Zalecenia 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy 2016/680

przyjęte 2 lutego 2021 r.

Spis treści

Europejska Rada Ochrony Danych,

uwzględniając art. 51 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJMUJE NINIEJSZE ZALECENIA:

1. WPROWADZENIE

1. Grupa Robocza Art. 29 opublikowała dokument roboczy[2] w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy ogólnego rozporządzenia o ochronie danych (RODO)[3]. Dokument ten został zatwierdzony przez Europejską Radę Ochrony Danych (EROD) na pierwszej sesji plenarnej.

2. Zgodnie z deklaracją nr 21 dołączoną do Traktatu z Lizbony konieczne może okazać się wprowadzenie zasad szczególnych dotyczących ochrony danych osobowych i swobodnego przepływu tych danych w dziedzinach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, zapewnianej na podstawie art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), ze względu na szczególny charakter tych dziedzin.

3. Na tej podstawie prawodawca UE przyjął dyrektywę (UE) 2016/680 ustanawiającą przepisy szczególne dotyczące przetwarzania danych osobowych przez właściwe organy do celów **zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom**.

4. W tym kontekście dyrektywa 2016/680 określa podstawy umożliwiające przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych. Jedną z podstaw tego rodzaju przekazywania danych jest decyzja Komisji Europejskiej stwierdzająca, że dane państwo trzecie lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony.

[1] Dz.U. L 119 z 4.5.2016, s. 89.
[2] Dokument WP254.rev01 przyjęty przez Grupę Roboczą Art. 29 w dniu 28 listopada 2017 r., ostatnio zmieniony i przyjęty w dniu 6 lutego 2018 r. Stanowi on aktualizację rozdziału I dokumentu roboczego WP12 „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 unijnej dyrektywy o ochronie danych" (ang. Transfer of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive) przyjętego przez Grupę Roboczą Art. 29 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), Dz.U. L 119 z 4.5.2016, s. 1.

5. Dokument roboczy WP254.rev01 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych ma na celu przekazanie Komisji Europejskiej wytycznych dotyczących stopnia ochrony danych osobowych w państwach trzecich i organizacjach międzynarodowych na podstawie RODO, natomiast niniejszy dokument ma na celu zapewnienie podobnych wytycznych na podstawie dyrektywy 2016/680. W tym kontekście określa się w nim podstawowe zasady ochrony danych, które muszą być zawarte w ramach prawnych państwa trzeciego lub organizacji międzynarodowej w celu zapewnienia merytorycznej równoważności z ramami UE w zakresie dyrektywy 2016/680 (tj. w odniesieniu do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar). Ponadto niniejszy dokument może zapewnić wskazówki państwom trzecim i organizacjom międzynarodowym zainteresowanym uzyskaniem odpowiedniego stopnia ochrony.

6. Niniejszy dokument dotyczy wyłącznie decyzji stwierdzających odpowiedni stopień ochrony. Są to akty wykonawcze Komisji Europejskiej przyjmowane zgodnie z art. 36 ust. 3 dyrektywy 2016/680.

2. POJĘCIE ODPOWIEDNIEGO STOPNIA OCHRONY

7. Dyrektywa 2016/680 określa zasady przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych w zakresie, w jakim takie przekazywanie danych wchodzi w zakres jej stosowania. Przepisy dotyczące międzynarodowego przekazywania danych osobowych określono w rozdziale V dyrektywy 2016/680, w szczególności w jej art. 35–39.

8. Na podstawie art. 36 dyrektywy 2016/680 przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, jeżeli państwo trzecie, terytorium lub przynajmniej jeden sektor w tym państwie trzecim, lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Z orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (TSUE)[4] wynika, że przepis ten należy interpretować w świetle art. 35 dyrektywy 2016/680, zatytułowanego „Ogólne zasady przekazywania danych osobowych", który stanowi, że „wszystkie przepisy [rozdziału V tej dyrektywy] stosuje się w celu zapewnienia, by stopień ochrony osób fizycznych zapewniony niniejszą dyrektywą nie został obniżony".

9. W przypadku gdy Komisja Europejska zdecydowała, że taki odpowiedni stopień ochrony jest zapewniony, przekazywanie danych osobowych do tego państwa trzeciego, terytorium, sektora lub organizacji międzynarodowej może nastąpić bez konieczności uzyskania specjalnego zezwolenia, z wyjątkiem sytuacji, w której inne państwo członkowskie, od którego uzyskano dane, musi udzielić zezwolenia na przekazanie, jak przewidziano w art. 35 i 36 oraz w motywie 66 dyrektywy 2016/680. Nie wpływa to na konieczność zapewnienia, by przetwarzanie danych przez organy zainteresowanych państw członkowskich było zgodne z przepisami krajowymi przyjętymi na podstawie dyrektywy (UE) 2016/680.

[4] Sprawa C-311/18, Data Protection Commissioner przeciwko Facebook Ireland Ltd i Maximillian Schrems, wyrok z dnia 16 lipca 2020 r., ECLI:EU:C:2020:559, pkt 92 (Schrems II).

10. Pojęcie „odpowiedniego stopnia ochrony", które istniało już na mocy dyrektywy 95/46/WE[5] i decyzji ramowej Rady 2008/977/WSiSW[6], zostało doprecyzowane w tym kontekście przez TSUE, a ostatnio w ramach RODO.

11. Jak wyjaśnił TSUE, o ile stopień ochrony w państwie trzecim musi być merytorycznie równoważny temu gwarantowanemu w UE, „środki, z jakich to państwo trzecie korzysta w tym względzie dla zapewnienia takiego stopnia ochrony, mogą różnić się od środków wprowadzonych w Unii", ale „środki te powinny w praktyce skutecznie zapewniać ochronę"[7]. W związku z powyższym norma dotycząca odpowiedniego stopnia ochrony danych nie wymaga dokładnego powielania przepisów unijnych, ale ustanowienia zasadniczych, tj. podstawowych, wymogów określonych w tych przepisach.

12. W tym kontekście Trybunał wyjaśnił również, że decyzja Komisji stwierdzająca odpowiedni stopień ochrony powinna zawierać wszelkie stwierdzenia dotyczące istnienia w państwie trzecim przepisów służących ograniczeniu ewentualnych ingerencji w prawa podstawowe osób, których dane zostały przekazane z Unii do tego państwa trzeciego, ingerencji, których organy państwowe tego kraju *mogłyby* dokonywać przy okazji dążenia do realizacji uzasadnionego prawem celu, takiego jak bezpieczeństwo narodowe[8].

13. Celem decyzji Komisji Europejskiej stwierdzających odpowiedni stopień ochrony jest formalne potwierdzenie ze skutkiem wiążącym dla państw członkowskich[9], w tym dla ich właściwych organów ochrony danych[10], że stopień ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej jest merytorycznie równoważny stopniowi ochrony danych osobowych w Unii Europejskiej. Państwo trzecie powinno dawać gwarancje zapewniające odpowiedni stopień ochrony, zasadniczo odpowiadający stopniowi przewidzianemu w Unii, w szczególności gdy dane są przetwarzane w jednym konkretnym sektorze lub większej ich liczbie[11].

14. 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[12].

---

[5] 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.

[6] Decyzja ramowa 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, Dz.U. L 350 z 30.12.2008, s. 60.

[7] Sprawa C−362/14, Maximillian Schrems przeciwko Data Protection Commissioner, wyrok z dnia 6 października 2015 r., ECLI:EU:C:2015:650, pkt 73 i 74 (Schrems I).

[8] Schrems I, pkt 88.

[9] Art. 288 akapit drugi TFUE.

[10] Schrems I, pkt 52.

[11] Motyw 67 dyrektywy 2016/680.

[12] Schrems I, pkt 72–74 oraz opinia TSUE 1/15 w sprawie projektu umowy między Kanadą a Unią Europejską, z dnia 26 lipca 2017 r., ECLI:EU:C:2017:592 (opinia 1/15), pkt 134: „Rzeczone prawo do ochrony danych osobowych wymaga w szczególności, by ciągłość wysokiego poziomu ochrony praw i wolności przyznanego

3. ASPEKTY PROCEDURALNE ZWIĄZANE Z USTALENIAMI DOTYCZĄCYMI ZAPEWNIENIA ODPOWIEDNIEGO STOPNIA OCHRONY NA PODSTAWIE DYREKTYWY 2016/680

15. Aby EROD mogła wypełnić swoje zadanie polegające na doradzaniu Komisji Europejskiej zgodnie z art. 51 ust. 1 lit. g) dyrektywy 2016/680, powinna otrzymać odpowiednią dokumentację, w tym odpowiednią korespondencję i ustalenia dokonane przez Komisję Europejską. Bezwzględnie konieczne jest, aby wszelkie istotne dokumenty były przekazywane EROD z odpowiednim wyprzedzeniem, w tłumaczeniu na język angielski, aby przed ostatecznym przyjęciem decyzji stwierdzającej odpowiedni stopień ochrony możliwe było przeprowadzenie merytorycznych i owocnych dyskusji. W przypadku gdy ramy prawne są złożone, dokumentacja taka powinna obejmować wszelkie przygotowane sprawozdania 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 EROD dokonanie oceny analizy przeprowadzonej przez Komisję w zakresie stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej.

16. EROD przedstawi w odpowiednim czasie opinię na temat ustaleń Komisji Europejskiej, wskazując możliwe braki w przepisach dotyczących odpowiedniego stopnia ochrony i w razie konieczności formułując ewentualne zalecenia.

17. Zgodnie z art. 36 ust. 4 dyrektywy 2016/680 do Komisji Europejskiej należy monitorowanie na bieżąco zmian mogących wpłynąć na obowiązywanie decyzji stwierdzającej odpowiedni stopień ochrony.

18. Art. 36 ust. 3 dyrektywy 2016/680 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.

19. Biorąc pod uwagę upoważnienie EROD 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, EROD 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 EROD powinna być na bieżąco informowana o każdym procesie przeglądu i misji przeglądowej w państwie trzecim lub organizacji międzynarodowej. EROD zaleca zapraszanie jej

prawem Unii była zapewniona w razie przekazywania danych osobowych z Unii do państwa trzeciego. Nawet jeżeli środki mające na celu zapewnienie takiego stopnia ochrony mogą różnić się od środków wprowadzonych w Unii w celu zagwarantowania poszanowania wymogów płynących z prawa Unii, to jednak środki te powinny w praktyce skutecznie zapewniać ochronę merytorycznie równoważną ochronie gwarantowanej w Unii".

do udziału w tych procesach przeglądu i misjach, jak przewidziano w decyzji w sprawie Tarczy Prywatności i w decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do Japonii.

20. Należy również zauważyć, że zgodnie z art. 36 ust. 5 dyrektywy 2016/680 Komisja Europejska ma prawo uchylić, zmienić lub zawiesić wydane decyzje stwierdzające odpowiedni stopień ochrony, jeżeli państwo trzecie lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony. Procedura uchylenia, zmiany lub zawieszenia wymaga zwrócenia się do EROD o wydanie opinii zgodnie z art. 51 ust. 1 lit. g) dyrektywy 2016/680.

21. Ponadto, bez uszczerbku dla uprawnień organów prokuratorskich, organy nadzorcze powinny również mieć uprawnienie do wnoszenia naruszeń tej dyrektywy przed organy sądowe lub do udziału w postępowaniu sądowym[13]. W szczególności z wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie Schrems I wynika, że organy ochrony danych muszą mieć możliwość wszczęcia postępowania sądowego przed sądami krajowymi, jeżeli uznają, że zarzuty danej osoby przeciwko decyzji stwierdzającej odpowiedni stopień ochrony są zasadne[14]. W wyroku w sprawie Schrems II potwierdzono tę ocenę[15].

4. UNIJNE NORMY DOTYCZĄCE ODPOWIEDNIEGO STOPNIA OCHRONY W ZAKRESIE WSPÓŁPRACY POLICYJNEJ I WSPÓŁPRACY WYMIARÓW SPRAWIEDLIWOŚCI W SPRAWACH KARNYCH

22. Co do istoty decyzje stwierdzające odpowiedni stopień ochrony powinny koncentrować się na ocenie obowiązującego prawodawstwa danego państwa trzeciego jako całości, w teorii i praktyce, w świetle kryteriów oceny określonych w art. 36 dyrektywy 2016/680. System państwa trzeciego lub organizacji międzynarodowej musi zawierać następujące podstawowe ogólne zasady i mechanizmy proceduralne w zakresie ochrony danych osobowych, jak również zasady i mechanizmy egzekwowania tej ochrony.

23. W art. 36 ust. 2 dyrektywy 2016/680 ustanowiono elementy, które Komisja Europejska uwzględnia podczas sprawdzania, czy stopień ochrony zapewniony w państwie trzecim lub organizacji międzynarodowej jest odpowiedni.

24. W szczególności Komisja bierze pod uwagę praworządność, poszanowanie praw człowieka i podstawowych wolności[16], odpowiednie przepisy, a także wdrażanie tych przepisów, skuteczne

[13] Zob. art. 47 ust. 5 dyrektywy 2016/680 i jej motyw 82.

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

[15] Zob. Schrems II, pkt 120: „nawet w przypadku wydania przez Komisję decyzji stwierdzającej odpowiedni stopień ochrony właściwy krajowy organ nadzorczy, do którego dana osoba wniosła skargę dotyczącą ochrony jej praw i wolności w związku z przetwarzaniem dotyczących jej danych osobowych, powinien mieć możliwość zbadania w sposób całkowicie niezależny tego, czy przekazywanie tych danych spełnia wymogi ustanowione w RODO oraz, w odpowiednim przypadku, wniesienia do sądów krajowych skargi mającej na celu skierowanie przez te sądy, jeśli podzielą one wątpliwości tego organu co do ważności tej decyzji stwierdzającej odpowiedni stopień ochrony, odesłania prejudycjalnego mającego doprowadzić do przeanalizowania tej ważności".

[16] Oceniając ramy prawne państwa trzeciego, należy wziąć pod uwagę możliwość nałożenia kary śmierci lub jakiejkolwiek innej formy okrutnego lub nieludzkiego traktowania na podstawie danych przekazywanych z UE. Gdyby taka kara lub takie traktowanie były przewidziane w prawie państwa trzeciego, w ramach prawnych

i egzekwowalne prawa osób, których dane dotyczą, oraz prawo osób, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia, istnienie i skuteczne funkcjonowanie co najmniej jednego niezależnego organu nadzorczego oraz zobowiązania międzynarodowe zaciągnięte przez państwo trzecie lub organizację międzynarodową.

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

26. Podstawowe ogólne zasady oraz wymogi proceduralne w zakresie ochrony danych i dotyczące egzekwowania tej ochrony, które można by postrzegać jako minimalny wymóg zapewnienia odpowiedniego stopnia ochrony, wynikają z Karty praw podstawowych UE i dyrektywy 2016/680. Przepisy ogólne dotyczące ochrony danych osobowych i prywatności w państwie trzecim nie są wystarczające. Wręcz przeciwnie ramy prawne państwa trzeciego lub organizacji międzynarodowej powinny obejmować przepisy szczególne określające w konkretny sposób prawo do ochrony danych osobowych w obszarze ścigania przestępstw. Państwo trzecie powinno dawać gwarancje zapewniające odpowiedni stopień ochrony, zasadniczo odpowiadający stopniowi przewidzianemu w Unii. Przepisy te muszą być możliwe do wyegzekwowania na drodze prawnej.

27. Ponadto w odniesieniu do zasady proporcjonalności[17] TSUE orzekł w odniesieniu do przepisów państw członkowskich, że kwestię, czy ograniczenie prawa do prywatności i ochrony danych może być uzasadnione, należy oceniać z jednej strony poprzez badanie **wagi ingerencji**, jaką stanowi takie ograniczenie[18], a z drugiej strony poprzez sprawdzenie, czy **znaczenie celu interesu ogólnego**, do którego zmierza to ograniczenie, jest proporcjonalne do tej wagi[19].

28. Zgodnie z orzecznictwem TSUE podstawa prawna umożliwiająca ingerencję w prawa podstawowe musi– aby spełniać wymóg proporcjonalności – sama określać zakres ograniczenia wykonywania danego prawa[20]. Odstępstwa od ochrony danych osobowych i jej ograniczenia mogą być stosowane jedynie wtedy, gdy jest to absolutnie konieczne[21]. Aby spełnić ten wymóg, oprócz określenia jasnych i precyzyjnych reguł dotyczących zakresu i stosowania rozpatrywanego środka, dane uregulowanie musi ustanawiać minimalne wymagania służące temu, aby osoby, których dane osobowe zostały przekazane, były zaopatrzone w wystarczające zabezpieczenia umożliwiające rzeczywistą ochronę ich danych przed ryzykiem nadużyć. „Powinno ono w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami może zostać

takiego państwa powinny znaleźć się dodatkowe zabezpieczenia gwarantujące, że dane przekazywane z UE nie będą wykorzystywane do żądania, orzekania lub wykonania kary śmierci ani do jakiejkolwiek innej formy okrutnego i nieludzkiego traktowania (np. umowa międzynarodowa nakładająca warunki przekazywania danych, zobowiązanie państwa trzeciego do nienakładania kary śmierci lub jakiejkolwiek innej formy okrutnego lub nieludzkiego traktowania na podstawie danych przekazywanych z UE lub moratorium na karę śmierci).

[17] Art. 52 ust. 1 karty.

[18] Sąd podkreślił na przykład, że „ingerencja, jaką stanowi gromadzenie w czasie rzeczywistym danych umożliwiających zlokalizowanie urządzeń końcowych, jest szczególnie poważna, ponieważ dane te umożliwiają właściwym organom krajowym dokładne i stałe monitorowanie przemieszczania się użytkowników telefonów komórkowych (...)” (sprawy połączone C-511/18, C-512/18 i C-520/18, La Quadrature du Net i in., wyrok z dnia 6 października 2020 r., ECLI:EU:C:2020:791, pkt 187 wraz z przytoczonym tam orzecznictwem).

[19] La Quadrature du Net i in., pkt 131.

[20] Schrems II, pkt 180.

[21] Schrems II, pkt 176 wraz z przytoczonym tam orzecznictwem.

przyjęty środek przewidujący przetwarzanie takich danych, gwarantując w ten sposób, że ingerencja będzie ograniczona do tego, co ściśle konieczne. Konieczność zaopatrzenia w takie gwarancje jest istotna jeszcze bardziej wówczas, gdy dane osobowe są przetwarzane w sposób zautomatyzowany”[22].

29. EROD przyjęła zalecenia odzwierciedlające orzecznictwo TSUE i Europejskiego Trybunału Praw Człowieka (ETPC) w dziedzinie nadzoru określające niezbędne gwarancje, których należy szukać w prawie państwa trzeciego w ramach oceny ingerencji takich środków nadzoru państwa trzeciego w prawa osób, których dane dotyczą, w przypadku gdy dane są przekazywane temu państwu trzeciemu na mocy RODO[23]. EROD uważa, że aby ocenić, czy spełnione są warunki, o których mowa w art. 36 ust. 2 lit. a) dyrektywy 2016/680, przy ocenie, czy państwo trzecie zapewnia odpowiedni stopień ochrony w obszarze nadzoru zgodnie z tą dyrektywą, należy wziąć pod uwagę gwarancje określone w tych zaleceniach, mając na uwadze w tym kontekście dalsze szczegółowe warunki w obszarze nadzoru.

30. W odniesieniu do wymogu określonego w art. 36 ust. 2 lit. b) państwo trzecie powinno nie tylko zapewnić skuteczny niezależny nadzór nad ochroną danych, ale również zapewnić mechanizmy współpracy z organami ochrony danych państw członkowskich[24].

31. W odniesieniu do wymogu określonego w art. 36 ust. 2 lit. c) poza międzynarodowymi zobowiązaniami, które przyjęły państwo trzecie lub organizacja międzynarodowa, należy również wziąć pod uwagę obowiązki wynikające z udziału państwa trzeciego lub organizacji międzynarodowej w systemach wielostronnych lub regionalnych, zwłaszcza w odniesieniu do ochrony danych osobowych, a także realizację tych obowiązków; w szczególności należy wziąć pod uwagę przystąpienie państwa trzeciego do innych umów międzynarodowych o ochronie danych osobowych, np. do Konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych oraz do Protokołu dodatkowego do tej konwencji (konwencja nr 108[25] i jej zaktualizowana wersja – konwencja nr 108+). Można również wziąć pod uwagę to, czy państwo trzecie przestrzega zasad zawartych w dokumentach międzynarodowych, takich jak wydany przez Radę Europy „Praktyczny przewodnik w sprawie wykorzystywania danych osobowych przez policję – sposoby ochrony danych osobowych podczas walki z przestępczością” (Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime).

32. Decyzja stwierdzająca odpowiedni stopień ochrony powinna gwarantować, że dany zagraniczny system jako całość zapewnia wymagany stopień ochrony, biorąc pod uwagę istotę prawa do prywatności i prawa do ochrony danych oraz skuteczne wprowadzenie w życie tych praw, nadzór nad ich przestrzeganiem i ich egzekwowanie, w tym w odniesieniu do danych przekazywanych do tego państwa trzeciego. Jak podkreślił TSUE w wyroku w sprawie Schrems II, wysoki stopień ochrony należy zapewnić również w sytuacji, gdy dane są przekazywane do państwa trzeciego[26].

33. Ponadto przy przyjmowaniu decyzji stwierdzających odpowiedni stopień ochrony w odniesieniu jedynie do konkretnego terytorium lub określonego sektora w państwie trzecim Komisja powinna wziąć pod uwagę jasne i obiektywne kryteria, na przykład odnoszące się do konkretnych czynności

[22] Schrems II, pkt 176 wraz z przytoczonym tam orzecznictwem.
[23] Zalecenia EROD 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru, przyjęte w dniu 10 listopada 2020 r.
[24] Motyw 67 dyrektywy 2016/680.
[25] Motyw 68 dyrektywy 2016/680.
[26] Zob. pkt 93.

przetwarzania lub zakresu właściwych norm prawnych i ustawodawstwa obowiązującego w państwie trzecim[27].

A. Zasady ogólne i zabezpieczenia

a) Pojęcia

34. W danym systemie prawnym powinny istnieć podstawowe pojęcia dotyczące ochrony danych osobowych. Nie muszą one odzwierciedlać terminologii dyrektywy 2016/680, ale powinny odzwierciedlać pojęcia zawarte w europejskim prawie w dziedzinie ochrony danych i być z nimi spójne. Przykładowo dyrektywa 2016/680 zawiera następujące istotne pojęcia: „dane osobowe", „przetwarzanie danych osobowych", „właściwe organy", „administrator danych", „podmiot przetwarzający dane", „odbiorca", „dane wrażliwe", „prawidłowość", „profilowanie", „uwzględnienie ochrony danych w fazie projektowania i domyślna ochrona danych", „organ nadzorczy" i „pseudonimizacja".

b) Zgodność z prawem i rzetelność przetwarzania danych osobowych (art. 4 – motyw 26)

35. Zgodnie z art. 8 ust. 2 karty dane osobowe powinny w szczególności być przetwarzane „w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą"[28]. W kontekście ścigania przestępstw należy jednak zauważyć, że wykonywanie zadań polegających na zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych, instytucjonalnie powierzonych na mocy prawa właściwym organom, pozwala tym organom wymagać lub nakazywać, aby osoby fizyczne zastosowały się do stawianych żądań. W takim przypadku zgoda osoby, której dane dotyczą, nie powinna stanowić podstawy prawnej przetwarzania danych osobowych przez właściwe organy[29].

36. Ta podstawa prawna powinna określać jasne i precyzyjne reguły dotyczące zakresu i stosowania odpowiednich czynności przetwarzania danych oraz ustanawiać minimalne zabezpieczenia[30]. Ponadto TSUE przypomniał, że „to uregulowanie musi być prawnie wiążące w prawie wewnętrznym"[31].

[27] Motyw 67 dyrektywy 2016/680.
[28] Zob. Schrems II, pkt 173.
[29] Motyw 35 dyrektywy 2016/680 stanowi również, że „[j]eżeli osoba, której dane dotyczą, musi wywiązać się z obowiązku prawnego, nie ma ona faktycznego, swobodnego wyboru, a tym samym nie można uznać, iż jej reakcja jest swobodnym wyrazem jej woli. Nie powinno to stanowić dla państw członkowskich przeszkody w ustanowieniu z mocy prawa, że osoba, której dane dotyczą, może wyrazić zgodę na przetwarzanie jej danych osobowych do celów określonych w niniejszej dyrektywie, takich jak badania DNA w postępowaniu przygotowawczym czy monitorowanie miejsca jej pobytu za pomocą aparatury elektronicznej na potrzeby wykonania kary".
[30] Zob. Schrems II, pkt 175 i 180 oraz opinia 1/15, pkt 139 i przytoczone tam orzecznictwo.
[31] Zob. sprawa C-623/17, Privacy International przeciwko Secretary of State for Foreign and Commonwealth Affairs i in., wyrok z dnia 6 października 2020 r., ECLI:EU:C:2020:790, pkt 68. Należy również wyjaśnić, że we francuskiej wersji wyroku TSUE posługuje się terminem „réglementation", którego znaczenie jest szersze i obejmuje nie tylko akty Parlamentu.

37. Aby przetwarzanie danych[32] było zgodne z prawem, powinno ono być niezbędne do wykonania zadania realizowanego przez właściwy organ do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom[33]. Cele te powinny być określone w prawie krajowym.

38. Dane osobowe są przetwarzane rzetelnie. Zasada rzetelnego przetwarzania obowiązująca w ochronie danych jest pojęciem odrębnym względem prawa do rzetelnego procesu, które jest zdefiniowane w art. 47 karty i w art. 6 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności („EKPC")[34].

c) Zasada ograniczenia celu (art. 4)

39. Konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie zbierania tych danych[35].

40. Dane powinny być przetwarzane w konkretnym, wyraźnym i prawnie uzasadnionym celu, mieszczącym się w ramach celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar[36], w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom w państwie trzecim, a następnie wykorzystywane do któregokolwiek z tych celów, o ile nie jest to niezgodne z pierwotnym celem przetwarzania danych (np. do celów toczących się równolegle postępowań egzekucyjnych lub archiwizacji w interesie publicznym, wykorzystania danych przetwarzanych w powyższych celach do celów naukowych, statystycznych lub historycznych) oraz z zastrzeżeniem stosowania odpowiednich zabezpieczeń chroniących prawa i wolności osób, których dane dotyczą. Jeżeli dane osobowe przetwarza ten sam lub inny administrator (właściwy organ[37]) w celu zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, innym niż cel, w którym dane zostały zebrane, przetwarzanie takie powinno być dopuszczalne, pod warunkiem że przetwarzanie jest dozwolone na podstawie właściwych przepisów prawa oraz jest niezbędne i proporcjonalne do tego innego celu[38]. Należy także wziąć pod uwagę istnienie mechanizmu informowania odpowiednich właściwych organów państw członkowskich o takim dalszym

[32] Przetwarzanie danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz przetwarzanie w sposób inny niż zautomatyzowany danych osobowych stanowiących lub mających stanowić część zbioru danych.
[33] Właściwymi organami są wszelkie organy publiczne właściwe do takich celów oraz wszelkie inne organy lub podmioty, którym prawo powierza wykonywanie władzy publicznej i uprawnień publicznych w tym celu.
[34] Motyw 26 dyrektywy 2016/680.
[35] Motyw 26 dyrektywy 2016/680.
[36] Cele te obejmują „czynności policji podejmowane, gdy nie wiadomo, czy dane zdarzenie jest czynem zabronionym. Czynności te mogą też polegać na sprawowaniu władzy poprzez stosowanie środków przymusu takich jak czynności policji podczas demonstracji, dużych imprez sportowych czy zamieszek. Czynności te obejmują również utrzymywanie prawa i porządku jako zadanie powierzone policji lub innym organom ścigania, gdy jest to konieczne do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i dla prawnie chronionych podstawowych interesów społecznych i do zapobiegania takim zagrożeniom, które mogą prowadzić do popełnienia czynu zabronionego" (motyw 12 dyrektywy 2016/680). Należy je odróżnić od celu związanego z bezpieczeństwem narodowym i od czynności, które wchodzą w zakres stosowania tytułu V rozdział 2 Traktatu o Unii Europejskiej (TUE) (motyw 14 dyrektywy 2016/680).
[37] Zob. przypis 33.
[38] Motyw 29 dyrektywy 2016/680.

przetwarzaniu danych[39]. Ponadto nie należy w żadnym wypadku obniżać stopnia ochrony osób fizycznych przewidzianego w Unii w dyrektywie 2016/680, także w przypadkach, gdy dane osobowe są przekazywane z państwa trzeciego administratorom lub podmiotom przetwarzającym w tym samym państwie trzecim[40].

d) Szczególne warunki dalszego przetwarzania do innych celów (art. 9)

41. Jeżeli chodzi o dalsze przetwarzanie lub ujawnianie danych przekazywanych z UE do celów innych niż ściganie przestępstw, takich jak cele związane z bezpieczeństwem narodowym, powinno ono być również przewidziane prawem, niezbędne i proporcjonalne. Należy także wziąć pod uwagę istnienie mechanizmu informowania odpowiednich właściwych organów państw członkowskich o takim dalszym przetwarzaniu danych[41]. Również w tym przypadku, po dalszym przetworzeniu lub ujawnieniu, dane powinny być objęte takim samym stopniem ochrony, jakim były objęte, gdy były pierwotnie przetwarzane przez właściwy organ odbierający dane.

e) Zasada minimalizacji danych

42. Dane powinny być adekwatne, stosowne i niewykraczające poza cele, w których są przetwarzane. W szczególności należy wziąć pod uwagę zastosowanie wymogów dotyczących uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, takich jak ograniczenia pól wprowadzania danych (ustrukturyzowane przekazywanie danych) lub zautomatyzowane i niezautomatyzowane kontrole jakości.

f) Zasada prawidłowości danych

43. Dane powinny być prawidłowe i w razie potrzeby uaktualniane. Zasadę prawidłowości danych należy jednak stosować z uwzględnieniem charakteru i celu przetwarzania. W szczególności w postępowaniu sądowym oświadczenia zawierające dane osobowe opierają się na subiektywnym osądzie osób fizycznych i nie zawsze są weryfikowalne. Dlatego wymóg prawidłowości danych nie powinien odnosić się do prawidłowości oświadczenia, lecz jedynie do faktu, że konkretne oświadczenie zostało złożone[42].

44. Należy zapewnić, aby nieprawidłowe, niekompletne lub nieaktualne dane osobowe nie były przesyłane ani udostępniane[43] oraz aby przewidziane były procedury korygowania lub usuwania nieprawidłowych danych. W szczególności należy wziąć pod uwagę wszelkie systemy klasyfikacji przetwarzanych informacji, wiarygodność źródła i stopień weryfikacji faktów[44].

g) Zasada zatrzymywania danych

45. Dane nie powinny być przechowywane przez okres dłuższy, niż jest to niezbędne do celów, w których są przetwarzane. Należy ustanowić odpowiednie mechanizmy usuwania danych

[39] Takim mechanizmem mogłyby być na przykład wspólnie uzgodnione kodeksy postępowania, obowiązek powiadamiania odpowiednich organów na mocy instrumentu międzynarodowego, w tym ewentualne powiadomienia automatyczne, lub inne podobne środki zapewniające przejrzystość.
[40] Motyw 64 dyrektywy 2016/680.
[41] Zob. przypis 39.
[42] Motyw 30 dyrektywy 2016/680.
[43] Motyw 32 dyrektywy 2016/680.
[44] Np. system oceny 4x4 dla ocen wiarygodności i kodeksów postępowania.

osobowych; może to być określony termin lub okresowy przegląd konieczności przechowywania danych osobowych (lub połączenie obu tych metod – określenie maksymalnego czasu przechowywania i przeprowadzanie okresowego przeglądu w wyznaczonych odstępach czasu)[45]. Dane osobowe przechowywane przez dłuższy okres w celu archiwizacji w interesie publicznym, wykorzystania do celów naukowych, statystycznych lub historycznych powinny podlegać odpowiednim zabezpieczeniom (np. dotyczącym dostępu)[46].

h) Zasada bezpieczeństwa i poufności (art. 29, motywy 28 i 71)

46. Podmiot przetwarzający dane osobowe powinien zapewnić przetwarzanie danych w sposób zapewniający im bezpieczeństwo, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu. Obejmuje to ochronę przed przetwarzaniem niezgodnym z prawem, a także przed przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych oraz odpowiednie środki służące zaradzeniu tym zjawiskom. Przy określaniu poziomu bezpieczeństwa należy uwzględnić stan wiedzy technicznej, koszty wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.

47. Należy zapewnić bezpieczne kanały komunikacji między organami państw członkowskich przekazującymi dane osobowe a organami państw trzecich, które je otrzymują.

i) Zasada przejrzystości (art. 13, motywy 26, 39, 42, 43, 44, 46)

48. Osobom fizycznym należy uświadomić ryzyko, zasady, zabezpieczenia i prawa związane z przetwarzaniem ich danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem[47].

49. Osobom fizycznym powinny być udostępniane informacje na temat najważniejszych elementów przetwarzania ich danych osobowych. Informacje te powinny być łatwo dostępne i zrozumiałe, napisane przy użyciu jasnego i prostego języka. Powinny one obejmować cel przetwarzania danych, tożsamość administratora danych, przyznane mu prawa[48] oraz inne informacje w zakresie, w jakim jest to niezbędne do zapewnienia rzetelności.

50. Mogą istnieć pewne wyjątki od tego prawa do informacji. Ograniczenie takie powinno być jednak dozwolone na podstawie aktu prawnego, a także powinno być niezbędne i proporcjonalne, aby uniknąć utrudniania prowadzenia urzędowych lub sądowych dochodzeń, postępowań przygotowawczych lub procedur, aby uniknąć uniemożliwienia zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, aby chronić bezpieczeństwo publiczne i narodowe oraz aby chronić prawa i wolności innych osób, o ile takie częściowe lub całkowite ograniczenie stanowi niezbędny i proporcjonalny środek w społeczeństwie demokratycznym, przy należytym uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej. Takie ograniczenia należy również rozważyć i ocenić z uwzględnieniem możliwości złożenia skargi do organu nadzorczego lub skorzystania ze środka ochrony prawnej. W każdym razie wszelkie ewentualne ograniczenia powinny mieć charakter tymczasowy, a nie ogólny, oraz powinny być objęte podobnymi warunkami, zabezpieczeniami i ograniczeniami do tych, jakie są wymagane na mocy Karty praw

[45] Art. 5 dyrektywy 2016/680.
[46] Motyw 26 dyrektywy 2016/680.
[47] Motyw 26 dyrektywy 2016/680.
[48] Zarówno prawa materialne (prawo dostępu, prawo do sprostowania itp.), jak i prawo do dochodzenia roszczeń.

podstawowych Unii Europejskiej i EKPC, zgodnie z wykładnią zawartą odpowiednio w orzecznictwie TSUE i ETPC, a w szczególności szanować istotę tych praw i wolności.

j) Prawo dostępu, prawo do sprostowania i usunięcia danych (art. 14 i 16)

51. Osoba, której dane dotyczą, powinna mieć prawo do uzyskania potwierdzenia, czy przetwarzane są dane jej dotyczące, a jeżeli takie dane są przetwarzane, powinna mieć prawo dostępu do swoich danych. Prawo to powinno obejmować co najmniej pewne informacje na temat przetwarzania, takie jak cele i podstawa prawna przetwarzania, informacje o prawie wniesienia skargi do organu nadzorczego oraz kategorie odnośnych danych osobowych[49]. Jest to szczególnie ważne w przypadku, gdy przejrzystość osiąga się za pomocą ogólnego zawiadomienia (np. informacji na stronie internetowej organu).

52. Osoba, której dane dotyczą, powinna mieć prawo do sprostowania swoich danych z określonych powodów, na przykład jeżeli okaże się, że są one nieprawidłowe lub niekompletne. Osoba, której dane dotyczą, powinna mieć również prawo do usunięcia swoich danych, na przykład gdy ich przetwarzanie nie jest już niezbędne lub jest niezgodne z prawem.

53. Wykonanie tych praw nie powinno być nadmiernie uciążliwe dla osoby, której dane dotyczą.

k) Ograniczenia praw osoby, której dane dotyczą

54. Ewentualne ograniczenia tych praw mogłyby zostać ustanowione, aby uniknąć utrudniania prowadzenia urzędowych lub sądowych dochodzeń, postępowań przygotowawczych lub procedur, aby uniknąć uniemożliwienia zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, aby chronić bezpieczeństwo publiczne i narodowe oraz aby chronić prawa i wolności innych osób, o ile takie częściowe lub całkowite ograniczenie stanowi niezbędny i proporcjonalny środek w społeczeństwie demokratycznym, przy należytym uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej. Takie ograniczenia należy również rozważyć i ocenić z uwzględnieniem możliwości złożenia skargi do organu nadzorczego lub skorzystania z sądowego środka zaskarżenia.

l) Ograniczenie dalszego przekazywania danych (art. 35, motywy 64–65)

55. W przypadku dalszego przekazywania danych osobowych przez pierwotnego odbiorcę do innego państwa trzeciego lub organizacji międzynarodowej nie należy obniżać przewidzianego w Unii stopnia ochrony danych osób fizycznych, których dane są przekazywane. W związku z tym takie dalsze przekazywanie danych powinno być dozwolone wyłącznie w przypadku zapewnienia ciągłości poziomu ochrony przyznanego prawem Unii[50]. W szczególności dalszy odbiorca (tj. odbiorca dalszego przekazywania) powinien być organem właściwym do celów ścigania przestępstw[51], a dalsze przekazywanie danych może odbywać się wyłącznie w ograniczonych i określonych celach i o ile istnieje podstawa prawna do takiego przetwarzania.

56. Należy również wziąć pod uwagę istnienie mechanizmu, w ramach którego właściwe organy danego państwa członkowskiego są informowane o dalszym przekazywaniu danych oraz wyrażają

[49] Art. 14 dyrektywy 2016/680.
[50] Zob. również opinia 1/15.
[51] Zob. przypis 33.

na nie zgodę. Pierwotny odbiorca danych przekazywanych z UE powinien ponosić odpowiedzialność za to, by odpowiedni właściwy organ państwa członkowskiego zezwolił na dalsze przekazywanie danych[52] oraz by zapewniono odpowiednie zabezpieczenia dla przekazywanych danych w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do państwa trzeciego, do którego dane byłyby dalej przekazywane[53], a ponadto pierwotny odbiorca danych powinien być w stanie udowodnić, że właściwy organ państwa członkowskiego udzielił takiej zgody oraz że zapewniono takie zabezpieczenia.

m) Zasada rozliczalności (art. 4 ust. 4)

57. Administrator powinien odpowiadać za przestrzeganie zasad ochrony danych określonych w art. 4 dyrektywy 2016/680 i być w stanie wykazać ich przestrzeganie.

[52] W tym kontekście należy uwzględnić istnienie obowiązku lub zobowiązania do wdrożenia odpowiednich kodeksów postępowania określonych przez organy państw członkowskich przekazujące dane.
[53] Powyższe wymogi nie naruszają szczególnych warunków dalszego przekazywania danych do odpowiedniego państwa określonych w dyrektywie 2016/680 (art. 35 ust. 1 lit. c) i e)).

B. Przykłady dodatkowych zasad, które mają być stosowane do konkretnych rodzajów przetwarzania

a) Szczególne kategorie danych (art. 10 i motyw 37)

58. Jeżeli przetwarzanie obejmuje „szczególne kategorie danych", powinny istnieć szczególne zabezpieczenia[54] służące ochronie przed szczególnymi rodzajami ryzyka[55]. Kategorie te powinny odzwierciedlać kategorie określone w art. 10 dyrektywy 2016/680. Przetwarzanie danych należących do szczególnych kategorii powinno zatem podlegać szczególnym zabezpieczeniom i być dozwolone wyłącznie wtedy, jeżeli jest absolutnie niezbędne, pod pewnymi warunkami, na przykład w celu ochrony żywotnych interesów danej osoby.

b) Zautomatyzowane podejmowanie decyzji i profilowanie (art. 11 i motyw 38)

59. Decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu (zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach), w tym profilowaniu, które wywołują negatywne skutki prawne lub istotnie wpływają na osobę, której dane dotyczą, powinny być podejmowane jedynie pod pewnymi warunkami określonymi w ramach prawnych państwa trzeciego[56].

60. W systemie prawnym Unii Europejskiej takie warunki obejmują na przykład udzielenie konkretnych informacji osobie, której dane dotyczą, i prawo do uzyskania interwencji ludzkiej ze strony administratora, a zwłaszcza prawo do wyrażenia własnego stanowiska, uzyskania wyjaśnienia decyzji wydanej wskutek takiej analizy lub zaskarżenia tej decyzji.

61. Prawo państwa trzeciego powinno w każdym przypadku przewidywać niezbędne zabezpieczenia praw i wolności osób, których dane dotyczą. W związku z tym należy również wziąć pod uwagę istnienie mechanizmu informowania właściwych organów danego państwa członkowskiego o dalszym przetwarzaniu, takim jak wykorzystywanie przekazanych danych do profilowania na dużą skalę.

c) Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych (art. 20)

62. Oceniając odpowiedni stopień ochrony, należy zwrócić uwagę na istnienie obowiązku przyjmowania przez administratorów wewnętrznych polityk i wdrażania środków, które są zgodne z zasadami ochrony danych w fazie projektowania i domyślnej ochrony danych, z uwzględnieniem stanu wiedzy technicznej, kosztu wdrożenia i charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia wynikające z przetwarzania – zarówno w czasie określania sposobów przetwarzania, jak i w czasie samego przetwarzania – oraz obowiązku przyjmowania przez administratorów odpowiednich środków technicznych i organizacyjnych, takich jak pseudonimizacja, zaprojektowanych w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń.

[54] Takie szczególne kategorie zostały również określone jako „dane wrażliwe" w motywie 37 dyrektywy 2016/680.
[55] Takimi dodatkowymi zabezpieczeniami mogą być np. szczególne środki bezpieczeństwa, ograniczone prawa dostępu dla pracowników, ograniczenia dotyczące dalszego przetwarzania, zautomatyzowanego podejmowania decyzji, dalszego udostępniania lub dalszego przekazywania danych.
[56] Opinia 1/15, pkt 173.

C. Mechanizmy proceduralne i mechanizmy egzekwowania prawa

63. Mimo że środki, z których korzysta państwo trzecie w celu zapewnienia odpowiedniego stopnia ochrony, mogą się różnić od środków stosowanych w Unii Europejskiej[57], system zgodny z systemem europejskim musi zawierać następujące elementy:

a) Właściwy niezależny organ nadzorczy (art. 36 ust. 2 lit. b), art. 36 ust. 3 i motyw 67)

64. Powinien istnieć co najmniej jeden niezależny organ nadzorczy odpowiedzialny za zapewnianie i egzekwowanie przestrzegania przepisów o ochronie danych osobowych i prywatności w państwie trzecim. Podczas wypełniania swoich zadań i wykonywania swoich uprawnień organ nadzorczy powinien działać w sposób w pełni niezależny i bezstronny, a w trakcie tych działań nie powinien zwracać się o żadne instrukcje ani takich instrukcji przyjmować. W tym kontekście organ nadzorczy powinien dysponować wszelkimi odpowiednimi uprawnieniami do egzekwowania skutecznego przestrzegania przepisów dotyczących ochrony danych osobowych i propagowania wiedzy na ten temat. Należy również rozważyć personel i budżet organu nadzorczego. Organ nadzorczy powinien być też w stanie prowadzić dochodzenia z urzędu. Jego zadaniem powinno być również udzielanie pomocy i doradzanie osobom, których dane dotyczą, w zakresie wykonywania przysługujących im praw (zob. również lit. c) poniżej). W decyzjach stwierdzających odpowiedni stopień ochrony należy określić, w stosownych przypadkach, ten organ nadzorczy lub te organy nadzorcze oraz mechanizmy współpracy z organami nadzorczymi państw członkowskich w celu egzekwowania przepisów o ochronie danych.

b) Skuteczne wdrażanie przepisów dotyczących ochrony danych

65. System państwa trzeciego powinien zapewniać wysoki stopień 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 wykonywania tych praw. 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.

66. 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 powinny obejmować prowadzenie rejestrów lub dzienników czynności przetwarzania danych przez odpowiedni okres. Mogą one również obejmować na przykład oceny skutków dla ochrony danych, wyznaczenie inspektora ochrony danych lub uwzględnienie ochrony danych w fazie projektowania i domyślną ochronę danych.

c) System ochrony danych ułatwia wykonywanie praw osobie, której dane dotyczą (art. 12, 17 i 46 dyrektywy 2016/680)

67. Ramy ochrony danych obowiązujące w państwie trzecim powinny zobowiązywać administratorów danych do ułatwiania osobom, których dane dotyczą, wykonywania praw, o których mowa w sekcji A lit. j) powyżej, oraz powinny przewidywać, że organ nadzorczy w tym

[57] Schrems I, pkt 74.

państwie trzecim informuje na wniosek każdą osobę, której dane dotyczą, o wykonywaniu przysługujących jej praw[58].

d) System ochrony danych zapewnia odpowiednie mechanizmy dochodzenia roszczeń

68. Chociaż obecnie brak jest orzecznictwa dotyczącego odpowiedniego stopnia ochrony danych w systemie prawnym państwa trzeciego w rozumieniu dyrektywy 2016/680, TSUE dokonał wykładni podstawowego prawa do skutecznej ochrony sądowej przewidzianego w art. 47 Karty praw podstawowych Unii Europejskiej. Art. 47 akapit pierwszy karty stanowi, że każdy, kogo prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka prawnego przed sądem[59], zgodnie z warunkami przewidzianymi w tym artykule.

69. Zgodnie z utrwalonym orzecznictwem TSUE samo istnienie skutecznej kontroli sądowej służącej zapewnieniu poszanowania przepisów prawa Unii jest nierozerwalnie związane z istnieniem praworządności. Tak więc uregulowanie nieprzewidujące dla jednostek żadnej drogi prawnej pozwalającej na uzyskanie dostępu do dotyczących ich danych osobowych lub sprostowanie czy usunięcie takich danych nie zapewnia poszanowania zasadniczej istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 karty[60].

70. 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.

71. W związku z tym 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.

72. W przypadku nieprzestrzegania przepisów osobie, której dane są przekazywane do państwa trzeciego, należy także zapewnić skuteczne administracyjne i sądowe środki zaskarżenia w państwie trzecim, 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.

[58] Wykonywanie praw osób, których dane dotyczą, może mieć charakter bezpośredni lub pośredni.
[59] TSUE jest zdania, że skuteczna ochrona sądowa może być zapewniona nie tylko przez sąd, ale również przez organ, który oferuje zabezpieczenia merytorycznie równoważne tym wymaganym w art. 47 karty (zob. Schrems II, pkt 197). Może to być istotne w szczególności dla organizacji międzynarodowych.
[60] Schrems II, pkt 187 i 194 wraz z przytoczonym tam orzecznictwem.