

Opinia 07/2025 dotycząca projektu decyzji wykonawczej Komisji Europejskiej w sprawie odpowiedniej ochrony danych osobowych przez Europejską Organizację Patentową na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679

Przyjęta 5 maja 2025 r.

Streszczenie

4 marca 2025 r. Komisja Europejska rozpoczęła proces zmierzający do przyjęcia projektu decyzji wykonawczej („projekt decyzji”) w sprawie odpowiedniej ochrony danych osobowych przez Europejską Organizację Patentową (EPO lub „Organizacja”)¹.

5 marca 2025 r. Komisja Europejska zwróciła się do Europejskiej Rady Ochrony Danych (EROD) o opinię w tej sprawie. EROD przeprowadziła ocenę odpowiedniości stopnia ochrony zapewnianego przez EPO na podstawie zbadania projektu decyzji oraz analizy dokumentacji przekazanej przez Komisję Europejską.

EROD skupiła się na ocenie ram prawnych i przepisów o ochronie danych stosowanych w EPO oraz środków ochrony prawnej dostępnych dla osób fizycznych w Europejskim Obszarze Gospodarczym (EOG), w tym m.in. kwestii dostępu organów publicznych do danych osobowych przekazywanych z EOG do EPO.

EROD oceniła również, czy przewidziane w ramach EPO zabezpieczenia zostały faktycznie wprowadzone i są skutecznie egzekwowane, zwłaszcza w zakresie nadzoru i kontroli, z uwzględnieniem specyfiki organizacji międzynarodowych.

Punktem odniesienia był dokument Grupy Roboczej Art. 29 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych².

EROD pozytywnie ocenia fakt, że ramy ochrony danych EPO wykazują wiele podobieństw do ram ochrony danych Unii Europejskiej, zwłaszcza w zakresie praw i zasad dotyczących ochrony danych.

Ustalono również, że niektóre kwestie powinny zostać doprecyzowane i ściśle monitorowane przez Komisję Europejską.

W szczególności EROD wzywa Komisję do wyjaśnienia, że w kontekście struktury zarządzania ochroną danych wdrożonej przez EPO to administrator (tj. Europejski Urząd Patentowy), ponosi ostateczną odpowiedzialność za naruszenia przepisów o ochronie danych.

W odniesieniu do dalszego przekazywania danych EROD zauważa, że wymóg nieobniżania stopnia ochrony nie został wyraźnie wymieniony w związku z tak zwanym „przesyłaniem” danych osobowych organom publicznym w państwach będących umawiającymi się państwami EPO. EROD zwraca się do Komisji o wyjaśnienie tej kwestii i sprecyzowanie, jakie zabezpieczenia obowiązują, gdy przekazywane są dane osobowe w szczególnym kontekście procedury udzielania patentów.

Biorąc pod uwagę ścisły związek między inspektorem ochrony danych (IOD) a Radą Ochrony Danych (ROD) oraz znaczenie uprawnień dochodzeniowych, kontrolnych i naprawczych, EROD zaleca Komisji dalsze doprecyzowanie wzajemnych powiązań między tymi podmiotami, w szczególności w odniesieniu do wykonywania uprawnień dochodzeniowych, kontrolnych i naprawczych, a także wyjaśnienie roli IOD w rozpatrywaniu wniosków osób, których dane dotyczą, oraz jego ewentualnej roli w procedurze dotyczącej skarg przed ROD. Ponadto EROD zauważa, że (uzasadnione) opinie ROD wydawane w ramach procedury dotyczącej skarg nie mają charakteru wiążącego i zwraca się zatem do Komisji o sprawdzenie, czy w tym kontekście uprawnienia ROD są wiążące, oraz o zapewnienie, by takie były, a także o ocenę, czy w tym celu mogłyby zostać wprowadzone dodatkowe zabezpieczenia .

¹ Komunikat prasowy https://ec.europa.eu/commission/presscorner/detail/sv/ip_25_613.

² Grupa Robocza Art. 29, dokument WP 254 rev. 01, przyjęty 28 listopada 2017 r. i ostatnio zmieniony i przyjęty 6 lutego 2018 r., zatwierdzony przez EROD.

EROD przeanalizowała również ramy prawne EPO w odniesieniu do dostępu organów publicznych do danych osobowych przekazywanych z UE do Organizacji i ich wykorzystywania. W związku z tym EROD zwraca uwagę, że ocena dostępu administracji rządowej w przedmiotowej sprawie różni się od oceny stopnia ochrony zapewnianej przez państwo trzecie. W tym określonym scenariuszu dotyczącym decyzji o odpowiedniej ochronie danych osobowych zapewnianej przez organizację międzynarodową należy dokonać przeglądu przepisów określających sposób, w jaki organizacja ta realizuje wnioski administracji rządowej o dostęp.

W odniesieniu do umawiających się państw, immunitety EPO uzupełnia obowiązek współpracy. W tym celu EPO może zrzec się immunitetu jurysdykcyjnego i egzekucyjnego, aby odpowiedzieć na wnioski administracji rządowej o dostęp do danych. EROD wzywa Komisję do dalszego wyjaśnienia, w szczególności w odniesieniu do wniosków o dostęp do danych do celów egzekwowania prawa i bezpieczeństwa narodowego, w jaki sposób obowiązek współpracy odnosi się do pojęcia immunitetu. W tym kontekście EROD zwraca się również do Komisji o wyjaśnienie uprawnień Prezesa i zakresu uprawnień dyskrecyjnych przy podejmowaniu decyzji w sprawie wniosku o współpracę.

Jeżeli EPO postanowi zastosować się do wniosku o dostęp od umawiającego się państwa, zastosowanie mają wymogi dotyczące przesyłania danych. Przepisy te znajdują zastosowanie do wszystkich umawiających się państw, niezależnie od tego, czy dane umawiające się państwo należy do EOG, czy jest uważane za państwo trzecie z punktu widzenia prawa UE dotyczącego ochrony danych. EROD podkreśla, że wymogi rozdziału V RODO w zakresie niezbędnym do ustanowienia merytorycznej równowagi muszą być w wystarczający sposób uwzględnione oraz zwraca się do Komisji o doprecyzowanie, jakie zabezpieczenia mają zastosowanie w takich przypadkach.

Spis treści

1.	WPROWADZENIE.....	5
1.1	Struktura i ramy ochrony danych w EPO	5
1.2	Specyfika organizacji międzynarodowych	6
1.3	Przywileje i immunitety EPO	7
1.4	Zarządzanie ochroną danych w EPO	7
2.	OGÓLNE ASPEKTY OCHRONY DANYCH	8
2.1	Zasady dotyczące treści.....	8
2.1.1	Pojęcia	8
2.1.2	Zasady ochrony danych.....	8
2.2	Prawa jednostek.....	9
2.3	Ograniczenia dotyczące dalszego przekazywania danych	10
2.3.1	Przesyłanie danych osobowych	11
2.4	Mechanizmy proceduralne i mechanizmy egzekwowania	12
2.4.1	Inspektor Ochrony Danych i Rada Ochrony Danych	12
2.4.2	Uprawnienia dochodzeniowe i naprawcze	13
2.4.3	Procedura dotycząca skarg przed Radą Ochrony Danych.....	15
2.4.4	Mechanizmy dochodzenia roszczeń i arbitraż	16
3.	DOSTĘP ORGANÓW PUBLICZNYCH DO DANYCH OSOBOWYCH PRZEKAZYWANYCH Z UNII DO EUROPEJSKIEJ ORGANIZACJI PATENTOWEJ I ICH WYKORZYSTYWANIE	17
3.1	Rozpatrywanie przez EPO wniosków administracji rządowych o dostęp do danych osobowych	17
3.2	Ograniczenie praw osób, których dane dotyczą	19
4.	WDROŻENIE I MONITOROWANIE PROJEKTU DECYZJI	20

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. s) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej „RODO”),

uwzględniając Porozumienie o Europejskim Obszarze Gospodarczym (EOG), w szczególności jego załącznik XI i protokół 37 w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z 6 lipca 2018 r.³,

uwzględniając art. 12 i art. 22 swojego regulaminu wewnętrznego,

PRZYJMUJE PONIŻSZĄ OPINIĘ.

1. WPROWADZENIE

1. W rozdziale V RODO określono warunki przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych. Przekazywanie danych osobowych może nastąpić na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony (art. 45 RODO), a w przypadku braku takiej decyzji – jeżeli administrator lub podmiot przetwarzający zapewnia odpowiednie zabezpieczenia, w tym egzekwowalne prawa osób, których dane dotyczą, oraz skuteczne środki ochrony prawnej (art. 46 RODO). W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń jednorazowe lub wielokrotne przekazanie danych osobowych jest dopuszczalne jedynie w określonych warunkach (art. 49 RODO).
2. EROD przypomina, że decyzje stwierdzające odpowiedni stopień ochrony zapewniają ciągłą ochronę danych osobowych przekazywanych z EOG do państw trzecich i są skutecznym narzędziem ochrony praw osób, których dane dotyczą, w przypadku przekazywania danych poza EOG.
3. Szczególnie pozytywnie oceniana jest przez EROD inicjatywa Komisji dotycząca opracowania pierwszej decyzji stwierdzającej odpowiedni stopień ochrony dla organizacji międzynarodowej. Ma ona istotne znaczenie, gdyż pokazuje, że ramy prawne organizacji międzynarodowych można uznać za zapewniające odpowiedni stopień ochrony w rozumieniu art. 45 RODO.
4. EROD przy tej okazji zachęca Komisję do kontynuowania dialogu z organizacjami międzynarodowymi w celu opracowania, poszerzenia i powielenia tego rodzaju decyzji stwierdzających odpowiedni stopień ochrony – wraz z dialogiem z państwami trzecimi.

1.1 Struktura i ramy ochrony danych w EPO

5. Europejska Organizacja Patentowa (EPO) z siedzibą w Monachium jest organizacją międzyrządową powołaną na mocy konwencji o patencie europejskim („konwencja”)⁴. Organizacja liczy 39 umawiających się państw i posiada osobowość prawną. Składa się z dwóch głównych organów: Europejskiego Urzędu Patentowego („Urząd”), który pełni funkcję organu wykonawczego, oraz Rady

³ Odniesienia do „państw członkowskich” w niniejszej opinii należy rozumieć jako odniesienia do „państw członkowskich EOG”.

⁴ Motyw 7 projektu decyzji.

Administracyjnej, wykonującej uprawnienia ustawodawcze w imieniu EPO i odpowiadającej za kwestie polityczne (art. 33 konwencji).

6. Do głównych kompetencji EPO należy udzielanie patentów europejskich, co realizuje Urząd pod nadzorem Rady Administracyjnej.
7. Na czele Urzędu składającego się z różnych wydziałów stoi prezes, reprezentujący EPO. Prezes jest odpowiedzialny za zarządzanie działalnością Urzędu i za sprawy dyscyplinarne oraz odpowiada przed Radą Administracyjną. Rada Administracyjna składa się z przedstawicieli umawiających się państw i nadzoruje zarówno kwestie polityczne, jak i działalność Urzędu.
8. 30 czerwca 2021 r. w EPO przyjęto przepisy o ochronie danych osobowych („przepisy ODO” lub „ODO”) wdrażające art. 1B i 32A Regulaminu pracowniczego⁵ i mające zastosowanie do przetwarzania danych osobowych przez Urząd⁶.
9. Uzupełnieniem ODO są instrumenty wydawane przez Prezesa, w szczególności okólniki, wewnętrzne instrukcje administracyjne i decyzje (takie jak decyzja w sprawie państw i podmiotów zapewniających odpowiednią ochronę danych z 17 listopada 2022 r. oraz okólnik nr 420 wdrażający art. 25 ODO dotyczący ograniczeń praw osób, których dane dotyczą. Wszystkie te dokumenty są prawnie wiążące⁷.
10. Dalszym uzupełnieniem ODO są dokumenty operacyjne wydawane przez inspektora ochrony danych, w których określono procedury i szczegółowe wymogi w zakresie przetwarzania danych osobowych (art. 1 ust. 2 lit. c) ODO). Wszystkie te dokumenty operacyjne są częścią ram ochrony danych EPO i są jako takie prawnie wiążące i dostępne dla osób, których dane dotyczą, na stronie internetowej EPO.

1.2 Specyfika organizacji międzynarodowych

11. Zgodnie z art. 4 ust. 26 RODO organizacja międzynarodowa to „organizacja i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy”. Na gruncie prawa międzynarodowego status organizacji międzynarodowych jest zbliżony do statusu suwerennych państw, jednak – zgodnie z zasadą immunitetu funkcyjnego – organizacje międzynarodowe korzystają z przywilejów i immunitetów jedynie w zakresie niezbędnym do realizacji powierzonych im funkcji⁸. „Przywileje” na ogół obejmują zwolnienia z przepisów prawa materialnego danego państwa (np. zwolnienia podatkowe i celne), natomiast „immunitety” to zwolnienia z postępowania prawnego, egzekucji i środków wykonawczych.
12. Źródła przywilejów i immunitetów organizacji międzynarodowych mogą obejmować: traktaty wielostronne, umowy międzynarodowe ustanawiające daną organizację międzynarodową, umowy w

⁵ Regulamin pracowniczy reguluje aspekty dotyczące pracowników EPO, w tym prawa i obowiązki pracowników. Zob. w tej sprawie art. 33 konwencji. Tekst konwencji jest dostępny pod następującym adresem: https://link.epo.org/web/EPC_17th_edition_2020_en.pdf.

⁶ Przetwarzanie danych osobowych przez Radę Administracyjną EPO podlega przepisom Rady Administracyjnej o ochronie danych osobowych, natomiast przetwarzanie danych osobowych przez komisję specjalną podlega przepisom komisji specjalnej dotyczące ochrony danych osobowych. Przepisy Rady Administracyjnej o ochronie danych osobowych i przepisy komisji specjalnej dotyczące ochrony danych osobowych określają odpowiednio stosowanie ODO do przetwarzania danych osobowych przez Radę Administracyjną i komisję specjalną, z niezbędnymi modyfikacjami. W art. 145 konwencji wyjaśniono rolę komisji specjalnej.

⁷ Art. 10 konwencji, art. 1 ust. 2 lit. a) ODO oraz art. 3 lit. y) ODO.

⁸ Christopher Kuner, *International Organizations and the EU General Data Protection Regulation* [„Organizacje międzynarodowe i rozporządzenie o ochronie danych osobowych UE”], University of Cambridge Faculty of Law Legal Studies Research Paper Series, [Paper 20/2018](#).

sprawie siedziby zawarte z państwem przyjmującym oraz prawo i prawodawstwo krajowe. Przywileje i immunitety są zazwyczaj uznawane przez państwa należące do danej organizacji, chyba że państwa trzecie w sposób wyraźny lub dorozumiany uznały daną organizację międzynarodową w swoim prawie krajowym. Immunitet od jurysdykcji krajowej nie ma jednak charakteru absolutnego i wymaga, aby jednostki dysponowały rozsądnymi alternatywnymi środkami w celu skutecznej ochrony swoich praw⁹.

1.3 Przywileje i immunitety EPO

13. Przywileje i immunitety EPO reguluje „Protokół w sprawie przywilejów i immunitetów Europejskiej Organizacji Patentowej” (PPI) i obejmują między innymi pomieszczenia EPO (art. 1 PPI); nienaruszalność archiwów (art. 2 PPI); jurysdykcję i egzekucję (art. 3 ust. 1 lit. a) PPI), mienie i aktywa EPO, z wyłączeniem tych przypadków, w jakich może to być czasowo niezbędne w związku z zapobieganiem wypadkom w z udziałem pojazdów należących do Organizacji lub eksploatowanych w imieniu Organizacji oraz prowadzeniem dochodzeń w ich sprawie. (art. 3 ust. 3 PPI); zwolnienie z podatków (art. 4 PPI).
14. Immunitety EPO uzupełnia obowiązek współpracy między EPO a organami publicznymi umawiających się państw, określony w art. 20 PPI. Ponadto zgodnie z art. 19 ust. 2 PPI Prezes EPO zobowiązany jest do uchylecia immunitetu jeżeli uzna, że taki immunitet utrudnia zwykły tok wymiaru sprawiedliwości oraz że istnieje możliwość rezygnacji z takiego immunitetu bez naruszenia interesów Organizacji.

1.4 Zarządzanie ochroną danych w EPO

15. Zgodnie z art. 3 lit. g) ODO Europejski Urząd Patentowy pełni funkcję administratora¹⁰. Ramy ochrony danych EPO przewidują możliwość określenia przez administratora jednostek operacyjnych działających w charakterze „administratorów delegowanych” (art. 28 ust. 3 ODO). Zgodnie z art. 3 lit. h) ODO „administrator delegowany to jednostka operacyjna, reprezentowana przez jej kierownika, zapewniająca zgodność wszystkich operacji przetwarzania danych osobowych wykonywanych w danej jednostce operacyjnej z niniejszymi przepisami. Osoba reprezentująca jednostkę musi być kierownikiem wyższego szczebla, zazwyczaj co najmniej głównym dyrektorem”.
16. EROD wskazuje, że taka wewnętrzna struktura zarządzania jest powszechna w organizacjach międzynarodowych¹¹ biorąc pod uwagę rozmiar i charakter pracy organizacji międzynarodowych. Podobnie przedsiębiorstwa odnoszą korzyści z posiadania wewnętrznej struktury wspierającej zgodność z przepisami o ochronie danych¹².

⁹Wyrok ETPC w sprawie Waite i Kennedy przeciwko Niemcom, skarga nr 26083/94, wyrok z 18 lutego 1999 r., pkt 67–73.

¹⁰ W art. 28 ODO dokładniej omówiono kwestię administrowania danymi w EPO.

¹¹ Na przykład w przepisach Europejskiej Organizacji ds. Bezpieczeństwa Żeglugi Powietrznej (Eurocontrol) o ochronie danych zastosowano pojęcie „administratorów wewnętrznych” <https://www.eurocontrol.int/sites/default/files/2024-05/eurocontrol-regulation-personal-data-protection-2024.pdf>; Europejski Bank Inwestycyjny (EBI) stosuje termin „administrator” zarówno w odniesieniu do administratorów delegowanych, jak i do EBI jednak w tekście często wymienia się „właściwych administratorów”, co wskazuje na to, że chodzi o konkretny podmiot w ramach EBI; tekst jest dostępny pod linkiem:

https://www.eib.org/attachments/lucalli/20220237_data_protection_rules_implementing_eu_regulation_en.pdf

¹² Wytyczne 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO, wersja 2.1, przyjęte 7 lipca 2021 r.

17. EROD zauważa jednak, że ostateczna odpowiedzialność w przypadku naruszenia przepisów o ochronie danych powinna spoczywać na administratorze (tj. Europejskim Urzędzie Patentowym)¹³. W związku z powyższym EROD zwraca się do Komisji o dalsze wyjaśnienie tej kwestii.

2. OGÓLNE ASPEKTY OCHRONY DANYCH

2.1 Zasady dotyczące treści

18. Rozdział 3 dokumentu Grupy Roboczej Art. 29 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych poświęcony jest „zasadom dotyczącym treści” i przedstawione w nim są podstawowe pojęcia oraz zasady z zakresu ochrony danych osobowych. System państwa trzeciego lub organizacji międzynarodowej musi obejmować te podstawowe pojęcia i zasady, aby zapewnić stopień ochrony danych osobowych merytorycznie równoważny poziomowi gwarantowanemu w prawie UE. Nie jest konieczne odwzorowywanie terminologii RODO, jednak przyjęte pojęcia muszą odzwierciedlać pojęcia zawarte w unijnym prawodawstwie ochrony danych i być spójne z nimi. W dokumencie Grupy Roboczej Art. 29 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych wskazano następujące kluczowe pojęcia: „dane osobowe”, „przetwarzanie”, „administrator danych”, „podmiot przetwarzający dane”, „odbiorca” i „dane wrażliwe”.
19. EROD pozytywnie ocenia uznanie praw do prywatności i ochrony danych za prawa podstawowe zgodnie z ODO.

2.1.1 Pojęcia

20. EROD przyjmuje do wiadomości, że terminologia stosowana w ramach ochrony danych EPO jest zgodna z unijną terminologią ochrony danych. Choć pełna zgodność nie jest warunkiem koniecznym dla uznania równoważności, stanowi istotny atut i zasługuje na uznanie.
21. W odniesieniu do pojęć „administrator delegowany” i „jednostka operacyjna” oraz ich praktycznych konsekwencji EROD odsyła do sekcji 1.4 powyżej.

2.1.2 Zasady ochrony danych

22. Zasady ochrony danych określone w art. 4 ust. 2 i art. 6 ODO są bardzo zbliżone do zasad z odpowiednio art. 5 i art. 6 ust. 4 RODO. Podobnie podstawy prawne przetwarzania określone w art. 5, 7, 11 i 12 ODO odzwierciedlają podstawy prawne określone w art. 6 RODO oraz warunki przewidziane w art. 9 i 10 RODO¹⁴.
23. Zgodnie z art. 11 ust. 2 ODO, szczególne kategorie danych osobowych mogą być przetwarzane na warunkach zbliżonych do tych określonych w art. 9 RODO, z pewnymi wyjątkami wynikającymi z charakteru działalności EPO. Przykładowo, zgodnie z art. 11 ust. 2 lit. f) ODO. dane takie mogą być przetwarzane, gdy jest to konieczne do wykonania konkretnego zadania realizowanego w ramach czynności urzędowych Organizacji lub w ramach zgodnego z prawem sprawowania władzy publicznej powierzonej administratorowi.

¹³ Ibidem, pkt 17 i 18.

¹⁴ Zob. motywy 26–29 projektu decyzji.

24. W takich przypadkach jednak art. 11 ust. 2 lit. f) ODO przewiduje konkretne środki ochrony, aby zapewnić, aby odpowiedni stopień ochrony szczególnych kategorii danych osobowych nie został naruszony.
25. EROD pozytywnie ocenia fakt, że w odniesieniu do zasady celowości zgodność dalszych celów jest rozumiana podobnie zarówno w art. 4 ust. 2 lit. b) i art. 6 ODO, jak i w art. 5 ust. 1 lit. b) i art. 6 ust. 4 RODO.
26. Ponadto EROD pozytywnie ocenia włączenie zasady rozliczalności do art. 4 ust. 1 ODO oraz środków niezbędnych do wykazania zgodności, takich jak prowadzenie rejestrów (art. 32), obowiązek zgłaszania naruszeń ochrony danych (art. 34), ocena skutków dla ochrony danych (art. 38 ODO) oraz uwzględnienie ochrony danych w fazie projektowania lub domyślnej ochrony danych (art. 27 ust. 1 i 2 ODO), co zapewnia również zgodność z zasadami minimalizacji danych i konieczności. EROD pozytywnie ocenia fakt, że takie zasady i obowiązki są bardzo zbliżone do tych określonych w RODO.
27. Ponadto EROD pozytywnie ocenia fakt, że art. 4 ust. 1 ODO stanowi, iż administrator aktywnie i nieustannie wdraża środki mające na celu zapewnienie ochrony danych osobowych w swoich czynnościach przetwarzania, nakładając tym samym na siebie odpowiedzialność za przestrzeganie przepisów o ochronie danych i zobowiązując się do stałego wykazywania tej zgodności wobec osób, których dane dotyczą.

2.2 Prawa jednostek

28. EROD pozytywnie ocenia, że ODO zapewniają osobom fizycznym prawa odpowiadające tym określonym w RODO (art. 12–22), mianowicie prawo dostępu (art. 18 ODO), prawo do sprostowania danych (art. 19 ODO), prawo do usunięcia danych (art. 20 ODO), prawo do ograniczenia przetwarzania (art. 21 ODO), prawo do przenoszenia danych (art. 22 ODO), prawo do sprzeciwu (art. 23 ODO) oraz prawo, by nie podlegać zautomatyzowanemu podejmowaniu decyzji (art. 24 ODO). W ten sam sposób uznano prawo do informacji o ograniczeniu praw osób, których dane dotyczą (art. 23 ust. 2 lit. h) RODO), w art. 7 okólnika nr 420 wydanego przez Prezesa EPO.
29. Podobnie jak art. 23 RODO art. 25 ODO stanowi, że niektóre przepisy prawne wchodzące w zakres ram prawnych EPO mogą ograniczać stosowanie praw określonych w art. 18–25 ODO i przewiduje minimalną treść, którą powinny zawierać środki przewidujące ograniczenia. Taka minimalna treść odzwierciedla treść wymaganą przepisami RODO. Ponadto każda ocena potrzeby wprowadzenia ograniczeń musi być należycie udokumentowana.
30. Do tej pory EPO wdrożyła ten przepis w drodze okólnika nr 420, w którym wyjaśniono, jakie prawa mogą być ograniczane i w jakich celach. Wyjaśniono tam również, że ograniczenie powinno mieć charakter tymczasowy i że to do administratora należy ustalenie, czy w danych okolicznościach ograniczenie ma zastosowanie. W tym celu administrator przeprowadza indywidualną analizę konieczności i proporcjonalności, którą należy udokumentować i przekazać inspektorowi ochrony danych EPO. Inspektor ochrony danych ma prawo zażądać oceny ograniczenia, a administrator jest zobowiązany przedstawić wynik na piśmie.
31. EROD z zadowoleniem zauważa, że zgodnie z art. 25 ust. 2 i 4 ODO oraz art. 7 okólnika nr 420 osoby, których dane dotyczą, muszą zostać poinformowane o ograniczeniach, chyba że unieważniałoby to skutek ograniczenia (zgodnie z art. 23 RODO i art. 25 rozporządzenia PE i Rady UE 2018/1725), oraz o przysługującym im prawie do skonsultowania się z inspektorem ochrony danych w celu zakwestionowania ograniczeń oraz o ich prawach wynikających z art. 49 i 50 ODO (art. 25 ust. 3 lit. b)

ODO). W tym kontekście EROD pozytywnie ocenia fakt, że informacje o ograniczeniach praw osób, których dane dotyczą, są dostępne na stronie internetowej EPO zgodnie z art. 7 okólnika nr 420.

32. Ponadto EROD zauważa, że w związku z zadaniami EPO przewidziano pewne ograniczenia praw osób, których dane dotyczą. Na przykład EPO jest zobowiązany do prowadzenia Europejskiego Rejestru Patentowego, w którym publikowane są określone prawnie dane osobowe. Ograniczone jest również prawo do sprostowania i usunięcia danych: EPO nie może przewidywać możliwości sprostowania informacji, w tym danych osobowych, zawartych w dokumentach wykorzystywanych w procedurze udzielania patentów (tak jak ma to miejsce w przypadku dokumentów z zakresu postępowań urzędowych i prawnych, takich jak pozew lub odpowiedź na pozew); EPO musi natomiast przestrzegać konkretnych okresów przechowywania oraz wymogów dotyczących publikacji niektórych dokumentów wykorzystywanych w procedurze udzielania patentów (art. 129 lit. a) konwencji).
33. EROD zauważa, że ograniczenia praw osób, których dane dotyczą, przewidziane przez EPO sprowadzają się do tego, co jest absolutnie niezbędne i proporcjonalne dla zapewnienia prawidłowego przebiegu procedury udzielania patentów; jednocześnie pozostają zgodne z zasadą poszanowania istoty praw podstawowych i wolności osób, których dane dotyczą, oraz wymogami w zakresie konieczności i proporcjonalności, określonymi w Karcie praw podstawowych Unii Europejskiej („Karta”) i w Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności.

2.3 Ograniczenia dotyczące dalszego przekazywania danych

34. W dokumencie Grupy Roboczej Art. 29 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych w związku z RODO wyjaśniono, że stopień ochrony osób fizycznych, których dane osobowe są przekazywane na mocy decyzji stwierdzającej odpowiedni stopień ochrony, nie może być podważony przez dalsze przekazywanie danych; oznacza to, że każde dalsze przekazywanie 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 danych¹⁵. Pomimo że w ODO dokonano rozróżnienia między tak zwanym „przesyłaniem danych osobowych” a „przekazywaniem danych osobowych”, przypisując im odmienne zasady¹⁶, EROD podkreśla, że wymóg niepodważania stopnia ochrony ma zastosowanie do każdego dalszego przekazywania danych osobowych z UE, niezależnie od stosowanej terminologii.
35. EROD zauważa, że do „przekazywania danych osobowych” (zgodnie z definicją zawartą w art. 3 lit. t) ODO) zastosowanie mają przepisy zbliżone do przepisów rozdziału V RODO, co ma na celu zapewnienie, by stopień ochrony gwarantowany na mocy przepisów ODO nie został naruszony (art. 9 i 10 ODO).
36. EROD pozytywnie ocenia tę spójność z rozdziałem V RODO, a także fakt, że wytyczne dotyczące przekazywania danych opracowane przez inspektora ochrony danych odwołują się zarówno do wytycznych EROD, jak i do zmian w unijnych ramach prawnych¹⁷.

¹⁵ Grupa Robocza Art. 29, dokument WP 254 rev. 01, przyjęty 28 listopada 2017 r., ostatnio zmieniony i przyjęty 6 lutego 2018 r., zatwierdzony przez EROD, rozdział 3, A.9.

¹⁶ Zob. motywy 62–72 projektu decyzji.

¹⁷ [Nota wyjaśniająca „EPO – przesyłanie i przekazywanie danych osobowych” \(nota dot. przesyłania i przekazywania\) wersja ze stycznia 2024 r., część 3.2 \(s. 9\).](#)

37. W świetle powyższego EROD w swojej analizie skoncentrowała się na przepisach dotyczących drugiej kategorii przekazywania danych w ramach ODO, czyli „przesyłaniu danych osobowych”.

2.3.1 Przesyłanie danych osobowych

38. Zgodnie z art. 3 lit. s) ODO przez „przesyłanie danych osobowych” rozumie się „ujawnianie, rozpowszechnianie lub inne udostępnianie, w tym poprzez udzielenie dostępu, danych osobowych stronie w ramach Europejskiej Organizacji Patentowej, krajowemu urzędowi ds. własności przemysłowej lub innemu organowi publicznemu umawiającego się państwa konwencji o patencie europejskim, na warunkach określonych w art. 8”.
39. Art. 8 ust. 1 ODO stanowi, że przesyłanie danych osobowych organowi publicznemu umawiającego się państwa EPO może nastąpić, jeżeli dane te są konieczne do wykonywania zadań tego organu publicznego oraz zgodne z zadaniami i funkcjonowaniem EPO¹⁸. Art. 8 ust. 2 ODO zezwala na przesyłanie danych osobowych do krajowego urzędu ds. własności przemysłowej w umawiającym się państwie EPO, jeżeli dane te są niezbędne do realizacji zadań w ramach kompetencji odbiorcy oraz jeżeli wykonywanie jego władzy publicznej i przetwarzanie jest niezbędne do wykonywania zadań w ramach działalności urzędowej EPO lub w ramach uzasadnionego wykonywania władzy publicznej powierzonej administratorowi, co obejmuje przetwarzanie niezbędne do zarządzania EPO i jej funkcjonowania. Takie przesyłanie danych odbywa się w ramach procedury udzielania patentów przewidzianej w konwencji EPC i Układzie o współpracy patentowej¹⁹.
40. Odbiorcy muszą przedstawić dowody na to, że przesyłanie danych jest konieczne w konkretnym celu wynikającym z obowiązków EPO w zakresie współpracy z umawiającym się państwem; z kolei administrator – jeśli przesyłanie mogłoby naruszyć uzasadnione interesy osoby, której dane dotyczą – musi być w stanie wykazać, że przesłanie danych jest proporcjonalne do konkretnego celu, po wyważeniu różnych wchodzących w grę interesów (art. 8 ust. 3 i 4 ODO).
41. Aby w ramach narzędzi przesyłania danych zapewnić odpowiedni stopień ochrony, konkretne przepisy o ochronie danych powinny być zawarte w egzekwowalnych instrumentach, takich jak protokoły ustaleń czy porozumienia administracyjne²⁰. Inspektor ochrony danych EPO przygotował wzory klauzul ochrony danych do włączenia do protokołów ustaleń, obejmujące między innymi zasady ochrony danych, w tym ograniczenie celu, prawa osób, których dane dotyczą, oraz niezależny nadzór i odpowiednie mechanizmy egzekwowania²¹. EROD przyjmuje do wiadomości zastosowanie takich zabezpieczeń, zauważa jednak, że wymóg nienaruszania stopnia ochrony nie został wyraźnie wskazany w odniesieniu do przesyłania danych – ani w art. 8 ODO, ani w nocie wyjaśniającej EPO dotyczącej przesyłania i przekazywania danych osobowych, ani w projekcie decyzji stwierdzającej odpowiedni stopień ochrony. EROD zauważa natomiast, że wymóg ten jest wyraźnie wymieniony w kontekście przekazywania danych²² i zwraca się do Komisji o wyjaśnienie tej kwestii.

¹⁸ Zob. motyw 63 projektu decyzji; mogłoby to być do celu współpracy za pośrednictwem procesów konsultacji; delegowania i rozmieszczania ekspertów; dostarczania informacji na temat pracowników EPO do celów ustalania świadczeń z zabezpieczenia społecznego, wymogów podatkowych itp.

¹⁹ Zob. motyw 62, przypis 165 projektu decyzji oraz [decyzja prezesa Europejskiego Urzędu Patentowego z dnia 13 grudnia 2021 r. dotycząca przetwarzania danych osobowych w postępowaniach o udzielenie patentu i powiązanych postępowaniach \(Dz.U. Europejskiego Urzędu Patentowego 2021, A98\)](#).

²⁰ [Nota wyjaśniająca „EPO – przesyłanie i przekazywanie danych osobowych” \(nota dot. przesyłania i przekazywania\), wersja ze stycznia 2024 r.](#), s. 6.

²¹ [Przegląd wymogów zawartych we wzorach porozumień administracyjnych EPO, wersja z czerwca 2024 r.](#)

²² Zob. motyw 67 projektu decyzji.

42. Ponadto z dodatkowych wyjaśnień Komisji EROD wnioskuje, że wymóg stosowania odpowiednich gwarancji jako narzędzi przesyłania danych nie ma zastosowania w przypadku, gdy odbiorcą jest krajowy urząd ds. własności przemysłowej. A zatem w ocenie EROD nie jest w pełni jasne, jakie zabezpieczenia służące ochronie danych obowiązują, gdy dane osobowe są przesyłane w związku z procedurą udzielania patentów. Dlatego EROD zachęca Komisję do doprecyzowania także tego punktu.

2.4 Mechanizmy proceduralne i mechanizmy egzekwowania

43. Zgodnie z dokumentem Grupy Roboczej Art. 29 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych²³ oraz odpowiednim orzecznictwem TSUE²⁴ system ochrony danych merytorycznie równoważny z modelem unijnym musi charakteryzować się istnieniem następujących elementów: (i) niezależny organ, który powinien nadzorować i egzekwować zgodność z przepisami dotyczącymi ochrony danych, posiadać uprawnienia do prowadzenia dochodzeń i podejmować działania bez wpływu z zewnątrz; systemy ochrony danych muszą zapewniać (ii) rozliczalność administratorów danych i podmiotów przetwarzających oraz jasne określenie spoczywających na nich obowiązków informowania osób, których dane dotyczą, o przysługujących im prawach; należy wprowadzić skuteczne sankcje i procesy weryfikacji zapewniające zgodność z przepisami; (iii) wykazywanie zgodności z przepisami przez administratorów danych i podmioty przetwarzające za pomocą środków takich jak oceny skutków dla ochrony danych, prowadzenie rejestrów czynności przetwarzania danych oraz wyznaczenie inspektorów ochrony danych. Ponadto (iv) system ochrony danych musi zapewniać wsparcie i pomoc osobom, których dane dotyczą, w wykonywaniu przysługujących im praw i korzystaniu z odpowiednich mechanizmów dochodzenia roszczeń.
44. W zakresie zasady rozliczalności, o której mowa w pkt (ii) i (iii) poprzedniego akapitu, EROD odsyła do sekcji 2.1.2 powyżej.
45. W kolejnych sekcjach EROD skoncentrowała swoją ocenę na istnieniu niezależnego organu i odpowiednich mechanizmów dochodzenia roszczeń.

1.1

2.4.1 Inspektor ochrony danych i Rada Ochrony Danych

46. W ramach systemu przedstawionego przez EPO ustanawia się dwa odrębne organy odpowiedzialne za nadzór nad przestrzeganiem przepisów o ochronie danych: inspektora ochrony danych i Radę Ochrony Danych (art. 32A Regulaminu pracowniczego).
47. Inspektor ochrony danych EPO, oprócz pełnienia tradycyjnej funkcji IOD znanej z RODO, posiada również uprawnienia dochodzeniowe zgodnie z art. 43 ODO.
48. Rolą ROD jest zapewnienie niezależnego, skutecznego i bezstronnego nadzoru nad stosowaniem przepisów o ochronie danych. Osoby, których dane dotyczą, mają prawo złożyć skargę przed ROD w przypadku braku zgody na decyzję lub dorozumianego odrzucenia wniosku o dokonanie przeglądu przez administratora delegowanego (art. 50 ODO).

²³ Grupa Robocza Art. 29, dokument WP 254 rev. 01, przyjęty 28 listopada 2017 r., ostatnio zmieniony i przyjęty 6 lutego 2018 r., zatwierdzony przez EROD, rozdział 3, C.

²⁴TSUE, 6 października 2015 r., wyrok w sprawie C-362/14, Maximilian Schrems przeciwko Data Protection Commissioner („Schrems”).

49. Choć ta podwójna struktura, uzasadniona charakterem EPO, nie jest sama w sobie niepokojąca ani problematyczna, konieczne jest, aby oba organy działały w sposób w pełni niezależny, aby zapewnić skuteczny nadzór i egzekwowanie oraz miały wszelkie uprawnienia niezbędne do wykonywania swoich zadań.
50. W tym zakresie EROD skupiła się w swojej ocenie na faktycznej niezależności tych organów nadzoru oraz na ich uprawnieniach. Jeżeli chodzi o niezależność, EROD pozytywnie ocenia nie tylko język popierający tę zasadę w odpowiednich artykułach, ale również dodatkowe wprowadzone zabezpieczenia.
51. W powyższych ramach EROD przeanalizowała przepisy regulujące powoływanie, odwoływanie i zwalnianie IOD i ROD, a w szczególności wymóg, aby Prezes każdorazowo zasięgał opinii ROD przed proponowanym usunięciem lub odwołaniem IOD z jego funkcji.
52. EROD uważa, że takie uprzednie konsultacje stanowią potencjalne zabezpieczenie niezależności IOD, jednak charakter i skutki takich konsultacji pozostają niejasne. W związku z tym EROD zwraca się do Komisji o dalsze wyjaśnienie tej kwestii i rozważenie monitorowania podczas przyszłych przeglądów, czy IOD w praktyce nie jest zwalniany lub karany przez administratora za wykonywanie swoich obowiązków.
53. EROD zauważa, że zgodnie z art. 47 ODO ROD pełni funkcję nadzorczą i doradczą, ponieważ udziela administratorowi i administratorom delegowanym porad w związku ze stosowaniem art. 38 i 39 ODO, doradza w sprawie odwołania IOD na mocy art. 48 ust. 2 ODO oraz wydaje opinię w sprawie korzystania z mechanizmu dochodzenia roszczeń na mocy art. 50 ODO.
54. W odniesieniu do powoływania członków ROD EROD zauważa, że zgodnie z art. 48 ust. 1 ODO Rada Ochrony Danych składa się z trzech zewnętrznych ekspertów w dziedzinie ochrony danych powoływanych przez Prezesa Urzędu, mianowicie przewodniczącego i dwóch innych członków, z których jeden pełni funkcję wiceprzewodniczącego. Zgodnie z art. 48 ust. 2 ODO, przewodniczący, dwaj pozostali członkowie i zastępcy członków ROD muszą posiadać kwalifikacje wymagane do mianowania na stanowisko sędziowskie lub być specjalistami w dziedzinie ochrony danych posiadającymi udokumentowaną wiedzę fachową i doświadczenie w tej dziedzinie.
55. EROD pozytywnie ocenia fakt, że zasady wyboru członków organu nadzorczego wymagają wiedzy fachowej w dziedzinie ochrony danych, i zachęca Komisję do monitorowania, czy wybrani członkowie ROD rzeczywiście posiadają niezbędny poziom wiedzy fachowej w dziedzinie ochrony danych, biorąc pod uwagę jej znaczenie dla funkcji nadzorczej.

2.4.2 Uprawnienia dochodzeniowe i naprawcze

56. W tym kontekście TSUE wskazał, że uprawnienia organów nadzorczych stanowią środki niezbędne do wykonywania ich obowiązków; powinny one mieć w szczególności uprawnienia do przeprowadzenia dochodzenia, takie jak prawo do gromadzenia wszelkich informacji niezbędnych do wykonywania spoczywających na nich obowiązków nadzorczych, skuteczne uprawnienia do przeprowadzenia interwencji, takie jak możliwość nałożenia tymczasowego lub ostatecznego zakazu przetwarzania danych, oraz uprawnienie do brania udziału w postępowaniu sądowym²⁵.

²⁵ TSUE, 6 października 2015 r., wyrok w sprawie C-362/14, Maximilian Schrems przeciwko Data Protection Commissioner („Schrems”), pkt 43.

57. Zgodnie z art. 43 ust. 1 lit. d) inspektor ochrony danych może przeprowadzać kontrole ochrony danych (kontrole OD) i dochodzenia (prowadzone w formie inspekcji OD lub zapytań ad hoc)²⁶. Zgodnie z notą dotyczącą nadzoru nad ochroną danych²⁷, w której doprecyzowano art. 43 ODO, inspektor ochrony danych w porozumieniu z ROD przygotowuje roczny plan kontroli ochrony danych (plan) i przedkłada go do zatwierdzenia Prezesowi EPO. Zatwierdzony plan przekazuje się do wiadomości ROD. ROD może w dowolnym momencie sformułować sugestie dotyczące obszarów, w których Urząd powinien przeprowadzić kontrolę OD.
58. Zgodnie z art. 43 ust. 1 lit. i) ODO inspektor ochrony danych musi odpowiadać na wnioski ROD oraz współpracować i konsultować się z ROD na jej wniosek lub z własnej inicjatywy. Zgodnie z art. 43 ust. 1 lit. j) ODO inspektor ochrony danych jest zobowiązany ułatwiać współpracę między Radą Ochrony Danych a Urzędem między innymi w zakresie dochodzeń w sprawie ochrony danych, rozpatrywania skarg, ocen skutków dla ochrony danych i uprzednich konsultacji. IOD musi również przekazywać ROD informacje o nowych środkach administracyjnych i przepisach wewnętrznych dotyczących przetwarzania danych osobowych.
59. IOD wypełnia sprawozdanie z przeprowadzonych dochodzeń i kontroli, a w przypadku stwierdzenia niezgodności z przepisami o ochronie danych sprawozdanie musi zawierać ustalenia, wnioski i zalecenia (w tym środki zaradcze).
60. W szczególności zgodnie z notą dotyczącą nadzoru nad ochroną danych zalecenia mogą obejmować „środki zapobiegawcze, łagodzące lub naprawcze” dla administratora w przypadku nieprawidłowości lub niezgodności z przepisami. Inspektor ochrony danych może zalecić: zapewnienie zgodności operacji przetwarzania z przepisami ODO; rozpatrywanie wniosków osób, których dane dotyczą, o skorzystanie z przysługujących im praw w ramach ODO; poinformowanie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych; wstrzymanie konkretnej operacji przetwarzania danych; wstrzymanie przepływu danych do określonych odbiorców²⁸.
61. Zgodnie z notą dotyczącą nadzoru nad ochroną danych oraz decyzją Prezesa Urzędu z 12 lipca 2024 r.²⁹ wnioski i zalecenia mogą stać się wiążące (z zastrzeżeniem ich zatwierdzenia przez Radę) i muszą zostać wdrożone przez administratora. Zgodnie z notą dotyczącą nadzoru nad ochroną danych, która doprecyzowuje zasady zawarte w art. 43 ust. 1 lit. i) i j) ODO, ROD ma prawo zgłosić uwagi do wniosków i zaleceń oraz do żądania zmian, które powinien wdrożyć IOD. Ponadto IOD jest uprawniony do prowadzenia inspekcji pokontrolnych lub rozszerzania zakresu inspekcji ochrony danych, a także do zalecania wszczęcia postępowania administracyjnego w celu ustalenia, czy konieczne jest podjęcie działań dyscyplinarnych bądź innych środków.

²⁶ Uprawnienia dochodzeniowe IOD opisano szczegółowo w notce dotyczącej nadzoru nad ochroną danych *How the Data Protection Office Conducts DP Audits and DP Inspections* [„W jaki sposób biuro ochrony danych przeprowadza kontrole i inspekcje ochrony danych”], dostępnej na stronie internetowej EPO pod następującym adresem: <https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf>.

²⁷ *How the Data Protection Office Conducts DP Audits and DP Inspections* [„W jaki sposób biuro ochrony danych przeprowadza kontrole i inspekcje ochrony danych”], dokument dostępny na stronie internetowej EPO pod następującym adresem: <https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf>.

²⁸ Tamże.

²⁹ Decyzja Prezesa Urzędu w sprawie Egzekwowania Zaleceń IOD zatwierdzonych przez Radę Ochrony Danych w ramach Wniosków z Kontroli i Inspekcji Ochrony Danych, dostępna pod adresem: <https://link.epo.org/web/office/data-protection-and-privacy/en-decision-of-the-president-on-enforceability-of-dpo-conclusions-and-recommendations.pdf>.

62. Biorąc pod uwagę ścisły związek między IOD a ROD oraz znaczenie uprawnień dochodzeniowych, kontrolnych i naprawczych, EROD zaleca Komisji doprecyzowanie wzajemnych powiązań pomiędzy nimi, zwłaszcza w zakresie wykonywania uprawnień dochodzeniowych, kontrolnych i naprawczych, a także doprecyzowanie roli IOD w zakresie rozpatrywania wniosków osób, których dane dotyczą (art. 43 ust. 1 lit k ODO) oraz jego ewentualnej roli w procedurze dotyczącej skarg przed ROD zgodnie z art. 50 ODO. W szczególności EROD zwraca się do Komisji o monitorowanie, czy w praktyce istnieje wyraźne rozróżnienie, kiedy IOD działa we własnym imieniu, a kiedy działa w imieniu ROD, aby wspierać Radę w wykonywaniu jej funkcji nadzorczych. Zapewniłoby to dodatkową przejrzystość co do struktury nadzoru oraz roli IOD i ROD.

2.4.3 Procedura dotycząca skarg przed Radą Ochrony Danych

63. EROD zauważa, że osoby, których dane dotyczą, mają prawo złożyć skargę do Rady Ochrony Danych, która rozpatruje tą skargę zgodnie z procedurą określoną w art. 50 ODO oraz w regulaminie wewnętrznym stanowiącym załącznik nr 1 do ODO.
64. W szczególności po rozpatrzeniu skargi ROD wydaje uzasadnioną opinię skierowaną do administratora danych, w której może znaleźć się zalecenie przyznania odszkodowania za szkodę materialną lub niematerialną.
65. Zgodnie z art. 50 ust. 4 ODO uzasadnione opinie ROD (zwane dalej również „opinią”) nie są wiążące dla administratora, który może podjąć decyzję o ich niezastosowaniu. W takim przypadku administrator musi przedstawić pisemne uzasadnienie swojej decyzji, a także poinformować osobę, której dane dotyczą, administratora delegowanego, a w stosownych przypadkach również podmiot przetwarzający, inspektora ochrony danych i ROD o swojej ostatecznej decyzji i o wnioskach ROD. Decyzja (na którą składa się uzasadniona opinia ROD i ostateczna decyzja administratora) może zostać zaskarżona przez osobę, której dane dotyczą, poprzez zwrócenie się do Prezesa Urzędu o wszczęcie postępowania arbitrażowego, o którym mowa w art. 52 ODO, lub wniesienie sprawy do Trybunału Administracyjnego Międzynarodowej Organizacji Pracy.
66. Zgodnie z wytycznymi EROD, dokumentem Grupy Roboczej Art. 29 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych oraz orzecznictwem TSUE, organ nadzoru powinien dysponować wiążącymi uprawnieniami, ponieważ jest to kluczowy czynnik zapewniający skuteczność mechanizmu nadzoru.
67. EROD zauważa, że opinie ROD wydane w kontekście rozpatrywania skarg pozostają niewiążące. Pomimo że wnioski i zalecenia IOD wynikające z dochodzeń i kontroli, które mogły zostać wszczęte na wniosek ROD, mogą stać się wiążące po ich zatwierdzeniu przez ROD, nie wydaje się, aby miały one zastosowanie do spraw wszczętych na podstawie art. 50 ODO, czyli skarg osób, których dane dotyczą.
68. W związku z powyższym EROD zwraca się do Komisji o weryfikację i zapewnienie, aby uprawnienia ROD w zakresie rozpatrywania skarg były wiążące na podstawie art. 50 rozporządzenia o ochronie danych, oraz o ocenę, czy w tym celu można wprowadzić dodatkowe zabezpieczenia.
69. Jednakże EROD pozytywnie ocenia fakt, że od decyzji administratora podjętej zgodnie z art. 50 ust. 6 ODO przysługuje odwołanie, co gwarantuje osobom, których dane dotyczą, skuteczne dochodzenie roszczeń i umożliwia egzekwowanie decyzji organu nadzoru.
70. Ponadto EROD pozytywnie ocenia fakt, że ROD może zalecić przyznanie odszkodowania za szkodę materialną lub niematerialną (art. 50 ust. 3 ODO).

2.4.4 Mechanizmy dochodzenia roszczeń i arbitraż

71. Zgodnie z dokumentem Grupy Roboczej Art. 29 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych osobom, których dane dotyczą, należy zapewnić skuteczne mechanizmy dochodzenia roszczeń, w tym prawo do odszkodowania za szkody wynikające z niezgodnego z prawem przetwarzania danych osobowych. Jest to kluczowy element, który musi obejmować system niezależnego orzekania lub arbitrażu, pozwalający zarówno na wypłatę odszkodowania, jak i – w stosownych przypadkach – nałożenie sankcji.
72. EROD zwraca uwagę, że w ramach ochrony danych EPO osoby, których dane dotyczą, mogą zwrócić się do administratorów delegowanych o dokonanie przeglądu przetwarzania ich danych osobowych, jeśli uznają, że doszło do naruszenia przepisów o ochronie danych. Jest to warunek konieczny do złożenia skargi do ROD jako niezależnego organu nadzoru zgodnie z art. 50 ODO. Wymóg ten stanowi nowatorski element w porównaniu z unijnym systemem ochrony danych, który nie narusza jednak stopnia ochrony zapewnianej przez system EPO, ponieważ nie wpływa ani na egzekwowalność praw osób, których dane dotyczą, ani na ich prawo do odszkodowania.
73. Zgodnie z art. 50 i art. 52 ust. 1 ODO, jeżeli osoby, których dane dotyczą, nie są usatysfakcjonowane ostateczną decyzją podjętą wskutek procedury przewidzianej w art. 50 ODO, mogą się od niej odwołać. Pracownicy EPO mogą zaskarżyć decyzję do Trybunału Administracyjnego Międzynarodowej Organizacji Pracy. Każda inna osoba, której dane dotyczą, ma trzy miesiące na złożenie do Prezesa wniosku o wszczęcie postępowania arbitrażowego.
74. EROD pozytywnie ocenia przepisy dotyczące mechanizmu dochodzenia roszczeń. W odniesieniu do mechanizmu arbitrażu EROD zauważa, że możliwe jest zapewnienie alternatywnych sposobów rozwiązywania sporów, gdy mechanizmy sądowe nie są dostępne, na przykład ze względu na status administratora jako organizacji międzynarodowej. Takie mechanizmy muszą jednak zapewniać osobie, której dane dotyczą, gwarancje merytorycznie równoważne z tymi wynikającymi z art. 47 Karty³⁰. W związku z tym zapewnienie alternatywnego mechanizmu samo w sobie nie wiąże się z nieodłącznymi obawami czy problemami³¹ pod warunkiem że arbitraż (i) gwarantuje niezależne i bezstronne rozstrzygnięcie zgodnie z zasadami należytego procesu, (ii) jest wiążący dla administratora (EPO)³², (iii) umożliwi uzyskanie odszkodowania oraz (iv) pozwala na nałożenie sankcji w stosownych przypadkach.
75. Podobnie Europejski Trybunał Praw Człowieka orzekł, że skuteczne środki odwoławcze można zapewnić za pomocą „racjonalnych sposobów alternatywnych”, takich jak arbitraż³³.
76. EROD pozytywnie ocenia fakt, że ramy prawne EPO przewidują (i) zasady gwarantujące niezależność arbitra (art. 52 ust. 3 ODO), (ii) wiążący charakter mechanizmu arbitrażowego (art. 52 ust. 1 ODO), a także (iii) prawo do odszkodowania za szkody poniesione w wyniku naruszenia przepisów o ochronie

³⁰ TSUE, 16 lipca 2020 r., wyrok w sprawie C-311/18, Data Protection Commissioner przeciwko Facebook Ireland Ltd i Maximillian Schrems („Schrems II”), pkt 96 i 186 i nast.

³¹ Dokument w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych Grupy Roboczej Art. 29, przyjęty 28 listopada 2017 r., ostatnio zmieniony i przyjęty 6 lutego 2018 r. Wytyczne 2/2020 w sprawie art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) rozporządzenia 2016/679 dotyczącego przekazywania danych osobowych między organami podmiotami publicznymi z EOG i spoza EOG, wersja 2.0 przyjęta 15 grudnia 2020 r., pkt 53 i pkt 75.

³² TSUE, 6 października 2015 r., wyrok w sprawie C-362/14, Maximillian Schrems przeciwko Data Protection Commissioner

(„Schrems”), pkt 41 i 95. TSUE, 16 lipca 2020 r., wyrok w sprawie C-311/18, Data Protection Commissioner przeciwko Facebook Ireland Ltd i Maximillian Schrems („Schrems II”), pkt 186, 187, 189, 195 i nast.

³³ETPC, Sekcja piąta, decyzja, skarga nr 415/07. Roland KLAUSECKER przeciwko Niemcom, dokument dostępny pod następującym adresem: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-151029%22%5D%7D>.

danych (art. 53 ODO) oraz (iv) w stosownych przypadkach nałożenie sankcji (art. 11 regulaminu arbitrażowy Europejskiego Sądu Arbitrażowego³⁴).

77. Ponadto EROD pozytywnie ocenia fakt, że koszty arbitrażu ponosi EPO, co zapewnia, że osoby, których dane dotyczą, nie są obciążone zaporowymi kosztami w dochodzeniu swoich praw³⁵.

3. DOSTĘP ORGANÓW PUBLICZNYCH DO DANYCH OSOBOWYCH PRZEKAZYWANYCH Z UNII DO EUROPEJSKIEJ ORGANIZACJI PATENTOWEJ I ICH WYKORZYSTYWANIE

78. Na wstępie EROD podkreśla, że ocena dostępu organów publicznych do danych osobowych przekazywanych z Unii oraz sposobu ich wykorzystywania w obecnej sytuacji różni się od oceny stopnia ochrony zapewnianego przez państwo trzecie. Zamiast dokonywania oceny poszczególnych przepisów i praktyk państw trzecich dotyczących dostępu organów państwowych do danych w określonym scenariuszu, jakim jest decyzja dotycząca odpowiedniości ochrony danych osobowych zapewnianej przez organizację międzynarodową, należałoby dokonać przeglądu przepisów określających sposób, w jaki dana organizacja realizuje wnioski administracji rządowych o dostęp do danych osobowych, w tym zwłaszcza możliwość odmowy ich realizacji. Dlatego w odniesieniu do dostępu administracji rządowych do danych standard oceny merytorycznej równoważności różni się od stosowanego w poprzednich decyzjach stwierdzających odpowiedni stopień ochrony.
79. Jako dodatkowa wstępna uwaga EROD zwraca uwagę, że zgodnie z dodatkowymi wyjaśnieniami Komisji EPO nie otrzymała jak dotąd żadnego wniosku o dostęp do danych na potrzeby egzekwowania prawa lub bezpieczeństwa narodowego.
80. A fakt, że do tej pory w EPO nie złożono żadnych wniosków do celów egzekwowania prawa lub bezpieczeństwa narodowego, oznacza, że przepisy mające zastosowanie w tych przypadkach w odniesieniu do tej kwestii nie zostały jeszcze sprawdzone w praktyce. W związku z tym EROD zachęca Komisję do monitorowania, czy EPO będzie otrzymywała takie wnioski w przyszłości oraz jak te odpowiednie przepisy są wdrażane w tym specyficznym kontekście. Komisja mogłaby w szczególności zbadać, w jaki sposób zasady i standardy EPO mają zastosowanie do wniosków organów ścigania i agencji wywiadowczych, w tym wymóg przedstawienia dowodów, że przesłanie danych jest niezbędne w określonym celu wynikającym z obowiązku współpracy ze strony EPO (art. 8 ust. 3 ODO). Takie dowody będą z kolei dla EPO podstawą do ustalenia, czy przesyłanie danych jest rzeczywiście konieczne i proporcjonalne (art. 8 ust. 4 ODO)³⁶.

3.1 Rozpatrywanie przez EPO wniosków administracji rządowych o dostęp do danych osobowych

81. W projekcie decyzji wskazano, że ramy prawne, zgodnie z którymi EPO ocenia wnioski organów publicznych o dostęp do danych osobowych i odpowiada na nie, wynikają z PPI, wymogów ODO dotyczących przesyłania i przekazywania danych osobowych, a także z prawa międzynarodowego

³⁴ Regulamin arbitrażowy Europejskiego Sądu Arbitrażowego jest dostępny pod następującym adresem: <https://cour-europe-arbitrage.org/arbitration-rules/>

³⁵ Grupa Robocza Art. 29, dokument WP 254 rev. 01, przyjęty 28 listopada 2017 r., ostatnio zmieniony i przyjęty 6 lutego 2018 r., zatwierdzony przez EROD, pkt. 4.

³⁶ W kwestii ram prawnych dotyczących przesyłania informacji zob. również powyższe pkt 56 i 57 niniejszej opinii.

publicznego³⁷. Chociaż ramy te obowiązują zasadniczo w odniesieniu do wniosków pochodzących zarówno od umawiających się państw, jak i państw niebędących umawiającymi się państwami, szczegółowe przepisy ustanawiają inny system dla wniosków wydawanych przez organy publiczne umawiających się państw i inny dla państw niebędących umawiającymi się państwami.

82. Jeżeli chodzi o umawiające się państwa, immunitety EPO określone w PPI (zob. pkt 14) są uzupełnione o obowiązek współpracy. Art. 20 ust. 1 PPI stanowi, że EPO „stale współpracuje z właściwymi organami umawiających się państw w celu ułatwienia właściwego działania wymiaru sprawiedliwości, zapewnienia przestrzegania zarządzeń policji oraz przepisów dotyczących zdrowia publicznego, inspekcji pracy lub innych podobnych przepisów krajowych oraz w celu zapobieżenia wszelkim naruszeniom przywilejów, immunitetów i ułatwień przewidzianych w niniejszym protokole”³⁸. W tym celu, na podstawie art. 3 ust. 1 lit. a) PPI, EPO może zrzec się immunitetu jurysdykcyjnego i egzekucyjnego, aby odpowiedzieć na wnioski administracji rządowych o dostęp. EROD zwraca uwagę, że rzeczywiście trzeba będzie ustanowić mechanizmy współpracy z organami publicznymi umawiających się państw, które w niektórych przypadkach mogą służyć interesom osób, których dane dotyczą, np. w zakresie świadczeń socjalnych i kwestii ubezpieczeniowych pracowników EPO. Jednocześnie jednak w art. 20 ust. 1 PPI poruszono kwestię zależności lub powiązań pomiędzy obowiązkiem współpracy a pojęciem immunitetu, szczególnie w odniesieniu do wniosków o dostęp związanych z egzekwowaniem prawa i bezpieczeństwem narodowym. Komisja wskazała, że zasady EPO dotyczące współpracy, należy interpretować w szerszym kontekście ogólnej zasady immunitetu, a zatem EPO byłaby w stanie odrzucić takie wnioski w wyżej wymienionych celach, niezależnie od postanowień art. 20 ust. 1 PPI. EROD wzywa Komisję do dalszego wyjaśnienia tej kwestii w decyzji.
83. Decyzję dotyczącą wniosku o współpracę podejmuje Prezes Urzędu, który – jak wskazano w projekcie decyzji – korzysta przy tym z uprawnień dyskrejonalnych³⁹. Choć w projekcie decyzji jako podstawę prawną uchylecia immunitetu Organizacji wskazano art. 3 ust. 1 lit. a) PPI, nie określono jednoznacznie przepisu nadającego Prezesowi przedmiotowe uprawnienia dyskrejonalne oraz kryteriów korzystania z takich uprawnień przy podejmowaniu decyzji w sprawie wniosku o współpracę. EROD zauważa, że zgodnie z art. 19 ust. 2 PPI Prezes „zobowiązany jest do uchylecia immunitetu, jeżeli uzna, że taki immunitet utrudnia zwykły tok wymiaru sprawiedliwości oraz że istnieje możliwość rezygnacji z takiego immunitetu bez naruszenia interesów Organizacji.” Powstaje więc pytanie o zakres swobody Prezesa przy podejmowaniu takich decyzji. W związku z poprzednim akapitem EROD zwraca się zatem do Komisji o wyjaśnienie tych aspektów w decyzji.
84. Jeżeli EPO postanowi odpowiedzieć pozytywnie na wniosek o dostęp złożony przez umawiające się państwo zgodnie z art. 20 ust. 1 PPI, zastosowanie mają wymogi ODO dotyczące przesyłania danych (zob. pkt 38 i nast.)⁴⁰. Przepisy te dotyczą wszystkich umawiających się państw, niezależnie od tego, czy dane umawiające się państwo należy do EOG, czy jest uważane za państwo trzecie z punktu widzenia prawa UE dotyczącego ochrony danych. Niemniej jednak zasady przesyłania danych, w przeciwieństwie do systemu przewidzianego dla przekazywania danych organom publicznym spoza umawiających się państw EPO, nie wymagają w wyraźny sposób zapewnienia odpowiedniego stopnia ochrony przekazywanych danych, jaki należy zapewnić w kraju odbiorcy⁴¹. W tym zakresie EROD

³⁷ Zob. motyw 96 projektu decyzji.

³⁸ Z dodatkowych informacji przekazanych przez Komisję wynika, że EPO do tej pory nie stosowała uprawnień wynikających z art. 20 ust. 2 i art. 25 PPI do zawierania umów uzupełniających z umawiającymi się państwami w zakresie egzekwowania prawa lub bezpieczeństwa narodowego.

³⁹ Zob. motyw 97 projektu decyzji.

⁴⁰ Tamże.

⁴¹ Zob. motywy 63–65 projektu decyzji i art. 8 ODO.

pragnie przypomnieć swoje Wytyczne w sprawie art. 48 RODO⁴², które stanowią, że „w przypadku gdy dane przetwarzane w UE są przekazywane lub ujawniane w odpowiedzi na żądanie organu państwa trzeciego, takie ujawnienie podlega RODO i stanowi przekazanie w rozumieniu rozdziału V. Oznacza to, że podobnie jak w przypadku każdego przekazania podlegającego przepisom RODO, musi istnieć podstawa prawna przetwarzania na mocy art. 6 oraz podstawa przekazania określona w rozdziale V”⁴³. W tym zakresie EROD potwierdza swój wniosek o wyjaśnienie wyrażony w pkt 41 powyżej i zwraca się do Komisji o wyjaśnienie, jakie zabezpieczenia obowiązują również w odniesieniu do przesyłania danych na podstawie wniosków administracji rządowych o dostęp, zwłaszcza tych dotyczących egzekwowania prawa i bezpieczeństwa narodowego. Należy zapewnić, aby wymogi rozdziału V RODO, niezbędne do ustalenia merytorycznej równoważności, zostały dostatecznie uwzględnione, również w przypadkach, gdy koncepcja państw trzecich w unijnym prawie o ochronie danych i ramach prawnych EPO nie jest w pełni zbieżna⁴⁴.

85. Choć EROD przyznaje, że w nocie wyjaśniającej EPO dotyczącej przesyłania i przekazywania danych osobowych wskazano, że „aby w ramach narzędzi przesyłania danych zapewnić odpowiednie gwarancje, należy do egzekwowalnych instrumentów, takich jak protokoły ustaleń czy porozumienia administracyjne, wprowadzić szczegółowe przepisy dotyczące ochrony danych”⁴⁵, w praktyce wdrożenie takich narzędzi w odniesieniu do organów ścigania i krajowych agencji bezpieczeństwa może być niewykonalne. Z tego względu EROD uważa, że przesyłanie danych osobowych do umawiających się państw spoza EOG, zwłaszcza na potrzeby egzekwowania prawa i bezpieczeństwa narodowego, wymagałoby szczególnej uwagi ze strony Komisji.
86. Ponieważ nie ma instrumentu prawnego, który szczegółowo regulowałby rozpatrywanie przez EPO wniosków od organów publicznych państw niebędących umawiającymi się państwami, zastosowanie mają ogólne zasady przekazywania danych wynikające z ODO, które są bardzo podobne do tych określonych w rozdziale V RODO (zob. pkt 35 i 36).

3.2 Ograniczenie praw osób, których dane dotyczą

87. Art. 25 ODO stanowi, że szczegółowe przepisy ram prawnych EPO mogą – pod warunkiem ścisłego odzwierciedlenia wymogów art. 23 RODO – ograniczać stosowanie praw osób, których dane dotyczą (zob. pkt 33 i nast.). W kontekście dostępu administracji rządowej do danych EROD zauważa, że ograniczenie zawarte w okólniku nr 420 lit. h) może prowadzić do wykładni rozszerzającej, ponieważ odnosi się do przypadków „udzielania pomocy właściwym organom publicznym, w tym umawiającym się państwom EPO i organizacjom międzynarodowym, lub otrzymywania od nich pomocy”. Pomimo że EROD rozpoznaje, że zakres tego przepisu obejmuje wyłącznie pracowników EPO, EROD zachęca Komisję do monitorowania jego praktycznego stosowania.

⁴² Wytyczne EROD 02/2024 dotyczące art. 48 RODO, przyjęte 2 grudnia 2024 r.

⁴³ Tamże, pkt 9.

⁴⁴ Pomimo że EROD przyjmuje do wiadomości, że wszystkie umawiające się państwa są stronami EKPC i Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, przypomina ona jednak, że ratyfikacja tych instrumentów nie musi sama w sobie zapewniać merytorycznie równoważnego poziomu ochrony, ponieważ zależy to w szczególności od ich konkretnego wdrożenia w każdym kraju.

⁴⁵ [Nota wyjaśniająca „EPO – przesyłanie i przekazywanie danych osobowych” \(nota dot. przesyłania i przekazywania\), wersja ze stycznia 2024 r.](#), s. 6.

4. WDROŻENIE I MONITOROWANIE PROJEKTU DECYZJI

88. W odniesieniu do monitorowania i przeglądu decyzji stwierdzającej odpowiedni stopień ochrony EROD zauważa, że zgodnie z orzecznictwem TSUE „w związku z tym, że poziom ochrony zapewniony w państwie trzecim może zmieniać się w czasie, do Komisji należy, po przyjęciu decyzji stwierdzającej odpowiedni stopień ochrony na podstawie art. 45 RODO, okresowe badanie, czy przy uwzględnieniu stanu faktycznego i prawnego ustalenia poczynione co do odpowiedniego stopnia ochrony zapewnionego przez dane państwo trzecie lub organizację międzynarodową są nadal zasadne. Takie badanie należy przeprowadzić w każdym razie wówczas, gdy wyjdą na jaw okoliczności mogące wzbudzić co do tego wątpliwości”⁴⁶.
89. EROD uważa, że funkcja nadzorcza – i w szczególności uprawnienia dochodzeniowe i naprawcze – oraz dostęp administracji rządowej do danych przekazywanych z UE do EPO będą wymagały szczególnej uwagi podczas kolejnych okresowych badań. Komisja powinna również w trakcie monitorowania decyzji stwierdzającej odpowiedni stopień ochrony w większym stopniu skupić się na zmianach w przepisach uzupełniających ODO, takich jak decyzja Prezesa Europejskiego Urzędu Patentowego z 12 lipca 2024 r. w sprawie egzekwowania zaleceń IOD zatwierdzonych przez Radę Ochrony Danych w ramach kontroli i inspekcji ochrony danych, nota dotycząca nadzoru nad ochroną danych „How the Data Protection Office Conducts DP Audits and DP Inspections” [„W jaki sposób biuro ochrony danych przeprowadza kontrole i inspekcje ochrony danych”] oraz Nota wyjaśniająca „EPO – przesyłanie i przekazywanie danych osobowych”, wersja ze stycznia 2024 r.
90. EROD zauważa, że przegląd ustalenia dotyczącego stwierdzenia odpowiedniego stopnia ochrony będzie przeprowadzany co najmniej raz na cztery lata, zgodnie z art. 45 ust. 3 RODO.
91. W zakresie praktycznego udziału EROD i jej przedstawicieli w przygotowywaniu i prowadzeniu przyszłych przeglądów okresowych, EROD podkreśla, że wszelka istotna dokumentacja, w tym korespondencja, powinna być przekazywana EROD na piśmie z odpowiednim wyprzedzeniem w stosunku do przeglądów.
92. EROD pozytywnie ocenia fakt, że projekt decyzji przewiduje udział EROD w spotkaniu organizowanym przez Komisję i EPO, poświęconym przeglądzie funkcjonowania decyzji stwierdzającej odpowiedni stopień ochrony.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Anu Talus)

⁴⁶ TSUE, 6 października 2015 r., wyrok w sprawie C-362/14, Maximillian Schrems przeciwko Data Protection Commissioner („Schrems”), pkt 76. Zob. również projekt decyzji, motyw 105 i art. 3 ust. 5.