18/PL

WP 254 rev. 01

**Grupa Robocza Art. 29**

# Odpowiedni stopień ochrony przekazywanych danych osobowych

Przyjęty dnia 28 listopada 2017 r.

Ostatnio zmieniony i przyjęty dnia 6 lutego 2018 r.

## Wprowadzenie

Grupa robocza organów ochrony danych UE[1] (Grupa Robocza Art. 29) opublikowała uprzednio dokument roboczy w sprawie przekazywania danych osobowych do państw trzecich (WP12)[2]. Wraz z zastąpieniem dyrektywy unijnym ogólnym rozporządzeniem o ochronie danych (RODO)[3] Grupa Robocza Art. 29 dokonała przeglądu dokumentu roboczego WP12, stanowiącego jej wcześniejsze wytyczne, aby zaktualizować go w kontekście nowych przepisów i najnowszego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (TSUE)[4].

Niniejszy dokument roboczy ma na celu aktualizację rozdziału pierwszego WP12 dotyczącego zasadniczej kwestii, jaką jest odpowiedni stopień ochrony danych osobowych w państwie trzecim, na terytorium lub w określonym sektorze lub określonych sektorach w tym państwie trzecim lub w organizacji międzynarodowej (zwanych dalej: „państwami trzecimi lub organizacjami międzynarodowymi"). Dokument ten będzie stale poddawany przeglądowi oraz, w razie potrzeby, aktualizowany w nadchodzących latach w oparciu o praktyczne doświadczenie zdobyte w trakcie stosowania RODO. Rozdział 2 („Stosowanie podejścia do państw, które ratyfikowały Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych") i rozdział 3 („Stosowanie podejścia do samoregulacji przemysłu") dokumentu roboczego WP12 należy zaktualizować na późniejszym etapie.

Niniejszy dokument roboczy dotyczy wyłącznie decyzji stwierdzających odpowiedni stopień ochrony, które są aktami wykonawczymi[5] Komisji Europejskiej zgodnie z art. 45 RODO. Inne aspekty przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych zostaną przeanalizowane w kolejnych dokumentach roboczych, które zostaną opublikowane oddzielnie (wiążące reguły korporacyjne, odstępstwa).

Celem niniejszego dokumentu jest dostarczenie wytycznych Komisji Europejskiej i Grupie Roboczej Art. 29 na podstawie RODO na potrzeby oceny stopnia ochrony danych osobowych w państwach trzecich i organizacjach międzynarodowych przez ustanowienie podstawowych zasad ochrony danych, które muszą być uwzględnione w ramach prawnych państwa trzeciego lub organizacji międzynarodowej w celu zapewnienia zasadniczej równoważności z ramami UE. Ponadto może on zapewnić wskazówki państwom trzecim i organizacjom międzynarodowym zainteresowanym uzyskaniem odpowiedniego stopnia ochrony. Zasady określone w niniejszym dokumencie roboczym nie są jednak skierowane bezpośrednio do administratorów danych ani podmiotów przetwarzających.

Niniejszy dokument składa się z czterech rozdziałów.

**Rozdział 1:** Ogólne informacje dotyczące pojęcia „odpowiedni stopień ochrony"

**Rozdział 2:** Aspekty proceduralne związane z ustaleniami dotyczącymi zapewnienia odpowiedniego stopnia ochrony na podstawie RODO

**Rozdział 3:** Ogólne zasady ochrony danych. Rozdział ten zawiera podstawowe ogólne zasady ochrony danych mające zapewnić, by stopień ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej był merytorycznie równoważny stopniowi określonemu w przepisach UE.

**Rozdział 4:** Niezbędne gwarancje dotyczące dostępu do danych w celu egzekwowania prawa i ze względów bezpieczeństwa narodowego mające na celu ograniczenie ingerencji w prawa podstawowe. W rozdziale tym określono niezbędne gwarancje dotyczące dostępu do danych w celu egzekwowania prawa i ze względów bezpieczeństwa narodowego zgodnie z wyrokiem TSUE w sprawie Schrems

---

[1] Utworzona zgodnie z art. 29 unijnej dyrektywy 95/46/WE o ochronie danych.

2 WP12, „Dokument roboczy: Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 unijnej dyrektywy o ochronie danych" przyjęty przez Grupę Roboczą w dniu 24 lipca 1998 r.

3 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG).

4 Uwzględniając wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, C-362/14.

[5] Więcej informacji na temat aktów wykonawczych można znaleźć w odpowiednich art. 45 ust. 3 i art. 93 ust. 2 RODO.

z 2015 r. i w oparciu o dokument roboczy Grupy Roboczej Art. 29 w sprawie niezbędnych gwarancji, przyjęty w 2016 r.

## Rozdział 1: Ogólne informacje dotyczące pojęcia „odpowiedni stopień ochrony”

W art. 45 ust. 1 RODO ustanowiono zasadę, że przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić jedynie wówczas, gdy państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony.

Pojęcie „odpowiedni stopień ochrony”, które istniało już na mocy dyrektywy 95/46, zostało doprecyzowane przez TSUE. W tym miejscu należy przypomnieć normę określoną przez TSUE w wyroku w sprawie Schrems, zgodnie z którą chociaż „stopień ochrony” w państwie trzecim musi być „merytorycznie równoważny” poziomowi gwarantowanemu w Unii, „środki, z jakich to państwo trzecie korzysta w tym względzie dla zapewnienia takiego stopnia ochrony, mogą różnić się od środków wprowadzonych w [Unii]”[6]. Dlatego też celem nie jest odzwierciedlenie punkt po punkcie prawodawstwa europejskiego, ale ustanowienie zasadniczych, tj. podstawowych, wymogów tego prawodawstwa.

Celem decyzji Komisji Europejskiej stwierdzających odpowiedni stopień ochrony jest formalne potwierdzenie ze skutkiem wiążącym dla państw członkowskich[7], że poziom ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej jest merytorycznie równoważny poziomowi ochrony danych osobowych w Unii Europejskiej[8]. Odpowiedni stopień ochrony można osiągnąć przez połączenie praw osób, których dane dotyczą, i obowiązków podmiotów, które przetwarzają dane lub sprawują kontrolę nad takim przetwarzaniem i nadzorem ze strony niezależnych organów. Przepisy o ochronie danych są jednak skuteczne tylko wtedy, gdy są możliwe do wyegzekwowania na drodze prawnej i przestrzegane w praktyce. Konieczne jest zatem rozważenie nie tylko treści przepisów mających zastosowanie do danych osobowych przekazywanych do państwa trzeciego lub organizacji międzynarodowej, ale także systemu stworzonego w celu zapewnienia skuteczności tych przepisów. Skuteczne mechanizmy egzekwowania prawa mają nadrzędne znaczenie dla skuteczności przepisów o ochronie danych.

W art. 45 ust. 2 RODO ustanowiono elementy, które Komisja Europejska uwzględnia podczas sprawdzania, czy stopień ochrony zapewniony w państwie trzecim lub organizacji międzynarodowej jest odpowiedni.

Na przykład Komisja uwzględnia praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie ustawodawstwo, istnienie i skuteczne działanie co najmniej jednego niezależnego organu nadzorczego oraz międzynarodowe zobowiązania zaciągnięte przez dane państwo trzecie lub daną organizację międzynarodową.

Jasne jest zatem, że jakakolwiek konstruktywna analiza odpowiedniej ochrony musi obejmować dwa podstawowe elementy: treść mających zastosowanie przepisów oraz środki służące zapewnieniu ich skutecznego stosowania. Do Komisji Europejskiej należy regularne sprawdzanie, czy obowiązujące przepisy są skuteczne w praktyce.

„Podstawowe” zasady ochrony „treści” danych i wymogi „proceduralne / dotyczące egzekwowania”, które mogłyby być postrzegane jako minimalny wymóg zapewnienia odpowiedniej ochrony, wynikają z Karty praw podstawowych Unii Europejskiej i RODO. Ponadto należy również uwzględnić inne umowy międzynarodowe dotyczące ochrony danych osobowych, np. Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[9].

---

[6] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, C-362/14, pkt 73, 74.

[7] Art. 288 ust. 2 TFUE.

[8] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, C-362/14, pkt 52.

9 Motyw 105 RODO.

Należy również zwrócić uwagę na ramy prawne dotyczące dostępu organów publicznych do danych osobowych. Dalsze wskazówki na ten temat znajdują się w dokumencie roboczym nr 237 (tj. w dokumencie w sprawie niezbędnych gwarancji)[10] dotyczącym gwarancji w kontekście nadzoru.

Przepisy ogólne dotyczące ochrony danych osobowych i prywatności w państwie trzecim nie są wystarczające. Wręcz przeciwnie, w ramach prawnych państwa trzeciego lub organizacji międzynarodowej należy zawrzeć przepisy szczególne regulujące konkretne potrzeby związane z praktycznie istotnymi aspektami prawa do ochrony danych osobowych. Przepisy te muszą być możliwe do wyegzekwowania na drodze prawnej.

## Rozdział 2: Aspekty proceduralne związane z ustaleniami dotyczącymi zapewnienia odpowiedniego stopnia ochrony na podstawie RODO

Aby Europejska Rada Ochrony Danych mogła wypełnić swoje zadanie polegające na doradzaniu Komisji Europejskiej zgodnie z art. 70 ust. 1 lit. s) RODO, powinna ona otrzymać odpowiednią dokumentację, w tym odpowiednią korespondencję i ustalenia dokonane przez Komisję Europejską. W przypadku gdy ramy prawne są złożone, dokumentacja taka powinna obejmować wszelkie sprawozdania przygotowane na temat stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej. W każdym razie informacje dostarczone przez Komisję Europejską powinny być wyczerpujące i powinny umożliwić Europejskiej Radzie Ochrony Danych dokonanie własnej oceny stopnia ochrony danych osobowych w państwie trzecim. Europejska Rada Ochrony Danych przedstawi w odpowiednim czasie opinię na temat ustaleń Komisji Europejskiej oraz wskaże ewentualne braki w ramach dotyczących odpowiedniego stopnia ochrony. Europejska Rada Ochrony Danych postara się również zaproponować zmiany lub poprawki, aby zaradzić ewentualnym brakom.

Zgodnie z art. 45 ust. 4 RODO do Komisji Europejskiej należy monitorowanie na bieżąco zmian mogących wpłynąć na obowiązywanie decyzji stwierdzającej odpowiedni stopień ochrony.

Art. 45 ust. 3 RODO stanowi, że okresowy przegląd musi odbywać się przynajmniej raz na cztery lata. Są to jednak ogólne ramy czasowe, które muszą zostać dostosowane do każdego państwa trzeciego lub organizacji międzynarodowej zgodnie z decyzją stwierdzającą odpowiedni stopień ochrony. W zależności od konkretnych okoliczności uzasadniony może być krótszy cykl przeglądu. Ponadto incydenty lub inne informacje na temat ram prawnych lub zmiany tych ram prawnych w danym państwie trzecim lub organizacji międzynarodowej mogą spowodować konieczność dokonania przeglądu przed planowanym terminem. Wydaje się również właściwe, aby pierwszy przegląd całkowicie nowej decyzji stwierdzającej odpowiedni stopień ochrony przeprowadzono dosyć szybko i stopniowo dostosowywano cykl przeglądu w zależności od wyniku.

Biorąc pod uwagę upoważnienie do przekazywania Komisji Europejskiej opinii na temat tego, czy państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub organizacja międzynarodowa nie zapewniają już odpowiedniego stopnia ochrony, Europejska Rada Ochrony Danych musi, w odpowiednim czasie, otrzymać istotne informacje dotyczące monitorowania przez Komisję Europejską istotnych zmian w tym państwie trzecim lub organizacji międzynarodowej. W związku z tym Europejska Rada Ochrony Danych powinna być na bieżąco informowana o każdym procesie przeglądu i misji przeglądowej w państwie trzecim lub organizacji międzynarodowej. Europejska Rada Ochrony Danych z zadowoleniem przyjęłaby zaproszenie do udziału w takich procesach i misjach przeglądowych.

Należy również zauważyć, że zgodnie z art. 45 ust. 5 RODO Komisja Europejska ma prawo uchylić, zmienić lub zawiesić istniejące decyzje stwierdzające odpowiedni stopień ochrony. W procedurze uchylania, zmieniania lub zawieszania powinna zatem uczestniczyć Europejska Rada Ochrony Danych, od której wymaga się przedstawienia opinii zgodnie z art. 70 ust. 1 lit. s).

Ponadto, jak obecnie uznano w art. 58 ust. 5 RODO i zgodnie z wyrokiem TSUE w sprawie Schrems, organy ochrony danych muszą mieć możliwość wszczęcia postępowania prawnego, jeżeli uznają, że zarzuty danej osoby dotyczące decyzji stwierdzającej odpowiedni stopień ochrony są zasadne: „W tym

[10] Dokument Roboczy 01/2016 w sprawie uzasadnienia ingerencji w podstawowe prawa do prywatności i ochrony danych poprzez środki nadzoru w przypadku przekazywania danych osobowych (niezbędne gwarancje europejskie), 16/EN WP 237, 13 kwietnia 2016 r.

względzie do krajowego ustawodawcy należy ustanowienie drogi prawnej umożliwiającej krajowemu organowi nadzorczemu podniesienie zarzutów, które uważa on za zasadne, przed sądami krajowymi, po to, aby te ostatnie, jeśli podzielają wątpliwości tego organu co do ważności decyzji Komisji, wystąpiły z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w celu zbadania ważności tej decyzji”[11].

[11] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, C-362/14, pkt 65.

**Rozdział 3: Ogólne zasady ochrony danych mające zapewnić, by stopień ochrony danych osobowych w państwie trzecim, na terytorium lub w określonym sektorze lub określonych sektorach w tym państwie trzecim lub organizacji międzynarodowej był merytorycznie równoważny stopniowi określonemu w przepisach UE**

**System państwa trzeciego lub organizacji międzynarodowej musi zawierać następujące podstawowe zasady i mechanizmy ochrony treści oraz zasady i mechanizmy proceduralne / dotyczące wdrażania w odniesieniu do danych osobowych:**

**A. <u>Zasady dotyczące treści:</u>**

**1) Pojęcia**

Powinny istnieć podstawowe pojęcia lub zasady dotyczące ochrony danych osobowych. Nie muszą one odzwierciedlać terminologii RODO, ale powinny odzwierciedlać pojęcia zawarte w europejskim prawie w dziedzinie ochrony danych i być z nimi spójne. Przykładowo RODO zawiera następujące istotne pojęcia: „dane osobowe", „przetwarzanie danych osobowych", „administrator danych", „podmiot przetwarzający", „odbiorca" i „dane wrażliwe".

**2) Podstawy zgodnego z prawem i rzetelnego przetwarzania danych do prawnie uzasadnionych celów**

Dane muszą być przetwarzane w sposób zgodny z prawem, rzetelny i prawnie uzasadniony.

Należy odpowiednio jasno określić uzasadnione podstawy, w ramach których można zgodnie z prawem, rzetelnie i w sposób prawnie uzasadniony przetwarzać dane osobowe. W przepisach unijnych przewidziano kilka takich uzasadnionych prawnie podstaw, w tym np. przepisy prawa krajowego, zgodę osoby, której dane dotyczą, wykonanie umowy lub prawnie uzasadniony interes realizowany przez administratora lub przez stronę trzecią, który nie jest nadrzędny wobec interesów osoby fizycznej.

**3) Zasada ograniczenia celu**

Dane powinny być przetwarzane w określonym celu, a następnie wykorzystywane tylko w takim zakresie, w jakim nie jest to niezgodne z celem przetwarzania danych.

**4) Zasada jakości danych oraz proporcjonalności**

Dane powinny być prawidłowe i w razie potrzeby uaktualniane. Dane powinny być adekwatne, stosowne i niewykraczające poza cele, w których są przetwarzane.

**5) Zasada zatrzymywania danych**

Co do zasady dane nie powinny być przechowywane przez okres dłuższy, niż jest to niezbędne do celów, w których te dane osobowe są przetwarzane.

**6) Zasada bezpieczeństwa i poufności**

Każdy podmiot przetwarzający dane osobowe powinien zagwarantować przetwarzanie danych osobowych w sposób zapewniający bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem

lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Poziom bezpieczeństwa powinien uwzględniać stan wiedzy technicznej oraz związane z nim koszty.

### 7) Zasada przejrzystości

Każda osoba fizyczna powinna być informowana o wszystkich głównych elementach przetwarzania jej danych osobowych w jasnej, łatwo dostępnej, zwięzłej, przejrzystej i zrozumiałej formie. Informacje takie powinny obejmować cel przetwarzania danych, tożsamość administratora danych, przyznane mu prawa oraz inne informacje w zakresie, w jakim jest to niezbędne do zapewnienia rzetelności. W pewnych okolicznościach możliwe są wyjątki od tego prawa do informacji, np. w celu ochrony postępowania przygotowawczego, ze względu na bezpieczeństwo narodowe, niezależność sądów i dobro postępowania sądowego lub z uwagi na inne ważne cele leżące w ogólnym interesie publicznym, jak w przypadku art. 23 RODO.

### 8) Prawo dostępu, prawo do sprostowania i usunięcia danych oraz prawo do sprzeciwu

Osoba, której dane dotyczą, powinna mieć prawo do uzyskania potwierdzenia, czy jej dane osobowe są przetwarzane, oraz prawo dostępu do swoich danych, w tym do otrzymania kopii wszystkich danych jej dotyczących, które są przetwarzane.

Osoba, której dane dotyczą, powinna mieć prawo do uzyskania, w stosownych przypadkach, sprostowania swoich danych osobowych, z określonych powodów, np. w przypadku wykazania, że są one nieprawidłowe lub niekompletne, oraz prawo do usunięcia swoich danych osobowych, np. gdy ich przetwarzanie nie jest już konieczne lub jest niezgodne z prawem.

Osoba, której dane dotyczą, powinna mieć również prawo do wniesienia w dowolnym momencie, z ważnych i prawnie uzasadnionych przyczyn związanych z jej szczególną sytuacją, sprzeciwu wobec przetwarzania jej danych osobowych na szczególnych warunkach określonych w przepisach prawnych państwa trzeciego. W RODO warunki te obejmują np. przypadki, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub gdy jest niezbędne do sprawowania władzy publicznej powierzonej administratorowi lub gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

Wykonanie tych praw nie powinno być nadmiernie uciążliwe dla osoby, której dane dotyczą. Możliwe ograniczenia tych praw mogą istnieć np. w celu ochrony postępowania przygotowawczego, ze względu na bezpieczeństwo narodowe, niezależność sądów i dobro postępowania sądowego lub z uwagi na inne ważne cele leżące w ogólnym interesie publicznym, jak w przypadku art. 23 RODO.

### 9) Ograniczenia dotyczące dalszego przekazywania danych

Dalsze przekazywanie danych osobowych przez pierwotnego odbiorcę pierwotnego przekazywania danych powinno być dozwolone tylko wtedy, gdy dalszy odbiorca (tj. odbiorca dalszego przekazywania) również podlega przepisom (w tym przepisom umownym) zapewniającym odpowiedni stopień ochrony i przestrzega odpowiednich instrukcji podczas przetwarzania danych w imieniu administratora danych. Dalsze przekazywanie danych nie może podważać stopnia ochrony osób fizycznych, których dane są przekazywane. Pierwotny odbiorca danych przekazywanych z UE jest odpowiedzialny za zapewnienie odpowiednich zabezpieczeń w odniesieniu do dalszego przekazywania danych w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony. Takie dalsze przekazywanie danych powinno być prowadzone jedynie w ograniczonych i określonych celach oraz dopóki istnieje podstawa prawna takiego przetwarzania.

## B. Przykłady dodatkowych zasad dotyczących treści, które mają być stosowane do konkretnych rodzajów przetwarzania:

### 1) Szczególne kategorie danych osobowych

Jeżeli przetwarzanie obejmuje „szczególne kategorie danych osobowych", powinny istnieć szczególne zabezpieczenia[12]. Kategorie te powinny odzwierciedlać kategorie określone w art. 9 i 10 RODO. Ochronę taką należy zapewnić przez wprowadzenie bardziej rygorystycznych wymogów dotyczących przetwarzania danych osobowych, takich jak np. udzielenie przez osobę, której dane dotyczą, wyraźnej zgody na przetwarzanie danych, lub poprzez dodatkowe środki bezpieczeństwa.

### 2) Marketing bezpośredni

W przypadku gdy dane są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, powinna mieć możliwość wniesienia w dowolnym momencie i bez ponoszenia żadnych kosztów sprzeciwu wobec przetwarzania jej danych osobowych do takich celów.

### 3) Zautomatyzowane podejmowanie decyzji i profilowanie

Decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu (zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach), w tym profilowaniu, które wywołują skutki prawne lub istotnie wpływają na osobę, której dane dotyczą, mogą być podejmowane jedynie pod pewnymi warunkami określonymi w ramach prawnych państwa trzeciego. W ramach europejskich warunki takie obejmują m.in. potrzebę uzyskania wyraźnej zgody osoby, której dane dotyczą, lub konieczność uzyskania takiej decyzji do celów zawarcia umowy. Jeżeli decyzja nie jest zgodna z takimi warunkami określonymi w ramach prawnych państwa trzeciego, osoba, której dane dotyczą, powinna mieć prawo do niepodlegania takiej decyzji. Przepisy państwa trzeciego powinny w każdym przypadku przewidywać niezbędne zabezpieczenia, w tym prawo do uzyskania informacji o konkretnych powodach podjęcia danej decyzji oraz o jej logice, prawo do skorygowania nieprawidłowych lub niekompletnych informacji oraz prawo do zakwestionowania decyzji, jeżeli została ona podjęta na podstawie błędnego stanu faktycznego.

## C. Mechanizmy proceduralne i mechanizmy egzekwowania prawa:

**Mimo że środki, z których korzysta państwo trzecie w celu zapewnienia odpowiedniego stopnia ochrony mogą się różnić od środków stosowanych w Unii Europejskiej[13], system zgodny z systemem europejskim musi charakteryzować się istnieniem następujących elementów.**

### 1) Właściwy niezależny organ nadzorczy

Powinien istnieć co najmniej jeden niezależny organ nadzorczy odpowiedzialny za monitorowanie, zapewnianie i egzekwowanie zgodności z przepisami dotyczącymi ochrony danych osobowych i prywatności w państwie trzecim. Organ nadzorczy powinien działać w sposób w pełni niezależny i bezstronny podczas wypełniania swoich zadań i wykonywania swoich uprawnień oraz w toku tych działań nie powinien zwracać się o żadne instrukcje ani ich przyjmować. W tym kontekście organ nadzorczy powinien dysponować wszystkimi niezbędnymi i dostępnymi uprawnieniami i funkcjami w celu zapewnienia przestrzegania praw do ochrony danych osobowych i propagowania wiedzy na

[12] Takie szczególne kategorie zostały również określone jako „dane wrażliwe" w motywie 10 RODO.

[13] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, C-362/14, pkt 74.

ten temat. Należy również zastanowić się nad personelem i budżetem organu nadzorczego. Organ nadzorczy powinien być również w stanie prowadzić dochodzenia z urzędu.

2) **System ochrony danych musi zapewnić odpowiedni stopień zgodności**

System państwa trzeciego powinien zapewniać wysoki stopień rozliczalności i świadomości wśród administratorów danych oraz podmiotów przetwarzających dane osobowe w ich imieniu w zakresie ich obowiązków, zadań i zakresu odpowiedzialności oraz wśród osób, których dane dotyczą, w zakresie ich praw i sposobów ich wykonywania. Istnienie skutecznych i zniechęcających sankcji może odegrać ważną rolę w zapewnieniu poszanowania przepisów, podobnie jak sprawić to mogą systemy bezpośredniej weryfikacji przez organy, audytorów lub niezależnych inspektorów ochrony danych.

3) **Rozliczalność**

Ramy ochrony danych osobowych obowiązujące w państwie trzecim powinny zobowiązywać administratorów danych lub podmioty przetwarzające dane osobowe w ich imieniu do przestrzegania tych ram oraz nakładać na nich obowiązek, by byli w stanie wykazać zgodność z ramami, w szczególności właściwemu organowi nadzorczemu. Tego rodzaju środki mogą obejmować m.in. ocenę skutków w zakresie ochrony danych, prowadzenie rejestrów lub dzienników czynności przetwarzania danych przez odpowiedni okres, wyznaczenie urzędnika ds. ochrony danych lub uwzględnienie ochrony danych w fazie projektowania lub domyślnej ochrony danych.

4) **System ochrony danych musi zapewniać wsparcie i pomoc poszczególnym osobom, których dane dotyczą, w wykonywaniu przysługujących im praw i korzystaniu z odpowiednich mechanizmów dochodzenia roszczeń**

Osoba fizyczna powinna mieć możliwość skorzystania ze środków ochrony prawnej w celu szybkiego i skutecznego egzekwowania swoich praw, bez nadmiernych kosztów oraz w celu zapewnienia przestrzegania tych praw. W tym celu muszą istnieć mechanizmy nadzoru pozwalające na niezależne rozpatrywanie skarg oraz umożliwiające identyfikowanie w praktyce wszelkich naruszeń prawa do ochrony danych osobowych i poszanowania życia prywatnego oraz nakładanie kar za takie naruszenia.

W przypadku nieprzestrzegania przepisów osobie, której dane dotyczą, należy zapewnić skuteczne administracyjne i sądowe środki zaskarżenia, w tym odszkodowanie z tytułu szkód poniesionych w wyniku niezgodnego z prawem przetwarzania jej danych osobowych. Jest to najważniejszy element, który wiąże się z systemem niezależnego orzekania lub arbitrażu, umożliwiający wypłatę odszkodowania i, w stosownych przypadkach, nałożenie sankcji.

**Rozdział 4: Niezbędne gwarancje w państwach trzecich dotyczące dostępu do danych w celu egzekwowania prawa i ze względów bezpieczeństwa narodowego mające na celu ograniczenie ingerencji w prawa podstawowe**

Oceniając, czy stopień ochrony jest odpowiedni, na mocy art. 45 ust. 2 lit. a) Komisja jest zobowiązana uwzględnić „odpowiednie ustawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz dostępu organów publicznych do danych osobowych, a także wdrażanie takiego ustawodawstwa (...)".

W wyroku w sprawie Schrems TSUE zauważył, że „wyrażenie »odpowiedni stopień ochrony« należy rozumieć jako wymagające od tego państwa trzeciego skutecznego zapewnienia, ze względu na jego ustawodawstwo wewnętrzne lub zobowiązania międzynarodowe, poziomu ochrony podstawowych praw i wolności merytorycznie równoważnego poziomowi gwarantowanemu w Unii na mocy dyrektywy 95/46 w związku z kartą". Jakkolwiek środki, z jakich to państwo trzecie korzysta w tym względzie, mogą różnić się od środków wprowadzonych w Unii, środki te muszą być jednak w praktyce skuteczne[14].

W tym kontekście Trybunał zauważył również krytycznie, że poprzednia decyzja w sprawie „bezpiecznej przystani" „nie zawiera żadnego stwierdzenia dotyczącego istnienia w Stanach Zjednoczonych reguł o charakterze ogólnopaństwowym służących do ograniczenia ewentualnych ingerencji w prawa podstawowe osób, których dane zostały przekazane z Unii do Stanów Zjednoczonych, ingerencji, które organy państwowe tego kraju mogłyby dokonywać przy okazji dążenia do realizacji uzasadnionego prawem celu, takiego jak bezpieczeństwo narodowe".

Grupa Robocza Art. 29 określiła w dokumencie roboczym WP237 przyjętym w dniu 13 kwietnia 2016 r. niezbędne gwarancje odzwierciedlające orzecznictwo TSUE i orzecznictwo związane z Konwencją o ochronie praw człowieka i podstawowych wolności w obszarze nadzoru. Chociaż zalecenia sformułowane w WP237 pozostają w mocy i powinny być brane pod uwagę przy ocenie, czy państwo trzecie zapewnia odpowiedni stopień ochrony w obszarze nadzoru, stosowanie tych gwarancji może się różnić w obszarach dostępu do danych w celu egzekwowania prawa i ze względów bezpieczeństwa narodowego. Aby poniższe cztery gwarancje zostały uznane za odpowiednie, muszą być jednak przestrzegane przez wszystkie państwa trzecie w odniesieniu do dostępu do danych, zarówno ze względów bezpieczeństwa narodowego, jak i do celów egzekwowania prawa:

1) **Przetwarzanie powinno opierać się na jasnych, precyzyjnych i dostępnych przepisach (podstawa prawna).**

2) **Należy wykazać konieczność i proporcjonalność w odniesieniu do zamierzonych prawnie uzasadnionych celów.**

3) **Przetwarzanie danych musi podlegać niezależnemu nadzorowi.**

4) **Osoby fizyczne muszą mieć dostęp do skutecznych środków ochrony prawnej.**

[14] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, C-362/14, pkt 74.