Opinia 15/2021 dotycząca projektu decyzji wykonawczej Komisji Europejskiej przyjętej na podstawie dyrektywy (UE) 2016/680 w sprawie odpowiedniego stopnia ochrony danych osobowych w Zjednoczonym Królestwie

Przyjęta 13 kwietnia 2021 r.

Historia wersji

Wersja 1.1	6 lipca 2021 r.	Zmiana formatowania
Wersja 1.0	13 kwietnia 2021 r.	Przyjęcie opinii

SPIS TREŚCI

Europejska Rada Ochrony Danych

uwzględniając art. 51 ust. 1 lit. g) 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 uchylająca decyzję ramową Rady 2008/977/WSiSW[1] (zwanej dalej „dyrektywą (UE) 2016/680(UE) 2016/680"),

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

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1 STRESZCZENIE

1. Komisja Europejska zatwierdziła swój projekt decyzji wykonawczej (zwany dalej „projektem decyzji") w sprawie odpowiedniego stopnia ochrony danych osobowych w Zjednoczonym Królestwie przyjęty na podstawie dyrektywy (UE) 2016/680 19 lutego 2021 r.[2]. Następnie Komisja Europejska rozpoczęła procedurę jego formalnego przyjęcia.

2. W tym samym dniu Komisja Europejska zwróciła się o opinię do Europejskiej Rady Ochrony Danych (zwanej dalej „EROD")[3]. EROD przeprowadziła ocenę odpowiedniego stopnia ochrony danych zapewnianego w Zjednoczonym Królestwie na podstawie analizy samego projektu decyzji, jak również na podstawie analizy dokumentacji udostępnionej przez Komisję Europejską.

3. Jako główny punkt odniesienia dla tych prac EROD wykorzystała swoje zalecenia w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680[4] przyjęte w dniu 2 lutego 2021 r., a także odpowiednie orzecznictwo odzwierciedlone w zaleceniach EROD 02/2020 dotyczących niezbędnych gwarancji europejskich dla środków nadzoru[5].

4. Podstawowym celem EROD jest przedstawienie Komisji Europejskiej opinii na temat odpowiedniego stopnia ochrony danych zapewnianego osobom fizycznym w Zjednoczonym Królestwie. Należy zauważyć, że EROD nie oczekuje, aby ramy prawne Zjednoczonego Królestwa powielały europejskie przepisy o ochronie danych.

5. EROD przypomina jednak, że w art. 36 dyrektywy (UE) 2016/680 oraz w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „TSUE") wymaga się, aby prawodawstwo państwa trzeciego było zgodne z istotą podstawowych zasad zapisanych w dyrektywie (UE) 2016/680, aby można je było uznać za zapewniające odpowiedni stopień ochrony. W obszarze ochrony danych EROD

[1] Dz.U. L 119 z 4.5.2016, s. 89.
[2] Zob. komunikat prasowy Komisji Europejskiej, komunikat prasowy, Ochrona danych: Komisja Europejska rozpoczyna procedurę dotycząca przepływu danych osobowych do Wielkiej Brytanii, 19 lutego 2021 r., https://ec.europa.eu/commission/presscorner/detail/pl/ip_21_661
[3] Tamże.
[4] Zob. zalecenia EROD 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680, przyjęte 2 lutego 2021 r., https://edpb.europa.eu/system/files/2021-05/recommendations012021onart.36led.pdf_pl.pdf.
[5] Zob. zalecenia EROD 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru, przyjęte 10 listopada 2020 r., https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_pl

zauważa, że istnieje duża zbieżność między ramami dyrektywy (UE) 2016/680 a ramami prawnymi Zjednoczonego Królestwa w zakresie niektórych podstawowych przepisów, takich jak np. przepisy dotyczące definicji pojęć (np. „dane osobowe"; „przetwarzanie danych osobowych"; „administrator danych"); podstaw zgodnego z prawem i rzetelnego przetwarzania danych do prawnie uzasadnionych celów; ograniczenia celu; jakości i proporcjonalności danych; zatrzymywania danych, ich bezpieczeństwa i poufności; przejrzystości; szczególnych kategorii danych; zautomatyzowanego podejmowania decyzji i profilowania.

6. EROD zaleca, aby Komisja Europejska uzupełniła swoją analizę o informacje dotyczące istnienia mechanizmu informowania właściwych organów państw członkowskich o dalszym przetwarzaniu lub ujawnianiu danych osobowych przez organy Zjednoczonego Królestwa, którym dane te zostały przekazane, oraz określiła jego skuteczność w ramach porządku prawnego Zjednoczonego Królestwa.

7. EROD uważa, że przepisy zawarte w części 3 rozdział 5 ustawy o ochronie danych z 2018 r. co do zasady zapewniają stopień ochrony merytorycznie równoważny stopniowi gwarantowanemu na mocy prawa UE, jeśli chodzi o przekazywanie danych osobowych przez organ ścigania Zjednoczonego Królestwa do państwa trzeciego.

8. Mimo że EROD odnotowuje zdolność Zjednoczonego Królestwa — zgodnie z jego ramami prawnymi — do uznawania terytoriów za zapewniające odpowiedni stopień ochrony danych w świetle ram ochrony danych Zjednoczonego Królestwa, EROD podkreśla, że może to prowadzić do potencjalnych zagrożeń w zakresie ochrony danych osobowych przekazywanych z UE, zwłaszcza jeśli w przyszłości ramy ochrony danych Zjednoczonego Królestwa będą odbiegać od dorobku prawnego UE. **W powyższych sytuacjach Komisja Europejska powinna zatem pełnić swoją rolę monitorującą, a w przypadku, gdy stopień ochrony danych osobowych przekazywanych z UE merytorycznie równoważny stopniowi przewidzianemu w UE nie zostanie utrzymany, Komisja Europejska powinna rozważyć zmianę decyzji stwierdzającej odpowiedni stopień ochrony w celu wprowadzenia szczególnych zabezpieczeń w odniesieniu do danych przekazywanych z UE lub zawieszenia decyzji stwierdzającej odpowiedni stopień ochrony.**

9. **Ponadto w odniesieniu do umów międzynarodowych zawartych między Zjednoczonym Królestwem a państwami trzecimi** zachęca się Komisję Europejską do zbadania zależności między ramami ochrony danych Zjednoczonego Królestwa a jego zobowiązaniami międzynarodowymi, w szczególności w celu zapewnienia ciągłości stopnia ochrony, w przypadku gdy dane osobowe są przekazywane z UE do Zjednoczonego Królestwa na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, a następnie przekazywane do innych państw trzecich; oraz do ciągłego monitorowania i podejmowania działań, w stosownych przypadkach, w przypadku gdyby zawarcie umów międzynarodowych między Zjednoczonym Królestwem a państwami trzecimi mogło zagrozić stopniowi ochrony danych osobowych przewidzianemu w UE.

10. W tym względzie EROD podkreśla, że wejście w życie umowy między Zjednoczonym Królestwem a Stanami Zjednoczonymi w sprawie dostępu do danych elektronicznych w celu zwalczania poważnych przestępstw (zwanej dalej „umową między Zjednoczonym Królestwem a USA na podstawie ustawy CLOUD Act")[6] może mieć wpływ na dalsze przekazywanie danych przez organy ścigania w Zjednoczonym Królestwie, w szczególności w odniesieniu do wydawania i przekazywania nakazów zgodnie z art. 5 umowy między Zjednoczonym Królestwem a USA na podstawie ustawy CLOUD.

[6] Zob. Umowa między rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej a rządem Stanów Zjednoczonych Ameryki w sprawie dostępu do danych elektronicznych w celu zwalczania poważnych przestępstw, zawarta 3 października 2019 r. w Waszyngtonie, D.C., w Stanach Zjednoczonych.

11. EROD zaleca również, aby Komisja Europejska monitorowała w sposób ciągły, czy zawarcie w przyszłości umów z państwami trzecimi w celu współpracy w zakresie egzekwowania prawa, stanowiących podstawę prawną dla przekazywania danych osobowych do tych państw, mogłoby wpłynąć na warunki dalszego udostępniania zgromadzonych informacji, w szczególności czy postanowienia tych umów międzynarodowych mogą mieć wpływ na stosowanie przepisów o ochronie danych Zjednoczonego Królestwa i przewidywać dalsze ograniczenia lub wyłączenia w odniesieniu do dalszego wykorzystywania i ujawniania za granicą informacji zgromadzonych w celu ścigania przestępstw. EROD uważa, że takie informacje i ocena są niezbędne, aby umożliwić kompleksowy przegląd stopnia ochrony zapewnianej przez ramy legislacyjne i praktyki Zjednoczonego Królestwa w odniesieniu do ujawniania informacji za granicą.

2 WPROWADZENIE

2,1 Ramy ochrony danych Zjednoczonego Królestwa

12. Ramy ochrony danych Zjednoczonego Królestwa są w dużej mierze oparte na unijnych ramach ochrony danych (w szczególności na dyrektywie (UE) 2016/680 i rozporządzeniu 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 (zwanym dalej „RODO")), co wynika z faktu, że Zjednoczone Królestwo było państwem członkowskim UE do 31 stycznia 2020 r. Co więcej, w części 3 ustawy o ochronie danych z 2018 r., która weszła w życie w dniu 23 maja 2018 r. i uchyliła ustawę o ochronie danych Zjednoczonego Królestwa z 1998 r., przewidziano transpozycję dyrektywy (UE) 2016/680, a ponadto doprecyzowano stosowanie RODO w prawie Zjednoczonego Królestwa, jak również przyznano uprawnienia krajowemu organowi nadzorczemu ds. ochrony danych, którym jest Urząd Rzecznika Informacji Zjednoczonego Królestwa (Information Commissioner's Office), i nałożono na niego obowiązki.

13. Jak wspomniano w motywie 12 projektu decyzji, rząd Zjednoczonego Królestwa uchwalił Ustawę o wystąpieniu z Unii Europejskiej z 2018 r., na mocy której włączono bezpośrednio stosowane przepisy UE do prawa Zjednoczonego Królestwa. Na mocy tej ustawy ministrowie Zjednoczonego Królestwa są uprawnieni do wprowadzania prawa wtórnego, za pomocą aktów prawnych, w celu dokonania niezbędnych zmian w utrzymanym prawie Unii po wystąpieniu Zjednoczonego Królestwa z UE, tak aby dostosować je do kontekstu krajowego.

14. W związku z tym odpowiednie ramy prawne mające zastosowanie w Zjednoczonym Królestwie po zakończeniu okresu przejściowego[7] obejmują:

- ogólne rozporządzenie o ochronie danych Zjednoczonego Królestwa (zwane dalej „rozporządzeniem o ochronie danych Zjednoczonego Królestwa"), włączone do prawa Zjednoczonego Królestwa na mocy Ustawy o wystąpieniu z Unii Europejskiej z 2018 r. i zmienione przez rozporządzenia o ochronie danych, prywatności i komunikacji elektronicznej (zmiany itp.) (w związku z wystąpieniem z UE) z 2019 r.;

[7] Okres przejściowy ustalono do dnia 31 grudnia 2020 r., po którym to dniu prawo Unii nie będzie już stosowane w Zjednoczonym Królestwie. Dodatkowy okres przejściowy (ang. *bridge period*) został ustalony najpóźniej do dnia 30 czerwca 2021 r. i odnosi się do dodatkowego okresu, w którym przekazywanie danych osobowych z UE do Zjednoczonego Królestwa nie jest uznawane za przekazywanie do państwa trzeciego.

- ustawę o ochronie danych z 2018 r., zmienioną rozporządzeniami o ochronie danych, prywatności i komunikacji elektronicznej (zmiany itp.) (w związku z wystąpieniem z UE) z 2019 oraz z 2020 r. oraz

- ustawę o uprawnieniach dochodzeniowo-śledczych z 2016 r. (Investigatory Power Act, zwana dalej „IPA 2016"),

(łącznie zwane „ramami ochrony danych Zjednoczonego Królestwa").

2,2 Zakres oceny przeprowadzonej przez EROD

15. Projekt decyzji Komisji Europejskiej jest wynikiem oceny ram ochrony danych Zjednoczonego Królestwa, która poprzedzała rozmowy z rządem Zjednoczonego Królestwa. Zgodnie z art. 51 ust. 1 lit. g) dyrektywy (UE) 2016/680 od EROD oczekuje się przedstawienia niezależnej opinii na temat ustaleń Komisji Europejskiej, określenia ewentualnych niedociągnięć w ramach oceny odpowiedniego stopnia ochrony danych oraz podjęcia starań w celu przedstawienia propozycji zaradzenia takim niedociągnięciom.

16. Jak wspomniano w zaleceniach w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680: „informacje dostarczone przez Komisję Europejską powinny być wyczerpujące i powinny umożliwić EROD dokonanie oceny stopnia ochrony danych osobowych w państwie trzecim"[8].

17. W tym względzie należy zauważyć, że EROD jedynie częściowo otrzymała na czas dokumenty niezbędne do przeprowadzenia analizy ram prawnych Zjednoczonego Królestwa. EROD otrzymała większość przepisów Zjednoczonego Królestwa, o których mowa w projekcie decyzji, za pośrednictwem linków zamieszczonych w tym projekcie. Komisja Europejska nie była w stanie przedstawić EROD pisemnych wyjaśnień i zobowiązań ze strony Zjednoczonego Królestwa w odniesieniu do wymiany informacji między władzami Zjednoczonego Królestwa a Komisją Europejską istotnych z punktu widzenia tego zadania[9].

18. Uwzględniając powyższe oraz z uwagi na ograniczony czas (2 miesiące) przyznany EROD na przyjęcie niniejszej opinii, EROD postanowiła skupić się na niektórych szczególnych elementach przedstawionych w projekcie decyzji i przedstawić swoją analizę i opinię na ich temat. Oczywiste jest, że analizując prawo i praktykę państwa trzeciego, które do niedawna było państwem członkowskim UE, EROD uznała wiele aspektów za merytorycznie równoważne tym przewidzianym w UE. Mając na uwadze swoją rolę w procesie przyjmowania ustaleń dotyczących zapewnienia odpowiedniego stopnia ochrony oraz szeroki zakres przepisów prawa i praktyk, które należy przeanalizować, EROD

[8] Zob. zalecenia 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680, pkt 15, s. 6.

[9] Chodzi o elementy, w przypadku których Komisja Europejska odnosi się w swoim projekcie decyzji do wyjaśnień władz Zjednoczonego Królestwa bez przedstawienia pisemnych dokumentów od władz Zjednoczonego Królestwa potwierdzających te wyjaśnienia, na przykład w odniesieniu do: skutków przepisów przejściowych oraz braku przepisu o wygaśnięciu (motyw 87); przykładów zgody jako właściwej podstawy przetwarzania danych (przypis 68); terminu „nieprawidłowe" oznaczającego „nieprawidłowe lub wprowadzające w błąd" dane osobowe (przypis 79); kompetencji Komisji ds. Wywiadu i Bezpieczeństwa (Intelligence and Security Committee – ISC) (przypis 245); niskiego progu wymaganego do złożenia skargi do Trybunału ds. Uprawnień Dochodzeniowo-Śledczych (Investigatory Powers Tribunal) oraz faktu, że często sąd ten stwierdza, iż skarżący w rzeczywistości nigdy nie był przedmiotem dochodzenia prowadzonego przez organ publiczny (przypis 263); połączenia uprawnień wynikających z prawodawstwa i prawa precedensowego (ang. *common law*) (przypis 52); prerogatyw rządu (przypis 62); faktu, że inne organizacje mogą stosować zasady kodeksu postępowania w zarządzaniu informacjami policyjnymi, jeżeli sobie tego życzą (przypis 86).

postanowiła skupić swoją uwagę na tych aspektach, w przypadku których dostrzegła największą potrzebę dokładniejszej analizy.

19. EROD uwzględniła obowiązujące europejskie ramy ochrony danych osobowych, w tym art. 7, 8 i 47 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą praw podstawowych UE"), chroniące odpowiednio prawo do życia prywatnego i rodzinnego, prawo do ochrony danych osobowych oraz prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu, a także art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności (zwanej dalej „EKPC") chroniący prawo do życia prywatnego i rodzinnego. Oprócz powyższego EROD wzięła pod uwagę wymogi dyrektywy (UE) 2016/680, jak również odpowiednie orzecznictwo.

20. Celem tego działania jest dostarczenie Komisji Europejskiej opinii na potrzeby oceny odpowiedniego stopnia ochrony danych osobowych w Zjednoczonym Królestwie. Pojęcie „odpowiedniego stopnia ochrony", które istniało już na gruncie dyrektywy 95/46/WE, zostało rozwinięte przez TSUE. Należy przypomnieć normę ustanowioną przez TSUE w wyroku w sprawie Schrems I, zgodnie z którą – choć „poziom 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"[10]. W związku z tym celem nie jest dokładne powielanie prawodawstwa europejskiego, lecz ustalenie zasadniczych i podstawowych wymogów analizowanego prawodawstwa. Odpowiedni stopień ochrony danych można osiągnąć poprzez 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 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 wprowadzonego w celu zapewnienia skuteczności tych przepisów. Skuteczne mechanizmy egzekwowania prawa mają pierwszorzędne znaczenie dla skuteczności przepisów o ochronie danych[11].

2,3 Uwagi i zastrzeżenia ogólne

2.3.1 Zobowiązania międzynarodowe zaciągnięte przez Zjednoczone Królestwo

21. Zgodnie z art. 36 ust. 2 lit. c) dyrektywy (UE) 2016/680 i zaleceniami w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy tej dyrektywy[12], oceniając odpowiedni stopień ochrony danych w państwie trzecim, Komisja Europejska bierze pod uwagę m.in. międzynarodowe zobowiązania państwa trzeciego lub inne obowiązki wynikające z jego udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych, a także realizację takich obowiązków. Ponadto należy wziąć pod uwagę przystąpienie państwa trzeciego do Konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym

[10] Zob. wyrok TSUE z dnia 6 października 2015 r., Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, (zwany dalej „Schrems I"), pkt 73–74.
[11] Zob. zalecenia EROD 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680, pkt 14, s. 5.
[12] Zob. zalecenia EROD 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680, pkt 24, s. 7.

przetwarzaniem danych osobowych (zwanej dalej „konwencją 108”)[13] oraz protokołu dodatkowego do tej konwencji[14].

22. **W tym względzie EROD z zadowoleniem przyjmuje fakt, że Zjednoczone Królestwo przystąpiło do Konwencji o ochronie praw człowieka i podstawowych wolności i podlega jurysdykcji Europejskiego Trybunału Praw Człowieka. Ponadto Zjednoczone Królestwo przystąpiło również do konwencji 108 i protokołu dodatkowego do tej konwencji, a w 2018 r. podpisało konwencję 108+[15] i obecnie pracuje nad jej ratyfikacją.**

2.3.2 Możliwe przyszłe rozbieżności ram ochrony danych Zjednoczonego Królestwa

23. Jak wspomniano w motywie 171 projektu decyzji, Komisja Europejska musi wziąć pod uwagę, że wraz z końcem okresu przejściowego przewidzianego w umowie o wystąpieniu[16], Zjednoczone Królestwo stosuje i egzekwuje własny system ochrony danych oraz zarządza nim, a gdy tylko przestanie obowiązywać przepis przejściowy[17] na mocy art. FINPROV.10A umowy o handlu i współpracy między Zjednoczonym Królestwem a UE[18], może to w szczególności pociągnąć za sobą poprawki lub zmiany ram ochrony danych ocenionych w projekcie decyzji, jak również inne istotne zmiany.

24. Komisja Europejska postanowiła zatem włączyć do projektu decyzji klauzulę wygaśnięcia[19], ustalając datę wygaśnięcia decyzji na cztery lata po jej wejściu w życie.

25. Należy zauważyć, że możliwość wprowadzenia przez ministrów i sekretarza stanu Zjednoczonego Królestwa prawodawstwa wtórnego po zakończeniu dodatkowego okresu przejściowego może doprowadzić w przyszłości do znacznej rozbieżności między ramami ochrony danych Zjednoczonego Królestwa a ramami unijnymi.

26. Ponadto od zakończenia okresu przejściowego Zjednoczone Królestwo nie tylko nie jest już związane orzecznictwem TSUE, ale również wydane już wyroki TSUE, uważane za zachowane orzecznictwo w ramach prawnych Zjednoczonego Królestwa, mogą nie być już wiążące dla Zjednoczonego Królestwa, zwłaszcza z uwagi na fakt, że Zjednoczone Królestwo ma możliwość zmiany zachowanego prawa Unii po zakończeniu dodatkowego okresu przejściowego, a jego Sąd Najwyższy nie jest związany żadnym zachowanym orzecznictwem UE[20].

---

[13] Zob. Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, konwencja 108, 28 stycznia 1981 r.

[14] Zob. Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych, sporządzony w dniu 8 listopada 2001 r.

[15] Zob. Protokół zmieniający Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (zwany dalej „konwencją 108+”) z dnia 18 maja 2018 r.

[16] Zob. Umowa o wystąpieniu Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej z Unii Europejskiej i Europejskiej Wspólnoty Energii Atomowej (Dz.U. L 029 z 31.1.2020, s. 7).

[17] Okres przejściowy ustalono do dnia 31 grudnia 2020 r., po którym to terminie prawo Unii nie będzie już stosowane w Zjednoczonym Królestwie. Dodatkowy okres przejściowy (ang. *bridge period*) został ustalony najpóźniej do dnia 30 czerwca 2021 r. i odnosi się do dodatkowego okresu, w którym przekazywanie danych osobowych z UE do Zjednoczonego Królestwa nie jest uznawane za przekazywanie do państwa trzeciego.

[18] Zob. Umowa o handlu i współpracy między Unią Europejską i Europejską Wspólnotą Energii Atomowej, z jednej strony, a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej, z drugiej strony (Dz.U. L 444 z 31.12.2020, s. 14).

[19] Zob. art. 4 projektu decyzji. Zob. również motyw 172 projektu decyzji.

[20] Zob. art. 6 ust. 3 do 6 umowy o wystąpieniu z UE z 2018 r.

27. **Mając na uwadze ryzyko związane z ewentualnymi rozbieżnościami między ramami ochrony danych Zjednoczonego Królestwa a dorobkiem prawnym UE po zakończeniu dodatkowego okresu przejściowego, EROD z zadowoleniem przyjmuje decyzję Komisji Europejskiej o wprowadzeniu do projektu decyzji czteroletniej klauzuli wygaśnięcia. EROD pragnie jednak podkreślić znaczenie monitorującej roli Komisji Europejskiej[21]. Komisja Europejska powinna monitorować na bieżąco i w sposób ciągły wszystkie istotne zmiany w Zjednoczonym Królestwie, które mogą mieć wpływ na niezbędną odpowiedniość stopnia ochrony danych osobowych przekazywanych na mocy decyzji stwierdzającej odpowiedni stopień ochrony w Zjednoczonym Królestwie, począwszy od momentu wejścia w życie tej decyzji. Ponadto Komisja Europejska powinna podjąć odpowiednie działania poprzez zawieszenie, zmianę lub uchylenie decyzji stwierdzającej odpowiedni stopień ochrony, w zależności od okoliczności, jeżeli po przyjęciu decyzji stwierdzającej odpowiedni stopień ochrony Komisja Europejska odnotuje sygnały świadczące o tym, że w Zjednoczonym Królestwie nie jest już zapewniony odpowiedni stopień ochrony.**

28. Ze swojej strony EROD dołoży wszelkich starań, aby informować Komisję Europejską o wszelkich istotnych działaniach podejmowanych przez organy nadzorcze ds. ochrony danych w państwach członkowskich (zwane dalej „organami nadzorczymi"), a w szczególności o skargach składanych przez osoby, których dane dotyczą, w UE dotyczących przekazywania danych osobowych z UE do Zjednoczonego Królestwa.

3 PRZEPISY MAJĄCE ZASTOSOWANIE DO PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ WŁAŚCIWE ORGANY DO CELÓW ŚCIGANIA PRZESTĘPSTW

3,1 Zakres przedmiotowy

29. W odniesieniu do motywu 24 i następnych motywów projektu decyzji EROD zauważa, że projekt decyzji stwierdzającej odpowiedni stopień ochrony danych zawiera niewiele szczegółów dotyczących działań i ram prawnych mających zastosowanie do agencji innych niż policja, wykonujących obowiązki w zakresie ścigania przestępstw.

30. Na przykład w „Ramach wyjaśniających Zjednoczonego Królestwa na potrzeby dyskusji na temat odpowiedniego stopnia ochrony", w sekcji F dotyczącej ścigania przestępstw[22] na stronie 11 zasugerowano, że **Krajowa Agencja ds. Przestępczości** (National Crime Agency, zwana dalej „NCA") mogłaby być szczególnie istotnym organem ścigania, który między innymi pełni szerszą funkcję w zakresie wywiadu kryminalnego. NCA określa swoją misję jako gromadzenie danych wywiadowczych z różnych źródeł w celu zmaksymalizowania analiz, ocen i możliwości taktycznych, w tym uzyskanych w ramach technicznego przechwytywania komunikacji oraz od partnerów zajmujących się ściganiem przestępstw w Zjednoczonym Królestwie i za granicą, agencji bezpieczeństwa i wywiadu[23]. NCA jest

[21] Zob. art. 36 ust. 4 dyrektywy (UE) 2016/680.

[22] Zob. rząd Zjednoczonego Królestwa, „Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement" [„Ramy wyjaśniające na potrzeby dyskusji na temat odpowiedniego stopnia ochrony, sekcja F: ściganie przestępstw"], 13 marca 2020 r. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf

[23] Zob. strona internetowa NCA, „Intelligence: enhancing the picture of serious organised crime affecting the UK" [„Wywiad: poprawa obrazu sytuacji w zakresie poważnej przestępczości zorganizowanej dotykającej

również jednym z głównych podmiotów w kontaktach z międzynarodowymi partnerami w dziedzinie ścigania przestępstw i odgrywa kluczową rolę w wymianie danych wywiadowczych dotyczących przestępstw[24].

31. EROD odnotowuje ponadto fakt, że Centrala Łączności Rządowej (Government Communications Headquarters, zwana dalej „GCHQ"), której działania zazwyczaj wchodzą w zakres części 4 ustawy o ochronie danych z 2018 r., tj. dotyczącej bezpieczeństwa narodowego, przyjmuje również aktywną rolę w ograniczaniu szkód społecznych i finansowych, jakie poważna i zorganizowana przestępczość wyrządza w Zjednoczonym Królestwie, ściśle współpracując z Ministerstwem Spraw Wewnętrznych (Home Office), NCA, Królewskim Urzędem Podatkowym i Celnym (HM Revenue and Customs, HMRC) i innymi departamentami rządowymi[25]. Jej działalność dotyczy zwalczania niegodziwego traktowania dzieci w celach seksualnych, nadużyć finansowych, innych rodzajów przestępstw gospodarczych, w tym prania pieniędzy, przestępczego wykorzystywania technologii, cyberprzestępczości, zorganizowanej przestępczości imigracyjnej, w tym handlu ludźmi, oraz handlu narkotykami, bronią palną i innych nielegalnych działań przemytniczych.

32. **EROD wzywa Komisję Europejską do uzupełnienia jej analizy o analizę agencji działających w dziedzinie ścigania przestępstw, które, jak się wydaje, uczyniły gromadzenie i analizę danych, w tym danych osobowych, centralnym punktem swojej codziennej działalności, w szczególności NCA. Ponadto EROD zachęca Komisję, aby bliżej przyjrzała się agencjom takim jak GCHQ, których działalność wchodzi w zakres zarówno ścigania przestępstw, jak i bezpieczeństwa narodowego, oraz podlega ramom prawnym mającym do nich zastosowanie w odniesieniu do przetwarzania danych osobowych.**

3,2 Zabezpieczenia, prawa i obowiązki

3.2.1 Przetwarzanie na podstawie „zgody" osoby, której dane dotyczą

33. EROD odnotowuje, że Komisja Europejska stwierdza w motywach 37 i 38 projektu decyzji, że **poleganie na zgodzie** nie jest uważane za istotne w scenariuszu dotyczącym odpowiedniego stopnia ochrony, ponieważ w sytuacjach przekazywania danych organ ścigania Zjednoczonego Królestwa nie zbiera danych bezpośrednio od osoby, której dane dotyczą, na podstawie zgody.

Zjednoczone Królestwo"], https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk

[24] Chociaż nie wszystkie dane wywiadowcze przetwarzane przez NCA są danymi osobowymi, znaczna ich część może stanowić takie dane, a opisane w tej części działania różnią się od klasycznych działań policyjnych, a zatem ocena dostępu do danych osobowych przez organy ścigania w Zjednoczonym Królestwie nie byłaby kompletna bez dokładnej oceny działań NCA. Rozsądne wydaje się dopilnowanie, aby zasady ochrony danych były interpretowane w taki sam sposób we wszystkich właściwych organach ścigania, co pozwoliłoby rzucić światło na agencję, której działalność w szczególności opiera się na danych, jaką jest NCA. Ponadto w sekcji dotyczącej przyszłych działań przedstawiono ciąg dalszy wyjaśnienia: „[n]ieustannie poszukujemy nowych możliwości gromadzenia, rozwijania i wzmacniania tradycyjnych zdolności w celu zwiększenia ilości i jakości danych wywiadowczych dostępnych do wykorzystania zarówno w Zjednoczonym Królestwie, jak i za granicą. W ramach tych działań rozwijamy nową Krajową Zdolność Wykorzystywania Danych, wykorzystując uprawnienia nadane agencji na mocy ustawy o zwalczaniu przestępczości i sądach, na potrzeby uzyskiwania dostępu do informacji przechowywanych przez różne departamenty rządu oraz łączenia ich i wykorzystywania. [...] Wszystkie te działania pozwolą zwiększyć naszą sprawność i elastyczność, aby reagować na nowe zagrożenia i działać w sposób proaktywny, gromadzić i analizować informacje i dane wywiadowcze na temat pojawiających się zagrożeń, abyśmy mogli działać, zanim zagrożenia się zmaterializują".

[25] Zob. strona internetowa GCHQ, sekcja poświęcona misjom w zakresie zwalczania poważnej i zorganizowanej przestępczości, https://www.gchq.gov.uk/section/mission/serious-crime

34. W tym względzie EROD przypomina, że art. 36 ust. 2 lit. a) dyrektywy (UE) 2016/680 zawiera wymóg, aby ocena uwzględniała szeroki wachlarz elementów, które nie ograniczają się do sytuacji przekazywania danych, w tym „praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie prawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie [...] prawa karnego".

35. Zgoda w kontekście ścigania przestępstw może być istotna jako podstawa prawna przetwarzania danych, jako dodatkowe zabezpieczenie lub – bardziej ogólnie – jako podstawa do wykonania uprawnień w zakresie prowadzenia postępowań, które to uprawnienia wiążą się z uzyskaniem danych osobowych, np. zgody osoby trzeciej na przeszukanie jej pomieszczeń lub konfiskatę przechowywanych danych.

36. EROD zauważa, opierając się również na informacjach dostarczonych przez Komisję Europejską w motywie 38 projektu decyzji, że wykorzystanie zgody, tak jak zostało to ujęte w systemie Zjednoczonego Królestwa, zawsze wymagałoby podstawy prawnej, na którą można by się powołać. Oznacza to, że nawet jeśli policja posiada ustawowe uprawnienia do przetwarzania danych w celu prowadzenia dochodzenia, w pewnych szczególnych okolicznościach (np. w celu pobrania próbki DNA) może ona uznać za stosowne zwrócenie się o zgodę osoby, której dane dotyczą.

37. **EROD zachęca Komisję Europejską do przeanalizowania, co do zasady, możliwości wykorzystania zgody w kontekście ścigania przestępstw przy ocenie, czy stopień ochrony w państwie trzecim jest odpowiedni na podstawie dyrektywy (UE) 2016/680.**

3.2.2 Prawa indywidualne

3.2.2.1 Certyfikaty bezpieczeństwa narodowego

38. Zgodnie z art. 79 ustawy o ochronie danych z 2018 r. administratorzy mogą ubiegać się o certyfikaty bezpieczeństwa narodowego wydawane przez ministra, członka gabinetu, prokuratora generalnego lub rzecznika generalnego ds. Szkocji, poświadczające, że ograniczenia obowiązków i praw zapisanych w części 3 rozdział 3 i 4 ustawy o ochronie danych z 2018 r. są niezbędnym i proporcjonalnym środkiem ochrony bezpieczeństwa narodowego.

39. Certyfikaty te mają na celu zapewnienie administratorom większej pewności prawa i będą stanowiły rozstrzygający dowód na to, że przy przetwarzaniu danych osobowych uwzględniane są kwestie dotyczące bezpieczeństwa narodowego. Należy jednak wspomnieć, że certyfikaty te nie są wymagane w celu powołania się na ograniczenia związane z bezpieczeństwem narodowym, lecz stanowią środek zapewniania przejrzystości[26].

40. EROD wnioskuje na podstawie pkt 17 i 18 załącznika 20 do ustawy o ochronie danych z 2018 r., że na potrzeby przetwarzania danych osobowych na podstawie ustawy o ochronie danych z 2018 r. okres obowiązywania certyfikatu bezpieczeństwa narodowego wydanego na podstawie ustawy o ochronie danych osobowych z 1998 r. (zwanego dalej „starym certyfikatem") przedłużono do dnia 25 maja 2019 r. Do tego dnia stare certyfikaty, o ile nie zostały zastąpione lub cofnięte, były traktowane tak, jakby zostały wydane na podstawie ustawy o ochronie danych z 2018 r. EROD wnioskuje jednak, że w przypadku braku wyraźnego wskazania daty wygaśnięcia ważności na certyfikacie bezpieczeństwa

[26] Zob. Ministerstwo Spraw Wewnętrznych (Home Office) Zjednoczonego Królestwa, ustawa o ochronie danych z 2018 r., wytyczne dotyczące certyfikatów bezpieczeństwa narodowego, sierpień 2020 r., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf, s. 4.

narodowego wydanym na podstawie ustawy o ochronie danych z 1998 r. taki certyfikat będzie nadal obowiązywać w odniesieniu do przetwarzania danych zgodnie ustawą o ochronie danych z 1998 r., chyba że zostanie cofnięty lub unieważniony[27]. Mimo że ochrona zapewniana przez te stare certyfikaty ogranicza się do przetwarzania danych osobowych na podstawie ustawy o ochronie danych z 1998 r., EROD odnotowuje fakt, że nowe certyfikaty bezpieczeństwa narodowego mogą być wydawane na mocy ustawy o ochronie danych z 1998 r. w odniesieniu do danych osobowych, które były przetwarzane na podstawie ustawy o ochronie danych z 1998 r.[28]

41. **W celu zarysowania pełnego obrazu sytuacji EROD zwraca się do Komisji Europejskiej o doprecyzowanie w projekcie decyzji stwierdzającej odpowiedni stopień ochrony, że certyfikaty bezpieczeństwa narodowego mogą być nadal wydawane na podstawie ustawy o ochronie danych z 1998 r. EROD zwraca się również do Komisji Europejskiej o przedstawienie w projekcie decyzji stwierdzającej odpowiedni stopień ochrony opisu mechanizmu dochodzenia roszczeń i mechanizmu nadzoru w odniesieniu do certyfikatów wydanych na podstawie ustawy o ochronie danych z 1998 r. Ponadto EROD zwraca się do Komisji Europejskiej o uwzględnienie w projekcie decyzji stwierdzającej odpowiedni stopień ochrony liczby istniejących certyfikatów wydanych na podstawie ustawy o ochronie danych z 1998 r. oraz do uważnego monitorowania tego aspektu.**

3.2.2.2 Zautomatyzowane podejmowanie decyzji na podstawie dyrektywy (UE) 2016/680

42. EROD podkreśla, że w art. 11 ust. 3 dyrektywy (UE) 2016/680 ustanowiono zakaz profilowania skutkującego dyskryminacją osób fizycznych na podstawie danych osobowych szczególnych kategorii. EROD zauważa jednak, że art. 50 ustawy o ochronie danych z 2018 r., w którym określono szczegółowe przepisy dotyczące zautomatyzowanego podejmowania decyzji, nie przewiduje takiego zakazu.

43. **EROD zwraca się zatem do Komisji Europejskiej o zweryfikowanie tego punktu i wyraźne przedstawienie ustaleń w decyzji stwierdzającej odpowiedni stopień ochrony. Ponadto EROD zachęca Komisję Europejską do ścisłego monitorowania spraw związanych ze zautomatyzowanym podejmowaniem decyzji i profilowaniem.**

44. Zgodnie z zaleceniami w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680 „[p]rawo 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[29].

45. **EROD wzywa Komisję do oceny tego elementu w świetle wytycznych przedstawionych przez EROD w jej zaleceniach.**

3.2.3 Dalsze przekazywanie danych

46. Zgodnie z zaleceniami w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na podstawie dyrektywy (UE) 2016/680 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

[27] Zob. Ministerstwo Spraw Wewnętrznych (Home Office) Zjednoczonego Królestwa, ustawa o ochronie danych z 2018 r., wytyczne dotyczące certyfikatów bezpieczeństwa narodowego, sierpień 2020 r., s. 5.
[28] Zob. Ministerstwo Spraw Wewnętrznych (Home Office) Zjednoczonego Królestwa, ustawa o ochronie danych z 2018 r., wytyczne dotyczące certyfikatów bezpieczeństwa narodowego, sierpień 2020 r., s. 5.
[29] Zob. zalecenia EROD 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680, pkt 59–61.

przekazywane. W związku z tym takie dalsze przekazywanie danych powinno być dozwolone wyłącznie w przypadku zapewnienia ciągłości stopnia ochrony przyznanego prawem Unii. EROD uważa, że – jak Komisja Europejska wskazała w swojej ocenie – przepisy zawarte w części 3 rozdział 5 ustawy o ochronie danych z 2018 r., a w szczególności w jej art. 73, co do zasady zapewniają stopień ochrony merytorycznie równoważny stopniowi gwarantowanemu na mocy prawa Unii, jeśli chodzi o przekazywanie danych osobowych przez organ ścigania Zjednoczonego Królestwa do państwa trzeciego.

47. Po pierwsze, w art. 73 ust. 1 lit. b) ustawy o ochronie danych z 2018 r. w szczególności przewidziano, że administrator nie może przekazać danych osobowych do państwa trzeciego ani organizacji międzynarodowej, chyba że „w przypadku gdy dane osobowe zostały pierwotnie przekazane lub w inny sposób udostępnione administratorowi lub innemu właściwemu organowi przez państwo członkowskie inne niż Zjednoczone Królestwo, to państwo członkowskie lub jakikolwiek podmiot z siedzibą w tym państwie członkowskim, który jest właściwym organem do celów dyrektywy (UE) 2016/680, zezwoliły na to przekazanie zgodnie z prawem tego państwa członkowskiego". Takie przepisy wydają się zgodne z zaleceniami w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680, w których przewidziano, że należy również wziąć pod uwagę istnienie mechanizmu, w ramach którego właściwe organy danego państwa członkowskiego są informowane o dalszym przekazywaniu danych oraz wyrażają 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 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, a ponadto pierwotny odbiorca danych powinien być w stanie udowodnić, że właściwy organ państwa członkowskiego udzielił takiej zgody oraz że zapewniono takie zabezpieczenia. „W tym kontekście należy uwzględnić istnienie obowiązku lub zobowiązania do wdrożenia odpowiednich kodeksów postępowania określonych przez organy państw członkowskich przekazujące dane"[30].

48. **EROD wzywa Komisję do oceny tego elementu w świetle wytycznych przedstawionych przez EROD w jej zaleceniach w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680.**

49. Po drugie, jak wyjaśniono w motywie 81 projektu decyzji, sekretarz stanu Zjednoczonego Królestwa jest uprawniony do uznania państwa trzeciego (lub terytorium lub sektora w państwie trzecim), organizacji międzynarodowej lub opisu takiego państwa, terytorium, sektora lub organizacji za zapewniające odpowiedni stopień ochrony danych osobowych, po konsultacji z Urzędem Rzecznika Informacji[31]. Przy ocenianiu, czy stopień ochrony jest odpowiedni, sekretarz stanu Zjednoczonego Królestwa musi uwzględnić te same elementy, które Komisja Europejska ma obowiązek ocenić na podstawie art. 36 ust. 2 lit. a)–c) dyrektywy (UE) 2016/680, interpretowanego łącznie z motywem 67 tej dyrektywy i zachowanym orzecznictwem UE. Oznacza to, że przy ocenie tego, czy stopień ochrony w państwie trzecim jest odpowiedni, właściwym standardem będzie ocenienie, czy dane państwo trzecie zapewnia stopień ochrony „merytorycznie równoważny" stopniowi gwarantowanemu w Zjednoczonym Królestwie. Chociaż EROD odnotowuje zdolność Zjednoczonego Królestwa – zgodnie

[30] Zob. zalecenia EROD 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680, pkt 55 i 56.

[31] Zob. art. 182 ust. 2 ustawy o ochronie danych z 2018 r. Zob. również protokół ustaleń w sprawie roli Urzędu Rzecznika Informacji w odniesieniu do nowych ocen odpowiedniości stopnia ochrony w Zjednoczonym Królestwie, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/

z ustawą o ochronie danych z 2018 r. – do uznawania terytoriów za zapewniającą odpowiedni stopień ochrony w świetle ram ochrony danych Zjednoczonego Królestwa, EROD pragnie podkreślić, że terytoria te mogą do tej pory nie korzystać z decyzji stwierdzającej odpowiedni stopień ochrony wydanej przez Komisję Europejską, uznającej stopień ochrony za „zasadniczo odpowiadający" stopniowi gwarantowanemu w UE. Może to prowadzić do potencjalnych zagrożeń w zakresie ochrony danych osobowych przekazywanych z UE, zwłaszcza jeśli w przyszłości ramy ochrony danych Zjednoczonego Królestwa będą odbiegać od dorobku prawnego UE. Należy zauważyć, że w lipcu 2020 r. precedensowa sprawa TSUE „Schrems II"[32] doprowadziła do unieważnienia decyzji w sprawie Tarczy Prywatności UE-USA, ponieważ zdaniem TSUE nie można było uznać, że ramy prawne Stanów Zjednoczonych zapewniają stopień ochrony merytorycznie równoważny ramom UE. Jednakże wydane już wyroki TSUE, uważane za zachowane orzecznictwo w ramach prawnych Zjednoczonego Królestwa, mogą nie być już wiążące dla Zjednoczonego Królestwa, zwłaszcza z uwagi na fakt, że Zjednoczone Królestwo ma możliwość zmiany zachowanego prawa Unii po zakończeniu dodatkowego okresu przejściowego, a jego Sąd Najwyższy nie jest związany żadnym zachowanym orzecznictwem UE[33].

50. **EROD zachęca zatem Komisję Europejską do ścisłego monitorowania procesu oceny odpowiedniości stopnia ochrony oraz kryteriów stosowanych przez organy brytyjskie w odniesieniu do innych państw trzecich, a w szczególności w odniesieniu do państw trzecich, które nie zostały uznane przez UE za zapewniające odpowiedni stopień ochrony na podstawie dyrektywy (UE) 2016/680.**

51. W przypadku gdy Komisja Europejska stwierdzi, że państwo trzecie uznane przez Zjednoczone Królestwo za zapewniające odpowiedni stopień ochrony nie zapewnia stopnia ochrony merytorycznie równoważnego stopniowi gwarantowanemu w UE na podstawie art. 36 dyrektywy (UE) 2016/680, **EROD wzywa Komisję Europejską do podjęcia wszelkich niezbędnych kroków, takich jak na przykład zmiana decyzji stwierdzającej odpowiedni stopień ochrony w Zjednoczonym Królestwie w celu wprowadzenia konkretnych zabezpieczeń dla danych osobowych pochodzących z UE, lub rozważenie zawieszenia decyzji stwierdzającej odpowiedni stopień ochrony w Zjednoczonym Królestwie, jeżeli dane osobowe przekazywane z UE do Zjednoczonego Królestwa podlegają dalszemu przekazywaniu do danego państwa trzeciego na podstawie przepisów Zjednoczonego Królestwa dotyczących odpowiedniego stopnia ochrony**.

52. **Ponadto w odniesieniu do umów międzynarodowych, które zostały lub zostaną w przyszłości zawarte przez Zjednoczone Królestwo – z możliwym dostępem państwa trzeciego (państw trzecich) będącego (będących) stroną tych umów do danych osobowych pochodzących z UE – EROD zaleca, aby Komisja Europejska zbadała zależności między ramami ochrony danych Zjednoczonego Królestwa a jego zobowiązaniami międzynarodowymi, w szczególności w celu zapewnienia ciągłości stopnia ochrony w przypadku dalszego przekazywania do innych państw trzecich danych osobowych przekazanych z UE do Zjednoczonego Królestwa na podstawie decyzji stwierdzającej odpowiedni stopień ochrony w Zjednoczonym Królestwie; oraz aby stale monitorowała sytuację i w razie potrzeby podejmowała działania w odniesieniu do zawierania umów międzynarodowych między Zjednoczonym Królestwem a państwami trzecimi, które mogą podważyć stopień ochrony danych osobowych przewidziany w UE**. Na przykład chociaż Komisja Europejska odniosła się do faktu, że umowa między Zjednoczonym Królestwem a USA na podstawie ustawy CLOUD[34] może mieć wpływ na

[32] Zob. wyrok TSUE z dnia 16 lipca 2020 r., Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (zwany dalej „Schrems II").

[33] Zob. art. 6 ust. 3–6 Ustawy o wystąpieniu z Unii Europejskiej z 2018 r.

[34] Zob. Umowa między rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej a rządem Stanów Zjednoczonych Ameryki w sprawie dostępu do danych elektronicznych w celu zwalczania poważnych przestępstw, zawarta w dniu 3 października 2019 r. w Waszyngtonie, D.C., w Stanach Zjednoczonych, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019

dalsze przekazywanie danych do Stanów Zjednoczonych przez dostawców usług w Zjednoczonym Królestwie, **EROD podkreśla, że wejście w życie tej umowy może mieć również wpływ na dalsze przekazywanie danych przez organy ścigania w Zjednoczonym Królestwie, w szczególności w odniesieniu do wydawania i przekazywania nakazów zgodnie z art. 5 tej umowy.**

53. EROD uważa również, że zawarcie w przyszłości umów z państwami trzecimi w celu współpracy w zakresie ścigania przestępstw, stanowiących podstawę prawną przekazywania danych osobowych do tych państw, może również w znacznym stopniu wpłynąć na warunki dalszego udostępniania zgromadzonych informacji, ponieważ – jak oceniono – takie umowy mogą mieć wpływ na ramy prawne ochrony danych Zjednoczonego Królestwa.

54. **EROD zaleca zatem, aby Komisja Europejska stale monitorowała, czy zawieranie przyszłych umów między Zjednoczonym Królestwem a państwami trzecimi może mieć wpływ na stosowanie przepisów o ochronie danych Zjednoczonego Królestwa, a także aby zapewniła dalsze ograniczenia lub wyłączenia w odniesieniu do dalszego udostępniania oraz dalszego wykorzystywania i ujawniania za granicą informacji zebranych do celów ścigania przestępstw. EROD uważa, że takie informacje i ocena są niezbędne, aby umożliwić kompleksowy przegląd stopnia ochrony zapewnianej przez ramy legislacyjne i praktyki Zjednoczonego Królestwa w odniesieniu do ujawniania informacji za granicą.**

55. Ponadto EROD przyjmuje do wiadomości, że zgodnie z art. 76 ust. 4 lit. b) ustawy o ochronie danych z 2018 r. (Przekazywanie na podstawie szczególnych okoliczności) organy ścigania w Zjednoczonym Królestwie mogą przekazywać dane osobowe do państwa trzeciego lub organizacji międzynarodowej, jeżeli takie przekazanie „jest konieczne do uzyskania porady prawnej w związku z którymkolwiek z celów w zakresie ścigania przestępstw". **EROD podkreśla, że art. 38 dyrektywy (UE) 2016/680 nie zawiera analogicznego przepisu i w związku z tym zwraca się do Komisji Europejskiej o wyjaśnienie, co należy rozumieć pod pojęciem porady prawnej i jakiego rodzaju dane osobowe są w takich przypadkach wymieniane.**

3.2.4 Dalsze przetwarzanie, w tym dalsze udostępnianie do celów związanych z bezpieczeństwem narodowym

56. W swoich zaleceniach w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680 EROD zwraca uwagę, że 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. Jak oceniła Komisja Europejska w projekcie decyzji, art. 36 ust. 3 ustawy o ochronie danych z 2018 r., ustawa o gospodarce cyfrowej z 2017 r., ustawa o zwalczaniu przestępczości i sądach z 2013 r. oraz ustawa o przeciwdziałaniu poważnej przestępczości z 2017 r. zapewniają jasne ramy prawne umożliwiające dalsze udostępnianie, pod warunkiem, że takie dalsze udostępnianie jest zgodne z przepisami określonymi w ustawie o ochronie danych z 2018 r.

57. EROD zauważa, że w kontekście dalszego przetwarzania do innych celów danych osobowych przekazywanych z UE Komisja Europejska nie oceniła, czy istnieją jakiekolwiek mechanizmy umożliwiające organom ścigania Zjednoczonego Królestwa informowanie właściwych organów państw członkowskich o ewentualnym dalszym przetwarzaniu danych. W zaleceniach w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680 uznano to jednak za element, który należy wziąć pod uwagę[35]. Ponadto istnienie takiego mechanizmu informowania odpowiednich właściwych organów państw członkowskich o dalszym

[35] Zob. zalecenia EROD 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680, pkt 41 i przypis 39.

przetwarzaniu danych do celów ścigania przestępstw również uznaje się za element, który należy uwzględnić, zgodnie z zaleceniami w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680[36].

58. **EROD zachęca zatem Komisję Europejską do uzupełnienia jej analizy o informacje dotyczące istnienia mechanizmów stosowanych przez organy ścigania Zjednoczonego Królestwa do celów powiadamiania odpowiednich właściwych organów państw członkowskich o możliwym dalszym przetwarzaniu danych przekazywanych z UE.**

59. Ponadto w odniesieniu do wymiany danych zgromadzonych przez organ ścigania z agencją wywiadu do celów bezpieczeństwa narodowego podstawą prawną upoważniającą do takiej dalszej wymiany jest ustawa o zwalczaniu terroryzmu z 2008 r. W tym względzie EROD zauważa, że zakres i przepisy art. 19 ustawy o zwalczaniu terroryzmu z 2008 r. nie zostały w pełni uwzględnione w ocenie Komisji Europejskiej i mogą sugerować dalsze wykorzystywanie o szerszym charakterze, w szczególności w odniesieniu do art. 19 ust. 2 ustawy o zwalczaniu terroryzmu z 2008 r., który stanowi, że „[i]informacje uzyskane przez którąkolwiek ze służb wywiadu w związku z wykonywaniem którejkolwiek z jej funkcji mogą być wykorzystane przez tę służbę w związku z wykonywaniem którejkolwiek z jej innych funkcji". W tym kontekście EROD podkreśla, że 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.

3,3 Nadzór i egzekwowanie przepisów

60. EROD zauważa, że nadzór nad organami ścigania jest zapewniany przez połączenie funkcji kilku różnych komisarzy (rzeczników), w tym Urzędu Rzecznika Informacji. W projekcie ustaleń dotyczących zapewnienia odpowiedniego stopnia ochrony wymieniono Komisarza ds. uprawnień dochodzeniowych (Investigatory Powers Commissioner), Komisarza ds. zatrzymywania i wykorzystywania materiału biometrycznego (Commissioner for the Retention and Use of Biometric Material) oraz Komisarza ds. kamer monitorujących (Surveillance Camera Commissioner). W tym kontekście należy zauważyć, że TSUE wielokrotnie podkreślał potrzebę zapewnienia niezależnego nadzoru. Komisarz ds. uprawnień dochodzeniowych ma szczególne znaczenie dla kwestii dostępu do danych osobowych przekazywanych do Zjednoczonego Królestwa. EROD sądzi, że Komisarz ds. uprawnień dochodzeniowo-śledczych jest tak zwanym komisarzem sądowym działającym podobnie jak inni komisarze sądowi, o których należy mówić w kontekście rozdziału dotyczącego bezpieczeństwa narodowego, oraz że ci komisarze sądowi korzystają z niezawisłości sędziów również podczas pełnienia funkcji komisarza. Jeśli chodzi o urząd Komisarza ds. uprawnień dochodzeniowych, Komisja Europejska wyjaśnia w motywie 245 projektu decyzji, że funkcjonuje on jako organ niezależny, ale jest finansowany przez Ministerstwo Spraw Wewnętrznych (Home Office).

61. Ponadto Komisarz ds. uprawnień dochodzeniowych posiada również kompetencje w zakresie nadzoru *ex post* nad środkami nadzoru. Wydaje się jednak, że w ramach tej funkcji rolą Komisarza ds. uprawnień dochodzeniowo-śledczych jest wydawanie zaleceń w przypadkach nieprzestrzegania przepisów oraz przekazanie powiadomienia osobie, której dane dotyczą, jeżeli błąd jest poważny, a poinformowanie jej leży w interesie publicznym.

62. EROD nie stwierdziła w projekcie decyzji dalszych wskazówek pozwalających ocenić niezależność Komisarza ds. uprawnień dochodzeniowych, Komisarza ds. zatrzymywania i wykorzystywania materiału biometrycznego oraz Komisarza ds. kamer monitorujących.

[36] Zob. zalecenia EROD 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy (UE) 2016/680, pkt 40.

63. **Wzywa się Komisję Europejską do przeprowadzenia dalszej oceny niezależności komisarzy sądowych, także w przypadkach, w których komisarz nie pełni (już) funkcji sędziego, a także do przeprowadzenia oceny niezależności Komisarza ds. zatrzymywania i wykorzystywania materiału biometrycznego oraz Komisarza ds. kamer monitorujących.**