzje w sprawie odpowiedniej ochrony danych osobowych. W wyroku Schrems Trybunał sprecyzował również, że przyjęta przez Komisję decyzja w sprawie odpowiedniej ochrony danych osobowych jest wiążąca dla wszystkich państw członkowskich i ich organów, w tym organów ochrony danych, do czasu jej wycofania, uchylenia lub unieważnienia przez Trybunał Sprawiedliwości, który posiada wyłączną kompetencję w tym zakresie. Organy ochrony danych zachowują kompetencję do rozpatrywania skarg w rozumieniu art. 28 ust. 4 dyrektywy 95/46/WE odnośnie do zgodności przekazywania danych z wymogami określonymi w dyrektywie (zgodnie z wykładnią Trybunału Sprawiedliwości), lecz nie mogą dokonywać ostatecznych ustaleń. Państwa członkowskie muszą natomiast przewidzieć możliwość wniesienia sprawy do sądu krajowego, co może z kolei prowadzić do zaangażowania w sprawę Trybunału Sprawiedliwości poprzez wystosowanie do niego wniosku o wydanie orzeczenia w trybie prejudycjalnym na podstawie art. 267 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE).

Ponadto Trybunał Sprawiedliwości wyraźnie potwierdził, że odwołanie się przez państwo trzecie do systemu samocertyfikacji (jak w przypadku zasad ochrony prywatności w ramach „bezpiecznej przystani") nie wyklucza stwierdzenia, że stopień ochrony danych jest odpowiedni zgodnie z art. 25 ust. 6 dyrektywy 95/46/WE, o ile istnieją skuteczne mechanizmy wykrywania i nadzoru, które umożliwiają w praktyce identyfikowanie i karanie za wszelkie naruszenia przepisów o ochronie danych.

Zważywszy, że decyzja w sprawie bezpiecznego przekazywania danych nie zawierała wystarczających ustaleń w tym zakresie, Trybunał Sprawiedliwości stwierdził jej nieważność. Jest zatem jasne, że przekazywanie danych między UE a Stanami Zjednoczonymi nie może już być dokonywane na tej podstawie, tj. wyłącznie powołując się na przestrzeganie zasad ochrony prywatności w ramach „bezpiecznej przystani". Jako że przekazywanie danych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony (lub przynajmniej gdy nie zostało to ustalone decyzją Komisji na mocy art. 25 ust. 6 dyrektywy 95/46/WE), jest co do zasady zakazane[47], będzie ono zgodne z prawem wyłącznie wtedy, gdy podmiot przekazujący dane będzie mógł zastosować jedno z alternatywnych narzędzi opisanych powyżej w sekcji 2. W sytuacji braku decyzji w sprawie odpowiedniej ochrony danych osobowych zapewnienie, że spełniono warunki stosowania (jednego z) tych narzędzi w odniesieniu do danego przekazania danych, należy do podmiotu przekazującego dane (pod kontrolą organów ochrony danych).

---

[46] Wniosek Komisji Europejskiej 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). Zob. również rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego 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)0011 – C7-0025/2012 – 2012/0011(COD); dokument Rady: przygotowanie podejścia ogólnego 9565/15 w sprawie wniosku dotyczącego 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). Wniosek znajduje się obecnie na końcowym etapie prac legislacyjnych.

[47] Zob. motyw 57 dyrektywy 95/46/WE.

Zakres wyroku jest ograniczony do decyzji Komisji w sprawie bezpiecznego przekazywania danych. Każda z pozostałych decyzji w sprawie odpowiedniej ochrony danych osobowych[48] zawiera jednak ograniczenie uprawnień organów ochrony danych, które jest identyczne z art. 3 decyzji w sprawie bezpiecznego przekazywania danych, uznanej przez Trybunał za nieważną[49]. Komisja wyciągnie wnioski z wyroku i sporządzi wkrótce decyzję, która zostanie przyjęta zgodnie z obowiązującą procedurą komitetową i która zastąpi ten przepis we wszystkich dotychczasowych decyzjach w sprawie odpowiedniej ochrony danych osobowych. Ponadto Komisja będzie prowadzić regularną ocenę istniejących i przyszłych decyzji w sprawie odpowiedniej ochrony danych osobowych, w tym poprzez regularne wspólne przeglądy ich funkcjonowania wraz z właściwymi organami danego państwa trzeciego.

4. PODSUMOWANIE

Jak potwierdziła Grupa Robocza Art. 29, alternatywne narzędzia umożliwiające przepływy danych nadal mogą być stosowane przez przedsiębiorstwa do celów zgodnego z prawem przekazywania danych do państw trzecich, takich jak Stany Zjednoczone. Komisja uważa jednak, że kluczowym priorytetem są nadal odnowione, odpowiednie ramy regulujące przekazywanie danych osobowych do Stanów Zjednoczonych. Takie ramy są najbardziej kompleksowym rozwiązaniem zapewniającym skuteczną ciągłość ochrony danych osobowych obywateli europejskich, które są przekazywane do Stanów Zjednoczonych. Są one również najlepszym rozwiązaniem dla transatlantyckiego handlu, gdyż oferują łatwiejszy, mniej obciążający i dlatego mniej kosztowny mechanizm przekazywania, zwłaszcza dla MŚP.

Już w 2013 r. Komisja rozpoczęła negocjacje z rządem USA na temat nowego porozumienia w sprawie transatlantyckiego przekazywania danych na podstawie swoich 13 zaleceń[50]. Dokonał się znaczący postęp w zbliżaniu stanowisk obydwu stron, np. w sprawie wzmocnionego systemu monitorowania i egzekwowania zasad ochrony prywatności w ramach „bezpiecznej przystani" przez, odpowiednio, Departament Handlu USA oraz Federalną Komisję Handlu USA, większej przejrzystości dla konsumentów co do ich praw do ochrony danych, łatwiejszych i tańszych możliwości uzyskania odszkodowania w przypadku skarg oraz w sprawie jaśniejszych przepisów dotyczących dalszego przekazywania danych z przedsiębiorstw będących uczestnikami programu bezpiecznego przekazywania danych do przedsiębiorstw nim nieobjętych (np. do celów przetwarzania danych lub przetwarzania w ramach podwykonawstwa). W związku ze stwierdzeniem nieważności decyzji w sprawie bezpiecznego przekazywania danych Komisja zintensyfikowała rozmowy z rządem Stanów Zjednoczonych, aby zapewnić przestrzeganie wymogów prawnych sformułowanych przez Trybunał. Komisja chce zamknąć rozmowy i zrealizować ten cel w terminie trzech miesięcy.

---

[48] Dotychczas decyzje w sprawie odpowiedniej ochrony danych osobowych przyjęto odnośnie do następujących krajów: Andora, Argentyna, Kanada, Wyspy Owcze, Guernsey, Wyspa Man, Izrael, Jersey, Nowa Zelandia, Szwajcaria i Urugwaj. Zob.: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

[49] Zob. pkt 99-104 wyroku Schrems.

[50] Zob. przypis 4 powyżej.

Do czasu ustalenia odnowionych ram transatlantyckiego przekazywania danych, przedsiębiorstwa muszą stosować dostępne narzędzia alternatywne. Wariant ten nakłada jednak dodatkową odpowiedzialność na podmioty przekazujące dane, pod nadzorem organów ochrony danych.

Podmioty przekazujące dane, zamiast polegać - do celów przekazywania danych z UE - na stwierdzeniu przez Komisję, że dane państwo trzecie zapewnia odpowiedni stopień ochrony danych, są obecnie odpowiedzialne za sprawdzenie, czy w trakcie stosowania przez nie alternatywnych narzędzi dane osobowe są skutecznie chronione. Może to obejmować konieczność podjęcia odpowiednich środków.

Organy ochrony danych odgrywają w tym zakresie ważną rolę. Organy ochrony danych, jako główne organy odpowiedzialne za egzekwowanie praw podstawowych osób, których dane dotyczą, są odpowiedzialne za nadzorowanie przekazywania danych z UE do państw trzecich, jak również do tego uprawnione, przy zachowaniu pełnej niezależności. Komisja zachęca administratorów danych do współpracy z organami ochrony danych, co pomogłoby im skutecznie wykonywać swoje zadania w zakresie nadzoru. Komisja będzie nadal współpracować z Grupą Roboczą Art. 29 w celu zapewnienia jednolitego stosowania unijnych przepisów o ochronie danych.