Krzysztof Wyderka
Autor jest radcą prawnym, członkiem Okręgowej Izby Radców Prawnych w Warszawie (ORCID: https://orcid.org/0000-0002-8793-1902).

Podejście oparte na ryzyku a transfery danych osobowych do państw trzecich w świetle orzecznictwa Trybunału Sprawiedliwości oraz praktyki organów nadzorczych

Słowa kluczowe: *dane osobowe, międzynarodowe transfery danych, standardowe klauzule umowne, środki uzupełniające, organy ochrony danych, Europejska Rada Ochrony Danych (EROD), Schrems*

Obowiązki związane z przekazywaniem danych osobowych do państw trzecich od lat stanowią poważne wyzwanie dla uczestników obrotu gospodarczego. Wyrok Trybunału Sprawiedliwości w sprawie C-311/18, Schrems II[1], zmienił sytuację podmiotów uczestniczących w międzynarodowych transferach danych osobowych. Istotne znaczenie ma w tym kontekście również późniejsza praktyka organów nadzorczych. Stanowiska prezentowane przez organy ochrony danych państw członkowskich Unii Europejskiej i Europejską Radę Ochrony Danych wzbudzają pewne wątpliwości z punktu widzenia wykładni przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (ogólnego rozporządzenia o ochronie danych)[2] oraz orzecznictwa Trybunału Sprawiedliwości. Celem artykułu jest weryfikacja praktyki organów ochrony danych dotyczącej w szczególności zastosowania podejścia opartego na ryzyku do międzynarodowych transferów danych osobowych.

1. Wprowadzenie

Wyrok Trybunału Sprawiedliwości w sprawie C-311/18, Schrems II, wywołał poważne konsekwencje, istotnie wpływając na sytuację podmiotów zaangażowanych w międzynarodowe transfery danych osobowych. Przede wszystkim, ze względu na unieważnienie decyzji Komisji Europejskiej w sprawie Tarczy Prywatności[3], ograniczył możliwość przekazywania danych osobowych do USA. Pomimo że Trybunał Sprawiedliwości nie unieważnił decyzji Komisji Europejskiej w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podwykonawcom mającym siedzibę w państwach trzecich[4], w praktyce jedynym rozwiązaniem dla wielu podmiotów stało się przetwarzanie danych osobowych wyłącznie na terytorium Unii Europejskiej[5]. Biorąc jednak pod uwagę znaczenie relacji gospodarczych pomiędzy przedsiębiorstwami zlokalizowanymi w państwach członkowskich Unii Europejskiej oraz w państwach trzecich, w tym zwłaszcza w USA, kluczowym problemem stało się wdrożenie rozwiązań

1 Wyrok Trybunału (Wielka Izba) z 16.07.2020 r., C-311/18, Data Protection Commissioner przeciwko Facebook Ireland Ltd, Maximillian Schrems, EU:C:2020:559 – dalej wyrok C-311/18, Schrems II.

2 Dz.Urz. UE L 119, s. 1 – dalej RODO.

3 Decyzja wykonawcza Komisji (UE) 2016/1250 z 12.07.2016 r., przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA (Dz.Urz. UE L 207, s. 1).

4 Decyzja Komisji 2010/87/UE z 5.02.2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w państwach trzecich na mocy dyrektywy Parlamentu Europejskiego i Rady 95/46/WE, zmieniona decyzją wykonawczą Komisji (UE) 2016/2297 z 16.12.2016 r. (Dz.Urz. UE L 39, s. 5).

5 Zob. M. Zalnieriute, G. Churches, *Rejecting the transatlantic outsourcing of data protection in the face of unrestrained surveillance*, „The Cambridge Law Journal" 2021/1, s. 10.

umożliwiających realizowanie transferów danych osobowych i ograniczenie ryzyka naruszenia przepisów o ochronie danych.

Wyzwaniem dla podmiotów uczestniczących w przekazywaniu danych do państw trzecich, będącym również konsekwencją wyroku w sprawie C-311/18, Schrems II, jest obowiązek przeprowadzania oceny adekwatności stopnia ochrony danych osobowych w państwie trzecim[6]. W związku z rezultatem przeprowadzonej oceny konieczne może okazać się wdrożenie dodatkowych środków mających na celu zapewnienie przestrzegania stopnia ochrony wymaganego przez prawo Unii Europejskiej, w tym zwłaszcza zabezpieczeń ograniczających dostęp organów państwa trzeciego do przekazanych danych osobowych[7]. W szczególności z uwagi na uwarunkowania techniczne, a także koszty wdrożenia nowych rozwiązań, całkowite wykluczenie możliwości uzyskania przez organy państwa trzeciego dostępu do danych osobowych przekazanych do tego państwa okazało się w praktyce bardzo trudne. Dlatego też istotnego znaczenia nabrała kwestia dopuszczalności przyjęcia w wypadku transferów danych osobowych podejścia opartego na ryzyku. Zakłada ono stosowanie środków adekwatnych do zidentyfikowanych zagrożeń, z uwzględnieniem analizy konkretnych procesów przetwarzania[8], a w kontekście przekazywania danych do państw trzecich, m.in. oceny prawdopodobieństwa uzyskania dostępu do danych przez organy państwa trzeciego. W celu rozstrzygnięcia tej kwestii celowa jest analiza praktyki organów ochrony danych, przepisów RODO oraz orzecznictwa Trybunału Sprawiedliwości.

2. Stanowiska organów ochrony danych państw Unii Europejskiej

Jedną z pierwszych decyzji organów ochrony danych dotyczących przekazywania danych osobowych do państw trzecich, wydanych po wyroku w sprawie C-311/18, Schrems II, była decyzja portugalskiego organu ochrony danych (*Comissão Nacional de Proteção de Dados* – CNPD) z 27.04.2021 r.[9] Portugalski organ ochrony danych nakazał Narodowemu Instytutowi Statystycznemu (*Instituto Nacional de Estatística Instituto Nacional de Estatística* – INE) zawieszenie przesyłania danych osobowych do USA oraz innych państw trzecich. Podczas prowadzonego w roku 2021 spisu powszechnego INE korzystał z usług amerykańskiego dostawcy Cloudfare. Portugalski organ ochrony danych, powołując się w decyzji[10] na wyrok w sprawie C-311/18, Schrems II, nakazał zawieszenie przekazywania danych do USA z niemal natychmiastowym skutkiem, z uwagi na niezapewnienie adekwatnego stopnia ochrony danych osobowych.

Istotny wpływ na kształtującą się praktykę organów ochrony danych wywarła decyzja austriackiego organu ochrony danych (*Die Datenschutzbehörde* – DSB) z 22.12.2021 r.[11], dotycząca korzystania z narzędzia Google Analytics. Decyzja ta zapoczątkowała serię podobnych rozstrzygnięć organów nadzorczych w innych państwach Unii Europejskiej. Austriacki organ ochrony danych uznał, że w związku z korzystaniem z Google Analytics dochodzi do transferu danych osobowych do USA, a wdrożone przez Google zabezpieczenia są niewystarczające, aby wyeliminować dostęp organów USA do przekazanych danych osobowych[12]. W ocenie austriackiego organu ochrony danych, dopóki istnieje możliwość uzyskania przez organy USA dostępu do danych osobowych, zastosowane środki techniczne nie mogą zostać uznane za skuteczne[13]. W kolejnej decyzji wydanej 22.04.2022 r.[14] DSB wyraźnie wykluczył dopuszczalność zastosowania podejścia opartego na ryzyku w odniesieniu do rozdziału V RODO, a zatem do przepisów regulujących przekazywanie danych osobowych do państw trzecich[15]. Według austriackiego organu ochrony danych do naruszenia art. 44 RODO dochodzi już w momencie, gdy dane osobowe są przekazywane do państwa trzeciego, które nie zapewnia odpowiedniego poziomu ochrony. Uzasadniając swoje stanowisko, austriacki organ ochrony danych wskazał, że w wypadku przepisów RODO, odnośnie do których należy stosować podejście oparte na ryzyku, prawodawca wyraźnie i bez wątpienia to unormował. Przykłady takich przepisów stanowią art. 24 ust. 1 i 2, art. 25 ust. 1, art. 30 ust. 5, art. 32 ust. 1 i 2, art. 34 ust. 1, art. 35 ust. 1 i 3 oraz art. 37 ust. 1 lit. b i c RODO. W ocenie DSB skoro prawodawca w wielu przepisach RODO unormował podejście oparte na ryzyku, ale nie w związku z art. 44 RODO, należy wykluczyć zastosowanie podejścia opartego na ryzyku do art. 44 RODO. Ponadto austriacki organ ochrony danych zakwestionował pogląd, w świetle którego Trybunał Sprawiedliwości w wyroku w sprawie C-311/18, Schrems II, potwierdził dopuszczalność stosowania podejścia opartego na ryzyku do międzynarodowych transferów danych[16].

W dniu 10.02.2022 r. francuski organ ochrony danych (*Commission Nationale de l'Informatique et des Libertés* – CNIL) ogłosił wydanie decyzji nakazującej administratorowi strony internetowej dostosowanie przetwarzania danych użytkowników do stanu zgodnego z art. 44 RODO, w razie potrzeby poprzez zaprzestanie korzystania z narzędzia Google Analytics[17]. Francuski organ ochrony danych uznał, że choć

6 Zob. B. Marcinkowski, *Przekazywanie danych osobowych do państw trzecich. Ramy prawne i praktyka w świetle wyroków Schrems I i Schrems II*, „Monitor Prawniczy" 2020/23 – dodatek: *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*, red. G. Sibiga, s. 74.

7 Wyrok C-311/18, Schrems II, pkt 133.

8 Zob. P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021, s. 284.

9 Zob. komunikat EROD, *Census 2021: Portuguese DPA (CNPD) suspended data flows to the USA,* https://edpb.europa.eu/news/national-news/2021/census-2021-portuguese-dpa-cnpd-suspended-data-flows-usa_en (dostęp: 27.02.2023 r.).

10 CNPD, *DELIBERAÇÃO/2021/533*, https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121875 (dostęp: 27.02.2023 r.).

11 Decyzja DSB w sprawie D155.027, 2021–0.586.257, https://noyb.eu/sites/default/files/2022–01/E-DSB – Google Analytics_DE_bk_0.pdf (dostęp: 27.02.2023 r.).

12 Zob. R. Lawne, *Google Analytics and EU-US transfers*, https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/google-analytics-and-eu-us-transfers (dostęp: 27.02.2023 r.).

13 Zob. C. Fennessy, *The Austrian Google Analytics decision: The race is on*, 7.02.2022 r., https://iapp.org/news/a/the-austrian-google-analytics-decision-the-race-is-on/ (dostęp: 27.02.2023 r.).

14 Decyzja DSB z 22.04.2022 r., https://noyb.eu/sites/default/files/2022–04/Bescheid%20geschw%C3%A4rzt.pdf (dostęp: 27.02.2023 r.).

15 Decyzja DSB z 22.04.2022 r., pkt D.4.

16 Zob. L. Moerel, *What happened to the risk-based approach to data transfers?*, 27.09.2022 r., https://fpf.org/blog/what-happened-to-the-risk-based-approach-to-data-transfers/ (dostęp: 27.02.2023 r.).

17 Komunikat CNIL, *Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply*, https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply (dostęp: 27.02.2023 r.).

Google wdrożył dodatkowe środki regulujące przekazywanie danych osobowych w związku z korzystaniem z narzędzia Google Analytics, nie są one wystarczające, by wykluczyć dostęp służb wywiadowczych USA do tych danych. Istnieje zatem ryzyko dla francuskich użytkowników strony internetowej. W opublikowanym 7.06.2022 r. zestawie pytań i odpowiedzi dotyczących korzystana z narzędzia Google Analytics[18] CNIL zakwestionował natomiast możliwość przyjmowania przez administratorów danych osobowych podejścia opartego na ryzyku, biorąc pod uwagę prawdopodobieństwo dostępu organów państwa trzeciego. W ocenie francuskiego organu nadzorczego konieczne jest w związku z tym wdrożenie dodatkowych środków technicznych, aby dostęp był niemożliwy lub nieskuteczny.

W decyzji wydanej 9.06.2022 r.[19], dotyczącej korzystania z narzędzia Google Analytics, włoski organ ochrony danych (*Garante per la Protezione dei Dati Personali* – GPDP) przedstawił stanowisko zbliżone do zajętego wcześniej przez organy nadzorcze w Austrii i we Francji. Włoski organ ochrony danych uznał, że amerykańskie agencje rządowe i wywiadowcze mogą uzyskać dostęp do danych osobowych użytkowników strony internetowej, które są przekazywane do USA bez wymaganych zabezpieczeń[20]. Środki uzupełniające wdrożone przez Google nie zapewniają natomiast odpowiedniego poziomu ochrony danych osobowych użytkowników w świetle zaleceń EROD 01/2020[21]. Włoski organ ochrony danych potwierdził to stanowisko w kolejnych decyzjach wydanych 7.07.2022 r.[22] oraz 21.07.2022 r.[23]

W dniu 21.09.2022 r. duński organ ochrony danych (*Datatilsynet*) opublikował komunikat[24], w którym stwierdzono, że zgodne z prawem korzystanie z narzędzia Google Analytics wymaga wdrożenia dodatkowych zabezpieczeń. Ponadto *Datatilsynet* zamieścił na swojej stronie internetowej podobny do opublikowanego wcześniej przez CNIL zestaw pytań i odpowiedzi dotyczących korzystania z Google Analytics[25], wskazując, że administrator nie może brać pod uwagę prawdopodobieństwa uzyskania dostępu do określonych danych osobowych przez organy państwa, stosując podejście oparte na ryzyku. W ocenie duńskiego organu ochrony danych w przypadku, gdy taki dostęp jest możliwy – i nie tylko wtedy, gdy dostęp jest prawdopodobny – a przepisy i praktyki prawne regulujące taki dostęp nie pozwalają na zapewnienie osobom, których dane dotyczą, poziomu ochrony zasadniczo równoważnego z ochroną w Unii Europejskiej, niezbędne jest wdrożenie dodatkowych środków technicznych, aby taki dostęp był niemożliwy lub nieskuteczny. Nie jest zatem możliwe przyjęcie podejścia, w którym administrator nie wdraża niezbędnych środków uzupełniających, zakładając, że jest mało prawdopodobne, aby organy państwa trzeciego miały dostęp do przekazanych danych osobowych.

Poza licznymi decyzjami europejskich organów ochrony danych dotyczącymi korzystania z narzędzia Google Analytics, w kontekście międzynarodowych transferów danych osobowych duże zainteresowanie wzbudziło również jedno z prowadzonych w Niemczech postępowań o udzielenie zamówienia publicznego. W decyzji z 13.07.2022 r.[26] Izba Zamówień Publicznych Badenii-Wirtembergii uznała, że sama możliwość przekazania danych osobowych spółce dominującej z siedzibą w państwie trzecim przez jej spółkę zależną z siedzibą na terenie Unii Europejskiej stanowi transfer danych osobowych. Wskutek tej decyzji podmiot ubiegający się o udzielenie zamówienia publicznego został wykluczony z postępowania. W dniu 15.08.2022 r. organ ochrony danych Badenii-Wirtembergii (*Der Landesbeauftragter für den Datenschutz und die Informationsfreiheit* – LfDI) przedstawił krytyczne stanowisko[27] wobec decyzji Izby. Organ ochrony danych Badenii-Wirtembergii zwrócił uwagę na fakt, że Izba Zamówień Publicznych niesłusznie zrównała kwestię ryzyka dostępu spółki dominującej z transferem danych osobowych oraz całkowicie pominęła kwestię stosowania środków technicznych i organizacyjnych, które mogą ostatecznie wyeliminować jakiekolwiek ryzyko. Podmiot wykluczony z postępowania o udzielenie zamówienia zaskarżył decyzję Izby do Wyższego Sądu Okręgowego w Karlsruhe, który postanowieniem z 7.09.2022 r.[28] uchylił zaskarżoną decyzję. Sąd uznał, że zamawiający może polegać na umownych zapewnieniach dostawcy dotyczących przetwarzania danych osobowych. W razie wątpliwości zamawiający powinien uzyskać dodatkowe informacje oraz sprawdzić, czy zrealizowanie zapewnień przez dostawcę jest możliwe[29]. Korzystanie z usług dostawcy, który przetwarza dane osobowe na terenie Unii Europejskiej, ale w ramach grupy kapitałowej, jest zależny od spółki dominującej z siedzibą w USA, nie narusza

18 CNIL, *Questions-réponses sur les mises en demeure de la CNIL concernant l'utilisation de Google Analytics*, https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/questions-reponses-sur-les-mises-en-demeure-de-la-cnil-concernant-lutilisation-de-google-analytics (dostęp: 27.02.2023 r.).

19 Decyzja GPDP z 9.06.2022 r. w sprawie 9782890, https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9782890 (dostęp: 27.02.2023 r.).

20 Komunikat EROD, *Italian SA bans use of Google Analytics: no adequate safeguards for data transfers from Caffeina Media S.r.l. to the U.S.*, https://edpb.europa.eu/news/national-news/2022/italian-sa-bans-use-google-analytics-no-adequate-safeguards-data-transfers_en (dostęp: 27.02.2023 r.).

21 EROD, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, https://edpb.europa.eu/system/files/2021–06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (dostęp: 27.02.2023 r.).

22 Decyzja GPDP z 7.07.2022 r. w sprawie 9806053, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9806053 (dostęp: 27.02.2023 r.).

23 Decyzja GPDP z 21.07.2022 r. w sprawie 9808698, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9808698 (dostęp: 27.02.2023 r.).

24 Komunikat Datatilsynet z 21.09.2022 r., *Use of Google Analytics for web analytics*, https://www.datatilsynet.dk/english/google-analytics/use-of-google-analytics-for-web-analytics (dostęp: 27.02.2023 r.).

25 Google Analytics, spørgsmål og svar, https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/internet-medier-og-apps-/google-analytics (dostęp: 27.02.2023 r.).

26 VK Baden-Württemberg, Beschluss vom 13.07.2022r., 1 VK 23/22, https://openjur.de/u/2447201.html (dostęp: 25.10.2022 r.).

27 Oświadczenie LfDi z 15.08.2022 r., *Stellungnahme zum Beschluss der Vergabekammer BW*, https://www.baden-wuerttemberg.datenschutz.de/stellungnahme-zum-beschluss-der-vergabekammer-bw/ (dostęp: 27.02.2023 r.).

28 Zob. komunikat Oberlandesgericht Karlsruhe, *Kein Ausschluss aus Vergabeverfahren wegen Einbindung der luxemburgischen Tochtergesellschaft eines US-amerikanischen Unternehmens als Hosting-Anbieterin*, https://oberlandesgericht-karlsruhe.justiz-bw.de/pb/,Lde/10537397 (dostęp: 27.02.2023 r.).

29 Zob. H.M. Wulf, *The Higher Regional Court of Karlsruhe clarifies that using a European server and hosting service provider that has a US parent company is not unlawful per se under data protection law*, https://www.heuking.de/en/news-events/newsletter-articles/detail/olg-karlsruhe-stellt-klar-einsatz-eines-europaeischen-server-und-hosting-dienstleisters-mit-us-amerikanischer-konzernmutter-nicht-per-se-datenschutzrechtlich-unzulaessig.html (dostęp: 27.02.2023 r.).

zatem przepisów RODO regulujących transfery danych, o ile nie wskazują na to dodatkowe okoliczności.

3. Podejście oparte na ryzyku w świetle przepisów RODO

Dotychczasowa praktyka organów ochrony danych państw członkowskich Unii Europejskiej świadczy o ich krytycznym stanowisku wobec możliwości stosowania przez administratorów danych podejścia opartego na ryzyku do międzynarodowych transferów danych osobowych. W celu weryfikacji tego stanowiska konieczne jest w szczególności ustalenie zakresu zastosowania podejścia opartego na ryzyku na podstawie analizy przepisów RODO.

Zasada *risk-based approach*, tj. podejścia opartego na ryzyku, stanowi podstawę konstrukcji obowiązków nałożonych w RODO na administratorów oraz podmioty przetwarzające[30]. Liczne przepisy rozporządzenia są przykładami emanacji tej zasady[31]. W kontekście przekazywania danych osobowych do państw trzecich istotne znaczenie ma ustalenie, czy podejście oparte na ryzyku znajduje zastosowanie również do obowiązków administratora określonych w rozdziale V RODO.

W literaturze prezentowany jest pogląd zakładający, że podejście oparte na ryzyku stanowi element zasady rozliczalności wyrażonej w art. 24 RODO i ma zastosowanie do wszystkich obowiązków określonych w RODO, a zatem również do wymogów dotyczących przekazywania danych osobowych do państw trzecich[32]. Umiejscowienie tego przepisu na początku sekcji 1 rozdziału IV, zatytułowanej „Obowiązki ogólne", a także bezpośrednio poprzedzający go nagłówek „Obowiązki administratora", przemawia za ogólnym stosowaniem podejścia opartego na ryzyku, a zatem również do pozostałych obowiązków administratora wynikających z przepisów RODO.

Treść art. 24 RODO, na podstawie którego administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO, „uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze", nie pozostawia wątpliwości co do faktu, że przepis ten odzwierciedla podejście oparte na ryzyku. Analizowany przepis nie ogranicza przy tym zastosowania podejścia opartego na ryzyku do konkretnych kwestii, a zatem rozciąga się ono zarówno na możliwość wykazania, tj. standard dowodowy, a zatem środki służące rozliczalności, jak i samą realizację obowiązków administratora. W doktrynie zwraca się ponadto uwagę na skalowalność wdrażanych środków, oznaczającą, że muszą być one odpowiednie z perspektywy charakteru przetwarzania, a także prawdopodobieństwa i wagi zagrożenia[33]. Zabezpieczenia wdrażane przez administratora „powinny być odpowiednie, nie chodzi tu o zabezpieczenia najlepsze z możliwych (najnowsze, najdroższe, najbardziej zaawansowane technologicznie), a o takie środki techniczne i organizacyjne, które są proporcjonalne"[34]. Określenie odpowiednich w danej sytuacji środków powinno natomiast zostać poprzedzone przeprowadzeniem przez administratora oceny ryzyka[35].

Przyjmując, że podejście oparte na ryzyku wynikające z treści art. 24 RODO znajduje szerokie zastosowanie do obowiązków administratora, celowa jest weryfikacja relacji pomiędzy tym przepisem a przepisami regulującymi przekazywanie danych osobowych do państw trzecich. Sposób, w jaki został sformułowany art. 46 RODO, dotyczący przekazywania danych osobowych z zastrzeżeniem odpowiednich zabezpieczeń, pozwala stwierdzić, że przepis ten określa obowiązki administratora, których spełnienie warunkuje dopuszczalność przekazania danych osobowych do państwa trzeciego. Z treści przepisów rozdziału V RODO nie wynika przy tym wyłączenie zastosowania podejścia opartego na ryzyku w wypadku transferów danych osobowych. Ponadto w literaturze wyrażony jest pogląd, że odpowiednie zabezpieczenia, o których mowa w art. 46 RODO, należy rozumieć jako środki techniczne i organizacyjne[36]. Ich celem jest zminimalizowanie ryzyka oraz zapewnienie zgodności z wymogami ochrony danych oraz prawami osób, których dane dotyczą, właściwymi dla przetwarzania danych osobowych w Unii Europejskiej. Ryzyko związane z transferem danych do państwa trzeciego nie jest jednak eliminowane przez takie odpowiednie zabezpieczenia. Stosowane środki techniczne lub organizacyjne, takie jak pseudonimizacja lub szyfrowanie, nie mogą bowiem w pełni zrekompensować wszystkich braków wynikających z niezapewnienia odpowiedniej ochrony w państwie trzecim.

Zastosowanie podejścia opartego na ryzyku do przekazywania danych osobowych do państw trzecich przy jednoczesnym zwiększeniu rozliczalności i przejrzystości działań administratorów jest wskazywane w piśmiennictwie jako potencjalne rozwiązanie problemów, z którymi po wyroku w sprawie C-311/18, Schrems II, spotykają się podmioty dokonujące transferów danych osobowych[37]. Oznacza to w szczególności konieczność wykazania, w tym udokumentowania, przez administratora zasadności wyboru określonego mechanizmu transferu danych, oceny możliwości i prawdopodobieństwa uzyskania przez organy państwa trzeciego dostępu do przekazanych danych osobowych, a także doboru odpowiednich w konkretnej sytuacji środków technicznych i organizacyjnych. Nie wiązałoby się to jednak z koniecznością całkowitego wykluczenia ryzyka dostępu do danych w każdym wypadku.

4. Stanowisko Trybunału Sprawiedliwości w sprawie Schrems II

W wyroku w sprawie C-311/18, Schrems II, Trybunał Sprawiedliwości nie odniósł się wprost do kwestii zastosowania podejścia opartego na ryzyku do przekazywania danych

30 Zob. D. Lubasz [w:] *Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2020, s. 100.

31 Przykładowo art. 27 ust. 2 lit. a, art. 30 ust. 5, art. 32 ust. 1, art. 35 ust. 1 RODO.

32 Zob. L. Moerel, *What*...

33 Zob. C. Docksey, *Article 24 Responsibility of the controller* [w:] *The EU General Data Protection Regulation (GDPR): A Commentary*, red. C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler, Oxford 2020, s. 564.

34 P. Fajgielski *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022, s. 347.

35 P. Fajgielski, *Ogólne*..., s. 348.

36 Zob. Z. Gulczyńska, *A certain standard of protection for international transfers of personal data under the GDPR,* „International Data Privacy Law" 2021/4, s. 368.

37 Zob. P. Breitbarth, *A Risk-Based Approach to International Data Transfers*, „European Data Protection Law Review" 2021/4, s. 548.

osobowych do państw trzecich. Nie znajduje jednak uzasadnienia pogląd, w świetle którego Trybunał miał wykluczyć taką możliwość[38]. Trybunał zwiększył wymagania dotyczące międzynarodowych transferów danych dokonywanych na podstawie art. 46 RODO, a zatem – przy zastosowaniu odpowiednich zabezpieczeń. Trybunał wskazał bowiem, że art. 46 ust. 1 i art. 46 ust. 2 lit. c RODO należy interpretować w ten sposób, iż wymagane przez te przepisy odpowiednie zabezpieczenia powinny zapewniać, by prawa osób, których dane osobowe są przekazywane do państwa trzeciego na podstawie klauzul ochrony danych, były chronione „w stopniu merytorycznie równoważnym temu gwarantowanemu w Unii"[39].

W praktyce poważne wątpliwości wzbudza zwłaszcza realizacja wymogu podjęcia przez administratora danych dodatkowych środków mających na celu zapewnienie przestrzegania stopnia ochrony wymaganego przez prawo Unii[40]. W konkretnej sytuacji nie jest bowiem jasne, jakie dokładnie środki są wystarczające, aby dostosować transfer danych do państwa trzeciego, wobec którego nie została wydana decyzja o adekwatności, do wymogów prawa Unii. Trybunał nie wskazał również, jaka forma lub treść jest konieczna, aby takie hipotetyczne środki uzupełniające były skuteczne[41].

Trybunał Sprawiedliwości stwierdził jednak, że administrator udziela „w razie potrzeby zabezpieczeń dodatkowych" w stosunku do tych zapewnianych w standardowych klauzulach ochrony danych[42], a ponadto w razie braku możliwości podjęcia „dodatkowych środków odpowiednich dla zagwarantowania takiej ochrony"[43] jest zobowiązany do zawieszenia lub zakończenia przekazywania danych osobowych do danego państwa trzeciego. Posłużenie się sformułowaniami „w razie potrzeby" oraz „odpowiednich" w ocenie niektórych przedstawicieli doktryny stanowi odwołanie do podejścia opartego na ryzyku[44].

W piśmiennictwie[45] wskazuje się ponadto, że Trybunał nie wymaga, aby dodatkowe zabezpieczenia dawały stuprocentową gwarancję, iż dostęp do danych przez organy państwa trzeciego nigdy nie będzie miał miejsca, ale raczej, aby stanowiły „skuteczne mechanizmy umożliwiające w praktyce zapewnienie przestrzegania wymaganego przez prawo Unii stopnia ochrony"[46]. W rezultacie wdrażane przez administratora danych środki techniczne i organizacyjne służące ograniczeniu dostępu do danych przekazanych do państwa trzeciego powinny być dobierane z uwzględnieniem podejścia opartego na ryzyku[47] i oceniane według kryterium proporcjonalności.

38 Zob. L. Moerel, *What*....
39 Wyrok C-311/18, Schrems II, pkt 105.
40 Wyrok C-311/18, Schrems II, pkt 133.
41 Zob. R.A. Costello, *Schrems II: Everything Is Illuminated?,* https://www.europeanpapers.eu/en/europeanforum/schrems-II-everything-is-illuminated#_ftn35 (dostęp: 27.02.2023 r.).
42 Wyrok C-311/18, Schrems II, pkt 134.
43 Wyrok C-311/18, Schrems II, pkt 135.
44 M. Ćwiakowski, M. Gawroński, *Usługi chmurowe w sektorze finansowym w kontekście transferów danych osobowych – aktualny krajobraz regulacyjny*, „Monitor Prawniczy" 2022/15, s. 50.
45 C. Kuner, *Schrems II Re-Examined*, 25.08.2020 r., https://verfassungsblog.de/schrems-ii-re-examined/ (dostęp: 27.02.2023 r.).
46 Wyrok C-311/18, Schrems II, pkt 137.
47 Zob. Centre's for Information Policy Leadership, *A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision*, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_gdpr_transfers_post_schrems_ii_24_september_2020_2_.pdf (dostęp: 27.02.2023 r.).

5. Zalecenia Europejskiej Rady Ochrony Danych 01/2020

W dniu 18.06.2021 r. EROD przyjęła po konsultacjach publicznych zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych[48]. Pomimo iż zgodnie ze stanowiskiem doktryny zalecenia EROD „nie mają charakteru norm prawnie wiążących, co oznacza, że podmioty które nie zastosują się do tego rodzaju wskazówek, nie powinny ponosić w związku z tym negatywnych konsekwencji, jeżeli są w stanie spełnić obowiązki wynikające z rozporządzenia w inny sposób"[49], wywierają one istotny wpływ na praktykę organów ochrony danych państw członkowskich Unii Europejskiej. Częstym zjawiskiem jest uzasadnianie przez krajowe organy nadzorcze swoich stanowisk poprzez odwołanie do zaleceń lub wytycznych EROD. Dlatego celowa jest analiza zaleceń w kontekście dopuszczalności zastosowania podejścia opartego na ryzyku do transferów danych osobowych do państw trzecich.

W zaleceniach 01/2020 EROD nie odwołuje się wprost do podejścia opartego na ryzyku. Kilkukrotnie odnosi się do zasady rozliczalności, wskazując przy tym art. 5 ust. 2 RODO, ale właściwie pomija art. 24 RODO. Brak wyraźnego uwzględnienia podejścia opartego na ryzyku jest dostrzegalny zwłaszcza w części dotyczącej oceny, czy wykorzystywane narzędzie transferu z art. 46 RODO jest skuteczne w świetle wszystkich okoliczności przekazywania[50], a także w części poświęconej przyjęciu środków uzupełniających[51]. W konsekwencji zalecenia tworzą stosunkowo sztywne ramy oceny, nie uwzględniając wielu istotnych okoliczności, takich jak: rodzaj przekazywanych danych osobowych, rzeczywista możliwość uzyskania do nich dostępu przez organy państwa trzeciego czy stosowane środki techniczne ograniczające w znacznym stopniu prawdopodobieństwo uzyskania dostępu do danych[52].

Podczas konsultacji zaleceń wiele zainteresowanych stron podnosiło, że EROD niesłusznie pominęła w pierwotnej wersji zaleceń podejście oparte na ryzyku[53]. Ostatecznie w tekście zaleceń przyjętych po konsultacjach można doszukać się co najmniej kilku elementów pozwalających administratorom uwzględnić poziom ryzyka związanego z transferem danych osobowych do państwa trzeciego[54]. Przykładowo EROD wskazuje, że ocena powinna obejmować nie tylko przepisy prawa, ale również praktyki organów publicznych państwa trzeciego[55]. Ponadto w świetle zaleceń 01/2020, jeżeli przeprowadzona ocena ujawni, że ustawodawstwo państwa trzeciego jest „problematyczne", dopuszczalne jest podjęcie decyzji o przekazaniu danych bez konieczności wdrażania środków uzupełniających, jeżeli

48 EROD, *Recommendations 01/2020*...
49 A. Grzelak, *Charakter prawny zaleceń i wytycznych Europejskiej Rady Ochrony Danych*, „Monitor Prawniczy" 2021/23 – dodatek: *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych. Aktualne problemy ochrony danych osobowych 2021*, red. G. Sibiga, s. 10.
50 EROD, *Recommendations 01/2020*..., krok 3, pkt 28–49.
51 EROD, *Recommendations 01/2020*..., krok 4, pkt 50–58.
52 M. Ćwiakowski, M. Gawroński, *Usługi*..., s. 50.
53 Zob. L. Moerel, *What*....
54 Zob. D. Karwala, *Znaczenie soft law dla transferów danych osobowych do państw trzecich na przykładzie zaleceń EROD 01/2020*, „Monitor Prawniczy" 2021/23 – dodatek: *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych. Aktualne problemy ochrony danych osobowych 2021*, red. G. Sibiga, s. 35.
55 EROD, *Recommendations 01/2020*..., pkt 43.

administrator uważa, że nie ma powodu, by sądzić, że w praktyce do przekazanych danych lub podmiotu odbierającego dane będą stosowane problematyczne przepisy[56]. Nie bez znaczenia jest również fakt, że w wersji po konsultacjach, w odróżnieniu od pierwotnej wersji zaleceń nie znalazło się stwierdzenie, zgodnie z którym nie powinno się polegać na czynnikach subiektywnych, takich jak prawdopodobieństwo, że organy publiczne uzyskają dostęp do danych w sposób niezgodny ze standardami Unii Europejskiej[57].

Analiza treści przyjętych przez EROD zaleceń 01/2020 skłania zatem do uznania, że pomimo braku bezpośredniego odwołania do podejścia opartego na ryzyku nie wykluczają one definitywnie zastosowania go w stosunku do transferów danych osobowych do państw trzecich.

6. Wnioski

Analiza dotychczasowej praktyki organów ochrony danych państw członkowskich Unii Europejskiej pozwala stwierdzić, że obecnie dominuje stanowisko wykluczające możliwość stosowania przez administratorów danych podejścia opartego na ryzyku do przekazywania danych osobowych do państw trzecich. Organy nadzorcze niejednokrotnie interpretują wyrok Trybunału Sprawiedliwości w sprawie C-311/18, Schrems II, przyjmując podejście zakładające wymóg bezwzględnego wyeliminowania ryzyka dostępu osób trzecich do przekazanych danych osobowych.

Prezentowana przez organy ochrony danych negatywna ocena możliwości zastosowania podejścia opartego na ryzyku wobec międzynarodowych transferów danych nie jest przekonująca, jeżeli weźmie się pod uwagę zarówno przepisy RODO, wyrok Trybunału Sprawiedliwości w sprawie C-311/18, Schrems II, jak i przyjęte przez EROD zalecenia 01/2020. Kolejne decyzje organów nadzorczych dotyczące zwłaszcza transferów danych do USA wskazują jednak na utrwalanie się pewnej linii orzeczniczej.

Mając na uwadze podpisanie przez prezydenta USA rozporządzenia wykonawczego 14086[58], a następnie opublikowanie przez Komisję Europejską projektu decyzji w sprawie odpowiedniego poziomu ochrony danych osobowych na mocy ram ochrony prywatności danych UE-USA[59], w niedalekiej perspektywie można oczekiwać wydania nowej decyzji o adekwatności dotyczącej USA. Ułatwiłoby to wielu podmiotom dokonywanie transferów danych osobowych. Trudno jednak przewidzieć, na ile trwałe okażą się oczekiwane, nowe ramy prawne przekazywania danych osobowych pomiędzy państwami Unii Europejskiej a USA. Ponadto aktualne pozostanie nadal wyzwanie związane z przekazywaniem danych osobowych do innych państw, w stosunku do których nie została wydana decyzja stwierdzająca adekwatny poziom ochrony danych. W konsekwencji istotną rolę będą prawdopodobnie odgrywać rozwiązania techniczne i organizacyjne umożliwiające skuteczne wykluczenie dostępu organów państw trzecich do przekazanych danych osobowych.

Przedstawione w artykule opinie stanowią wyraz osobistych poglądów autora i nie powinny być utożsamiane ze stanowiskiem żadnej organizacji lub instytucji, z którą autor był lub jest powiązany.

56 EROD, *Recommendations 01/2020…*, pkt 43.3.

57 Zob. EROD, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020*, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf, pkt 42 (dostęp: 27.02.2023 r.).

58 Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ (dostęp: 27.02.2023 r.).

59 Draft adequacy decision on the EU-U.S. Data Privacy Framework, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631 (dostęp: 27.02.2023 r.).

Abstract

Krzysztof Wyderka
The author is an attorney at law,
a member of the Warsaw Bar Association, Poland
(ORCID: https://orcid.org/0000-0002-8793-1902).

Risk-Based Approach and Transfers of Personal Data to Third Countries in the Light of Case Law of the Court of Justice and the Practice of Supervisory Authorities

Keywords: *personal data, international data transfers, standard contractual provisions, supplementary measures, data protection authorities, EDPB,* Schrems

Obligations connected with transferring personal data to third countries have been a major challenge for economic actors for years. The judgment of the Court of Justice in the Schrems II *case has changed the situation for entities involved in international transfers of personal data. The subsequent practice of supervisory authorities is also relevant in this context. The views presented by the data protection authorities of EU Member States and by the European Data Protection Board give rise certain doubts from the point of view of interpreting the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and case law of the Court of Justice. This article aims to review the practice of data protection authorities regarding in particular the application of a risk-based approach to international transfers of personal data.*

Bibliografia/References

Breitbarth P., *A Risk-Based Approach to International Data Transfers*, „European Data Protection Law Review" 2021/4.
Costello R.A., *Schrems II: Everything Is Illuminated?*, https://www.europeanpapers.eu/en/europeanforum/schrems-II-everything-is-illuminated#_ftn35 (dostęp: 27.02.2023 r.).
Ćwiakowski M., Gawroński M., *Usługi chmurowe w sektorze finansowym w kontekście transferów danych osobowych – aktualny krajobraz regulacyjny*, „Monitor Prawniczy" 2022/15.
Docksey C., *Article 24 Responsibility of the controller* [w:] *The EU General Data Protection Regulation (GDPR): A Commentary*, red. C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler, Oxford 2020.
Fajgielski P. *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022.
Fennessy C., *The Austrian Google Analytics decision: The race is on*, 7.02.2022 r., https://iapp.org/news/a/the-austrian-google-analytics-decision-the-race-is-on/ (dostęp: 27.02.2023 r.).

Grzelak A., *Charakter prawny zaleceń i wytycznych Europejskiej Rady Ochrony Danych*, „Monitor Prawniczy" 2021/23 – dodatek: *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych. Aktualne problemy ochrony danych osobowych 2021*, red. G. Sibiga.
Gulczyńska Z., *A certain standard of protection for international transfers of personal data under the GDPR*, „International Data Privacy Law" 2021/4.
Karwala D., *Znaczenie soft law dla transferów danych osobowych do państw trzecich na przykładzie zaleceń EROD 01/2020*, „Monitor Prawniczy" 2021/23 – dodatek: *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych. Aktualne problemy ochrony danych osobowych 2021*, red. G. Sibiga.
Kuner C., *Schrems II Re-Examined*, 25.08.2020 r., https://verfassungsblog.de/schrems-ii-re-examined/ (dostęp: 27.02.2023 r.).
Lawne R., *Google Analytics and EU-US transfers*, https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/google-analytics--and-eu-us-transfers (dostęp: 27.02.2023 r.).
Litwiński P. [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021.
Lubasz D. [w:] *Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2020.
Marcinkowski B., *Przekazywanie danych osobowych do państw trzecich. Ramy prawne i praktyka w świetle wyroków Schrems I i Schrems II*, „Monitor Prawniczy" 2020/23 – dodatek: *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*, red. G. Sibiga.
Moerel L., *What happened to the risk-based approach to data transfers?*, 27.09.2022 r., https://fpf.org/blog/what-happened-to-the-risk-based-approach-to-data-transfers/ (dostęp: 27.02.2023 r.).
Wulf H.M., *The Higher Regional Court of Karlsruhe clarifies that using a European server and hosting service provider that has a US parent company is not unlawful per se under data protection law*, https://www.heuking.de/en/news-events/newsletter-articles/detail/olg-karlsruhe-stellt-klar-einsatz-eines-europaeischen-server-und-hosting-dienstleisters-mit-us-amerikanischer-konzernmutter-nicht-per-se-datenschutzrechtlich-unzulaessig.html (dostęp: 27.02.2023 r.).
Zalnieriute M., Churches G., *Rejecting the transatlantic outsourcing of data protection in the face of unrestrained surveillance*, „The Cambridge Law Journal" 2021/1.