Gdańskie Studia Prawnicze

Rok XXV — Nr 4(52)/2021

Reforma ochrony danych osobowych w Unii Europejskiej – praktyka i orzecznictwo

Redakcja naukowa
Wojciech R. Wiewiórowski

Wydawnictwo Uniwersytetu Gdańskiego
Gdańsk 2021

Czasopismo sfinansowane ze środków własnych
Wydziału Prawa i Administracji Uniwersytetu Gdańskiego
oraz Wolters Kluwer Polska Sp. z o.o.

Adres redakcji:
ul. Bażyńskiego 6, 80-952 Gdańsk

ISSN 1734-5669

Wydawnictwo Uniwersytetu Gdańskiego
ul. Armii Krajowej 119/121, 81-824 Sopot
tel. (+48) 58 523 11 37
e-mail: wydawnictwo@ug.edu.pl
wydawnictwo.ug.edu.pl
Księgarnia internetowa: wydawnictwo.ug.edu.pl/sklep/

Druk i oprawa
Zakład Poligrafii
Uniwersytetu Gdańskiego
ul. Armii Krajowej 119/121
81-824 Sopot
tel. (+48) 58 523 14 49

Reforma ochrony danych osobowych w Unii Europejskiej – praktyka i orzecznictwo

Spis treści

ARTYKUŁY I KOMENTARZE

GLOSY

VARIA

Personal Data Protection Reform in the European Union – Practice and Jurisprudence

Table of contents

ARTICLES

COMMENTARIES

VARIA

Artykuły i komentarze

Paweł Fajgielski
Katolicki Uniwersytet Lubelski
pawel.fajgielski@kul.pl
ORCID: 0000-0002-4293-1917

https://doi.org/10.26881/gsp.2021.4.01

Rzetelność jako ogólna zasada przetwarzania danych osobowych

Wprowadzenie

Jedną z ogólnych zasad przetwarzania danych osobowych jest zasada rzetelności, legalności i przejrzystości. Można uznać, że omawiana zasada, łącząca w sobie trzy elementy, stanowi jeden z fundamentów, na którym opiera się prawna regulacja przetwarzania i ochrony danych osobowych. Wymóg rzetelności nie został przez prawodawcę zdefiniowany, jego treść nie jest w aktach normatywnych wyjaśniona, a tłumaczenie sformułowania określającego ten wymóg na różne języki ukazuje, że może być on rozmaicie rozumiany i interpretowany, co może prowadzić do rozbieżności w praktyce stosowania przepisów o ochronie danych. Pomimo istotnego znaczenia wśród norm prawnych odnoszących się do przetwarzania danych osobowych, wymóg rzetelności przetwarzania nie był dotąd poddawany szczegółowej analizie w literaturze przedmiotu.

W niniejszym artykule przedstawiona zostanie rzetelność jako jedna z zasad przetwarzania danych uregulowana w przepisach obowiązujących przed unijną reformą ochrony danych osobowych oraz w przepisach obowiązującego obecnie ogólnego rozporządzenia o ochronie danych[1]. Wskazane zostaną różnorodne poglądy prezentowane w literaturze odnoszące się do tej zasady, a także rozmaite możliwości odczytywania jej treści i znaczenia. W kolejnej części opracowania ukazane zostaną ogólne wnioski płynące z przeprowadzonych analiz.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1 ze zm.; dalej: rozporządzenie 2016/679).

Terminologia

Będąca przedmiotem rozważań w niniejszym artykule zasada (ściśle rzecz ujmując, jeden z wymogów składających się na pierwszą ogólną zasadę przetwarzania danych) jest określana w różnych językach różnymi nazwami, co może pociągać za sobą wątpliwości interpretacyjne. W angielskim tekście rozporządzenia 2016/679 na oznaczenie omawianej zasady używane jest sformułowanie *fairly processing (fairness)*, które zostało przetłumaczone na język polski jako „przetwarzane rzetelnie (rzetelność)". Jednak w literaturze przedmiotu trafnie zwracano uwagę, że pomimo tego, iż wywodzącą się z anglosaskiego systemu prawnego zasadę działania *fair* tradycyjnie tłumaczy się w polskich dokumentach jako zasadę rzetelności, to jednak w kontekście ochrony danych osobowych określeniem lepiej oddającym istotę tej zasady jest słowo „uczciwość"[2]. Jeszcze inaczej nazwa omawianej zasady została ujęta w niemieckim tłumaczeniu przepisów europejskich, gdzie posłużono się sformułowaniem *nach Treu und Glauben*, co należy przełożyć jako „w dobrej wierze". Odmiennie także w wersji francuskiej, omawianą zasadę określono jako *loyale (loyauté)*, co tłumaczyć można jako „lojalnie, uczciwie". Jeszcze inaczej omawianą zasadę ujęto w języku włoskim, gdzie posłużono się określeniem *correttezza*, co tłumaczyć można jako „poprawność". W innych wersjach językowych również dostrzec można różnorodność w tłumaczeniu nazwy omawianej zasady[3], choć rozumienie tych nazw jest z reguły bliskie jednemu ze znaczeń przedstawionych powyżej. Porównanie różnych wersji językowych unijnych aktów normatywnych z zakresu ochrony danych osobowych ukazuje brak jednolitości terminologicznej, co może przekładać się na różny sposób rozumienia omawianej zasady i prowadzić do rozbieżności przy jej stosowaniu w różnych państwach członkowskich UE. Jednak z porównania nazw wykorzystywanych na oznaczenie analizowanej

[2] M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010, s. 78.

[3] W języku bułgarskim określenie to jest tożsame z wersją niemiecką i wskazuje na dobrą wiarę (добросъвестно); w wersji czeskiej posłużono się określeniem *korektnost*, co rozumieć można jako „prawidłowość, rzetelność"; w wersji duńskiej użyto sformułowania *rimelighed*, które można tłumaczyć jako „rozsądnie, uczciwie"; w wersji greckiej użyto sformułowania *αντικειμενικότητα*, które tłumaczyć można jako „obiektywność, rzetelność"; w wersji hiszpańskiej i portugalskiej posłużono się określeniami *lealtad, lealdade*, które tłumaczyć można jako „lojalność", co jest zbieżne z wersją francuską; w języku estońskim wykorzystano określenie *õiglus*, które oznacza „uczciwość, sprawiedliwość"; w języku irlandzkim użyto określenia *cothroime*, które przełożyć można jako „uczciwie, słusznie"; w wersji chorwackiej i słoweńskiej użyto sformułowań *pošteno (poštenost, pravičnost)*, co oznacza „uczciwie"; w wersji łotewskiej użyto określenia *godprātība*, które rozumieć można jako „w dobrej wierze, uczciwie"; w języku litewskim wykorzystano sformułowanie *sąžiningumo*, które można przetłumaczyć jako „uczciwie"; w języku węgierskim wykorzystano określenie *tisztességes eljárás*, które może być rozumiane jako „w uczciwym postępowaniu"; w języku maltańskim występuje zwrot *ġustizzja*, który można tłumaczyć jako „słuszność, sprawiedliwość"; w języku niderlandzkim posłużono się określeniem *behoorlijkheid*, które można rozumieć jako „uczciwość, przyzwoitość"; w języku rumuńskim wykorzystano określenie *echitate*, które można tłumaczyć jako „uczciwie"; po słowacku omawianą zasadę określono jako *spravodlivosť*, czyli „uczciwie, sprawiedliwie"; w wersji fińskiej użyto sformułowania *asianmukaisesti (kohtuullisuus)*, które tłumaczyć można jako „należycie, z umiarem"; natomiast w języku szwedzkim posłużono się określeniem *korrekthet*, które można tłumaczyć jako „poprawność".

zasady można wyciągnąć wniosek, że zasada ta jest rozległa i może być interpretowana szeroko, z uwzględnieniem różnych jej wymiarów.

Zasada rzetelności przed unijną reformą ochrony danych

Wymóg rzetelności (uczciwości) przetwarzania danych niewątpliwie stanowi jeden z europejskich standardów prawnych ochrony danych. Zasada rzetelności i legalności przetwarzania została zawarta zarówno w konwencji nr 108 Rady Europy[4] (w art. 5), jak również w unijnej dyrektywie 95/46/WE[5] (w art. 6). O jej dużym znaczeniu świadczy nie tylko fakt, że została wskazana jako pierwsza pośród zasad ogólnych, ale również okoliczność, iż została ona ujęta w art. 8 Karty praw podstawowych UE[6], przy ogólnym określeniu prawa podmiotowego do ochrony danych osobowych.

W literaturze przedmiotu zwrócono uwagę na to, że omawianą zasadę powszechnie uznaje się za podstawową klauzulę wyznaczającą standardy ochrony danych osobowych, jednak jej ogólny charakter skutkuje tym, że raczej trudno liczyć na wiążącą prawnie definicję tego pojęcia, a jej analiza stała się przedmiotem incydentalnych rozstrzygnięć praktyki i generalizacji doktryny. Najogólniej treść omawianej zasady można ująć w stwierdzeniu, że administrator przy przetwarzaniu danych osobowych ma obowiązek dbać o interesy osoby, której dane dotyczą, i nie powinien wykorzystywać danych przeciwko podmiotowi danych[7].

Na gruncie art. 6 dyrektywy 95/46/WE uznawano, że wymóg rzetelności połączony z wymogiem legalności przetwarzania stanowią podstawową, główną zasadę (*primary principle)*, ponieważ tworzy ona i wzmacnia pozostałe ogólne zasady prawa ochrony danych. Zwracano jednocześnie uwagę na to, że nie jest możliwe wyczerpujące omówienie tej zasady w sposób abstrakcyjny, a ponadto jej rozumienie może być zmienne w czasie. Wskazywano, że na dużym poziomie ogólności można uznać, iż pojęcie *fair processing* oznacza, że w dążeniu do realizacji celów przetwarzania danych administratorzy muszą brać pod uwagę interesy i uzasadnione oczekiwania osób, których dane dotyczą. Oznacza to, że gromadzenie i późniejsze przetwarzanie danych osobowych powinno być dokonywane w sposób, który w danych okolicznościach nie narusza w nieuzasadniony sposób prywatności osób, których dane dotyczą, ani nie ingeruje

[4] Konwencja nr 108 Rady Europy sporządzona w Strasburgu dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz. U. z 2003 r., poz. 25), uzupełniona protokołem dodatkowym, sporządzonym w Strasburgu dnia 8 listopada 2001 r. (Dz. U. z 2006 r., poz. 15).

[5] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. UE L 281, s. 31; dalej: dyrektywa 95/46/WE).

[6] Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 303 z 2007 r., s. 1).

[7] M. Jagielski, *Prawo do ochrony…*, s. 78–79.

w nieuzasadniony sposób w ich autonomię i integralność. Omawianą zasadę łączono z wymogami równowagi i proporcjonalności[8].

W literaturze przedmiotu, bazując na motywie 38 preambuły do dyrektywy 95/46/WE, wskazywano, że w zakresie szeroko rozumianej rzetelności (uczciwości) mieści się także m.in. wymóg przetwarzania danych w sposób jawny dla osoby, której dane dotyczą, tak aby osoba miała świadomość procesów przetwarzania jej danych, natomiast za naruszenie tej zasady (z pewnymi wyjątkami) uznawano przetwarzanie danych w sposób niejawny, gromadzenie danych z wykorzystaniem ukrytych urządzeń, przy pomocy których potajemnie i bez wiedzy podmiotu danych jego dane byłyby zbierane[9]. Niekiedy nawet uznawano, że wymóg przejrzystości przetwarzania danych względem osoby, której dane dotyczą, jest kluczową kwestią w zasadzie rzetelności – wskazywano bowiem także na potrzebę budowania zaufania podmiotów danych do administratorów[10].

Zasada rzetelności przetwarzania, określona w dyrektywie 95/46/WE, została zaimplementowana do prawa wewnętrznego państw członkowskich UE. W wielu krajowych regulacjach ustawowych zasadę tę wskazano wprost obok innych ogólnych zasad przetwarzania danych. Jednym z przykładów może być brytyjska ustawa *Data Protection Act* z roku 1998, w której zasada rzetelności (uczciwości) została ujęta jako pierwsza z zasad ogólnych (łącznie z zasadą zgodności z prawem), a prawodawca, określając jak powinna być ona interpretowana, podkreślił, że przy ocenie zgodności z tą zasadą należy zwrócić uwagę na sposób gromadzenia danych, w szczególności na to, czy osoba, której dane dotyczą, nie została oszukana lub wprowadzona w błąd co do celów, w jakich dane mają być przetwarzane, oraz czy osoba ta została odpowiednio poinformowana[11]. Jako przykład naruszenia omawianej zasady, w literaturze przedmiotu wskazano m.in. działania firmy reklamowej polegające na poinformowaniu klientów o wykorzystywaniu ich danych do innych celów (sprzedaż listy adresów klientów) dopiero po uzyskaniu danych, co zostało uznane za nieuczciwe, ponieważ osoby, od których dane były zbierane, mogły zostać wprowadzone w błąd[12].

W piśmiennictwie niemieckim, w okresie obowiązywania federalnej ustawy o ochronie danych z roku 1990[13] wskazywano, że nieuczciwość przetwarzania może polegać m.in. na ukrywaniu przed podmiotem danych ważnych okoliczności przetwarzania albo na świadomym wprowadzaniu w błąd, podsłuchiwaniu rozmów, czy też kontroli pracowników z wykorzystaniem ukrytych kamer[14].

---

8 L.A. Bygrave, *Data protection law. Approaching Its Rationale, Logic and Limits*, Hague – London – New York 2002, s. 58.

9 Por. E. Ehmann. M. Helfrich, *EG Datenschutzrichtlinie. Kurzkommentar*, Köln 1999, s. 100–101.

10 *Handbook on European data protection law*, Luxembourg 2014, s. 73–75.

11 *Data Protection Act 1998, Schedule 1, The data protection principles, Part II, Interpretation of the principles in Part I, The first principle*.

12 P. Carey, *Data Protection. A Practical Guide to UK and EU Law*, Oxford 2004, s. 66.

13 Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954, ze zm.).

14 M.T. Tinnefeld, E. Ehmann, *Einführung in das Datenschutzrecht*, München 1998, s. 224.

Przepisy hiszpańskie obowiązujące przed unijną reformą ochrony danych wyraźnie zabraniały zbierania danych osobowych w sposób oszukańczy, nieuczciwy (*medios fraudulentos, desleales*), jednak w praktyce zakaz ten był rozciągany także na inne poza gromadzeniem formy przetwarzania danych, zgodnie z dyrektywą 95/46/WE[15].

Z odmiennym sposobem prawnej regulacji omawianej zasady mieliśmy do czynienia na gruncie polskiej ustawy o ochronie danych osobowych z roku 1997[16]. Zasada rzetelności (uczciwości) nie została *explicite* wyrażona wśród innych ogólnych zasad przetwarzania danych, jednak w przepisie zawierającym wskazanie zasad ogólnych jako obowiązków administratora (art. 26 u.o.d.o.1997) zawarty został ogólny obowiązek dołożenia szczególnej staranności przy przetwarzaniu danych, w celu ochrony interesów osób, których dane dotyczą. Takie sformułowanie mogło być interpretowane jako swoista implementacja wymogu rzetelności przetwarzania danych[17]. Ponadto, na gruncie u.o.d.o.1997 prezentowany był pogląd, zgodnie z którym omawiany wymóg (rzetelności, uczciwości) można wywodzić także z obowiązku przetwarzania danych osobowych, zgodnie z zasadami współżycia społecznego, które stanowią część systemu prawnego[18].

Zasada rzetelności w przepisach rozporządzenia 2016/679

W art. 5 ust. 1 rozporządzenia 2016/679 określono, że „dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą («zgodność z prawem, rzetelność i przejrzystość»)". Oznacza to, że w unijnym ogólnym rozporządzeniu o ochronie danych pierwsza z ogólnych zasad przetwarzania danych została unormowana bardziej szczegółowo niż w przepisach dyrektywy 95/46/WE; zmiana polega na wyodrębnieniu przejrzystości jako wymogu wyraźnie wskazanego w przepisie, który to wymóg był wcześniej uznawany w drodze wykładni zasady rzetelności (uczciwości) przetwarzania danych.

Oprócz podstawowej regulacji prawnej omawianej zasady, zawartej w art. 5 ust. 1 lit a rozporządzenia 2016/679, odniesienia do zasady rzetelności przetwarzania zawarte zostały również w preambule (motywy: 39, 45, 60, 71) oraz w kilku przepisach ogólnego rozporządzenia: w art. 6 ust. 2 (w kontekście podstaw dopuszczalności

---

15 D. Korff, *EC study on implementation of data protection directive. Comparative study of national law*, Cambridge 2002, s. 61.

16 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2016 r., poz. 922 ze zm.; dalej: u.o.d.o.1997).

17 P. Fajgielski, *Zasady ogólne przetwarzania i ochrony danych osobowych* [w:] *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, red. G. Goździewicz, M. Szabłowska, Toruń 2008, s. 20. Podobnie: P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016, s. 306. Szerzej na temat ogólnych zasad przetwarzania danych na gruncie u.o.d.o.1997, por. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2015, s. 468 i n.

18 A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2007, s. 156.

przetwarzania danych); w art. 13 ust. 2 i w art. 14 ust. 2 (w zakresie obowiązków informacyjnych) oraz w art. 40 ust. 2 (w przepisie dotyczącym kodeksów postępowania).

W komentarzach do art. 5 ogólnego rozporządzenia uznaje się, że wymóg przetwarzania danych *fair* oznacza, że dane nie mogą być zbierane, ani poddawane dalszemu przetwarzaniu w sposób nieuczciwy, oszukańczy lub bez wiedzy osoby, której dane dotyczą[19]. W literaturze podkreśla się ścisłą łączność między omawianą zasadą na gruncie obecnie obowiązujących przepisów oraz poprzedniej regulacji prawnej stwierdzając, iż nic nie wskazuje na to, aby ogólny obowiązek rzetelności (uczciwości) przetwarzania danych wiązał się z jakimkolwiek odstępstwem od dyrektywy, nadal przetwarzanie nie powinno naruszać innych przepisów lub obowiązków prawnych, a uczciwość jest wciąż ogólną zasadą nadrzędną[20].

W piśmiennictwie niemieckim wskazuje się, że użyte na określenie omawianej zasady w niemieckojęzycznej wersji rozporządzenia sformułowanie *Treu und Glauben* – „w dobrej wierze" znane jest jako klauzula prawa cywilnego, jednakże określenie to jako ogólna zasada przetwarzania danych powinno być rozumiane inaczej, czyli z uwzględnieniem kontekstu normatywnego ogólnego rozporządzenia o ochronie danych, gdyż w tym zakresie zostało uregulowane autonomicznie[21]. Mając na uwadze znaczeniową otwartość tej zasady, może być ona rozumiana jako zbiór okoliczności faktycznych (zespół znamion naruszenia), obejmujący przede wszystkim sytuacje, w których podmiot danych doświadcza niekorzystnych skutków w wyniku przetwarzania jego danych osobowych, co pozostaje w sprzeczności z określonym w unijnym rozporządzeniu ogólnym ukształtowaniem równowagi sił między podmiotem danych a administratorem, jednak bez naruszenia określonego przepisami prawa (konkretnego) zakazu[22]. W wyjątkowych przypadkach, w których brakuje stosownych uregulowań, możliwa pozostaje ocena przetwarzania jako niezgodnego z prawem, włączenie omawianego wymogu do unijnego rozporządzenia legitymizuje tego rodzaju miernik i pozwala na „otwarcie drzwi" dla uzasadnienia rozstrzygnięcia sądowego, którego nie dałoby się inaczej uzasadnić[23]. Zasada ta stanowi normę kierunkową dla uwzględnienia ochronnego celu rozporządzenia 2016/679 (określonego w jego art. 1 ust. 2) przy stosowaniu jego przepisów i zabrania niedopuszczalnego wykonywania praw przez administratora na niekorzyść osoby, której dane dotyczą[24].

---

19 C. de Terwangne, *Komentarz do art. 5* [w:] *The EU General Data Protection Regulation (GDPR). A Commentary*, red. Ch. Kuner, L.A. Bygrave, Ch. Docksey, Oxford 2020, s. 314.

20 R. Jay, *The Principles and Grounds for Processing* [w:] *eadem*, W. Malcolm, W. Parry *et al.*, *Guide to the General Data Protection Regulation. A Companion to Data Protection Law and Practice*, Thomson Reuters 2017, s. 85.

21 T. Herbst, *Komentarz do art. 5* [w:] *Datenschutz – Grundverordnung / BDSG. Kommentar*, red. J. Kühling, B. Buchner, München 2018, s. 215.

22 *Ibidem*, s. 217.

23 Por. E. Frenzel, *Komentarz do art. 5* [w:] *Datenschutz – Grundverordnung*, red. B.P. Paal, D.A. Pauly, 2017, s. 74.

24 H. Heberlein, *Komnetarz do art. 5* [w:] E. Ehmann, M. Selmayr, *DSV-GVO. Datenschutz – Grundverordnung. Kommentar*, München 2018, s. 192.

Rzetelność a uczciwość przetwarzania danych

W polskiej literaturze przedmiotu wymóg rzetelności przetwarzania danych jest różnie rozumiany. W komentarzach do ogólnego rozporządzenia o ochronie danych niektórzy autorzy (niekiedy odwołując się do określenia omawianej zasady w innych językach), utożsamiają rzetelność z uczciwością przetwarzania[25], jednak z uwagi na odmienne znaczenie wskazanych powyżej pojęć, rzetelność może być rozumiana szerzej niż uczciwość.

Zgodnie ze słownikową definicją „rzetelny" oznacza: „1. wypełniający należycie swoje obowiązki, uczciwy, słowny, solidny, sumienny, godny zaufania; 2. dokładny, należyty, właściwy"[26]. W języku potocznym pojęcie rzetelności łączy się zazwyczaj z wymogiem należytego wypełniania swoich obowiązków, określenie to jest bliskie znaczeniowo prawnemu pojęciu staranności, które – jak wspomniano powyżej – w kwalifikowanej jego postaci (jako „szczególna staranność") było uznawane za odpowiednik wymogu „rzetelności przetwarzania" na gruncie u.o.d.o.1997.

W kontekście prawnej regulacji ochrony danych osobowych, uwzględniając brak legalnej definicji omawianego pojęcia, należy przyjąć, że znaczenie określenia „rzetelny" nie odbiega od powszechnego rozumienia znaczenia tego słowa i tak też powinno być interpretowane. Określenie to jest szerokie i zawiera w sobie zarówno elementy odnoszące się do staranności w wykonywaniu swoich zadań (wypełniający należycie obowiązki, solidny, sumienny), jak również elementy dotyczące poszanowania praw podmiotu danych (uczciwy, godny zaufania). Oznacza to, że zasadę rzetelności przetwarzania rozumieć należy szerzej niż tylko jako należyte wypełnianie obowiązków (ocena dokonywana w kategoriach prawnych, dotycząca prawidłowego spełnienia obowiązków określonych przepisami), ale także jako uczciwość (ocena dokonywana w kategoriach etycznych, wykraczających poza ramy w postaci obowiązków wyraźnie określonych przepisami).

Tak rozumiana zasada rzetelności może być pojmowana jako swoista reguła naczelna wśród wszystkich ogólnych zasad przetwarzania danych osobowych. Stanowi ona najogólniejszą normę postępowania administratora, a zarazem łączy pozostałe zasady, nadając im szerszy wymiar. Można nawet twierdzić, że inne ogólne zasady przetwarzania danych wynikają z szeroko rozumianej zasady rzetelności i stanowią jej konkretyzację. Jest to widoczne na przykładzie wymogu przejrzystości, który przez wiele lat był formułowany w drodze wykładni zasady rzetelności, a który obecnie stanowi wyodrębniony wymóg, wyraźnie wskazany w art. 5 rozporządzenia 2016/679. Jednakże również inne zasady ogólne przetwarzania (np. zasada prawidłowości) są

[25] P. Drobek stwierdza: „rzetelnie, czyli uczciwie", zob. *idem*, *Komentarz do art. 5* [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 326. Tak również: A. Nerka, *Komentarz do art. 5*, teza 3 [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 143.

[26] *Mały słownik języka polskiego*, red. E. Sobol, Warszawa 1993, s. 825.

ściśle powiązane z zasadą rzetelności, a ich treść powinna być odczytywana w perspektywie omawianej zasady.

Realizacja podstawowego celu ochrony danych osobowych – zapewnienia ochrony osobom, których dane są przetwarzane wymaga nie tylko, by administratorzy prawidłowo wypełniali obowiązki nałożone na nich przepisami prawa, ale także aby postępowali uczciwie wobec podmiotów danych. Lojalność administratora wobec podmiotu danych przyczynia się do budowania relacji opartych na zaufaniu i pozwala bardziej skutecznie chronić prawa i interesy osób, których dane poddawane są przetwarzaniu.

Rzetelność w aspekcie należytego wypełniania obowiązków, to wymóg, aby administrator spełniający obowiązki określone przepisami o ochronie danych osobowych czynił to ze szczególną starannością, nie traktował obowiązków wyłącznie w kategoriach wymogów formalnych, ale także jako mechanizmy, które mają pozwolić na zapewnienie skutecznej ochrony podmiotów danych.

Administratorzy, przetwarzając dane, powinni działać „w dobrej wierze", jednak klauzula ta nie może być utożsamiana z występującą w prawie cywilnym (m.in. w art. 7 k.c.) dobrą wiarą w znaczeniu subiektywnym, rozumianą jako „stan psychiczny określonej osoby, polegający na jej błędnym, ale usprawiedliwionym mniemaniu o istnieniu jakiegoś prawa czy stosunku prawnego"[27]. W kontekście ochrony danych osobowych sformułowanie „dobra wiara" powinno być pojmowane w znaczeniu obiektywnym, jako wymóg „obiektywnej miary dla oceny czyjegoś zachowania się jako odpowiedniego lub nieodpowiedniego z punktu widzenia norm etycznych przyjętych w obrocie"[28].

Rzetelność w wymiarze uczciwości przetwarzania danych oznacza, że administrator powinien postępować etycznie, nie powinien wprowadzać podmiotu danych w błąd, działać podstępnie, oszukiwać, wykorzystywać jego trudnej sytuacji, ograniczeń bądź przymusowego położenia, wykorzystywać swojej silniejszej pozycji, narzucając uciążliwe warunki przetwarzania danych, a powinien szanować wolę i respektować interesy oraz słuszne oczekiwania osoby, której dane dotyczą.

Wprowadzenie w błąd może polegać m.in. na nieprzekazywaniu istotnych informacji, które mogą pozwolić podmiotowi danych na uświadomienie sobie konsekwencji udzielenia zgody na przetwarzanie danych. Działanie podstępne może przejawiać się np. w tym, że administrator ukrywa pewne informacje bądź nadmiernie eksponuje inne w celu osiągnięcia zamierzonego skutku (m.in. uzyskania zgody, niekorzystania z uprawnień), pozbawiając podmiot danych możliwości dokonania całościowej oceny. Działanie w sposób oszukańczy może wiązać się m.in. z wyłudzaniem danych osobowych poprzez składanie obietnic, których administrator nie zamierza dotrzymać. Wykorzystywanie trudnej sytuacji lub przymusowego położenia może dotyczyć m.in. prób uzyskania przez administratora zgody od osoby, która wskutek szczególnych okoliczności nie ma pełnej swobody decyzyjnej. Z kolei wykorzystywanie silniejszej

[27] J. Ignatowicz, K. Stefaniuk, A. Wolter, *Prawo cywilne. Zarys części ogólnej,* Warszawa 2017, s. 495.
[28] R. Longchamps de Berier, *Polskie prawo cywilne. Zobowiązania*, Lwów 1939, wydanie anastatyczne, Poznań 1999, s. 141.

pozycji może wiązać się z postępowaniem, które opiera się na założeniu, że podmiot danych nie ma możliwości wyboru usług świadczonych przez innego administratora[29].

Można zasadnie twierdzić, że nadużycie przez administratora zaufania podmiotu danych przejawiające się np. wprowadzeniem w błąd osoby, której dane dotyczą, może być negatywnie oceniane w kategoriach etycznych, co pozwala uznać, że mamy do czynienia z naruszeniem zasady rzetelności. W praktyce jednak kwestia naruszenia omawianej zasady powinna być oceniana indywidualnie, przy uwzględnieniu okoliczności konkretnej sprawy. Szczególnie istotną rolę w tym zakresie powinny odgrywać: organ nadzorczy oraz sądy rozstrzygające spory między administratorem a podmiotem danych.

Ogólne i abstrakcyjne ujęcie w przepisach zasady rzetelności nie oznacza jednak, że nie istnieją przewidziane prawem możliwości jej konkretyzacji. Z przepisów ogólnego rozporządzenia o ochronie danych wynika, że omawiana zasada może zostać doprecyzowana zarówno przez prawodawcę w przepisach krajowych określających obowiązki prawne ciążące na administratorze oraz gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym, lub w ramach sprawowania władzy publicznej powierzonej administratorowi, zgodnie z art. 6 ust. 2 rozporządzenia 2016/679, a także przez podmioty przygotowujące sektorowe samoregulacje w kodeksach postępowania przyjmowanych na podstawie art. 40 rozporządzenia 2016/679 i zatwierdzanych przez organ nadzorczy. Dzięki temu możliwe jest uwzględnienie specyfiki sektorowej i bardziej szczegółowe określenie wymogów odnoszących się do rzetelności przetwarzania danych.

Zakończenie

Z przedstawionych w artykule analiz można wyciągnąć kilka ogólnych wniosków. Zasada legalności, rzetelności i przejrzystości przetwarzania stanowi pierwszą i najważniejszą zasadę ogólną, i to w jej perspektywie powinno być oceniane każde postępowanie administratora. Rzutuje ona nie tylko na sposób wykonywania konkretnych obowiązków nałożonych na administratora przepisami, ale także na interpretację pozostałych ogólnych zasad oraz podstaw dopuszczalności przetwarzania danych (w tym w szczególności zgody). Można zasadnie twierdzić, że wymóg rzetelności przetwarzania stanowi swego rodzaju regułę naczelną, która pozostaje w ścisłym związku z innymi zasadami i wymogami nałożonymi na administratora i powinna wywierać istotny wpływ na sposób ich realizacji.

[29] Na ten aspekt braku uczciwości postępowania administratora zwrócili uwagę: P. Barta, M. Kawecki i P. Litwiński, przywołując przykład udostępnienia przez British Gas danych dla celów marketingowych innym podmiotom bez wyraźnej zgody osób, których dane dotyczą, w sytuacji gdy wskazany administrator zajmował pozycję monopolisty na rynku dostaw gazu. Por. *eidem*, *Komentarz do art. 5*, teza 4 [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021, s. 157.

Porównanie sformułowań wykorzystywanych w różnych wersjach językowych rozporządzenia 2016/679 na określenie omawianej zasady ukazuje różnorodność, a zarazem dużą pojemność znaczeniową wymogu rzetelności przetwarzania. Okoliczność ta może być uznawana za przesłankę wskazującą, że omawiany wymóg nie powinien być interpretowany wąsko i utożsamiany jedynie z uczciwością przetwarzania danych, ale należy rozumieć go szerzej – z uwzględnieniem innych aspektów rzetelności. Bez wątpienia istotne znaczenie dla interpretacji omawianej zasady ma także uwzględnienie poglądów prezentowanych w literaturze przedmiotu zarówno na gruncie poprzednio obowiązujących przepisów (dyrektywy 95/46/WE oraz krajowych regulacji prawnych), jak też w oparciu o obowiązujący stan prawny (rozporządzenie 2016/679).

Zasada rzetelności przetwarzania danych osobowych powinna być interpretowana szeroko, zgodnie z powszechnym rozumieniem jej znaczenia. Obejmuje ona nie tylko wymóg starannego, należytego wypełniania przez administratora obowiązków nałożonych przepisami prawa, ale także wymóg uczciwości działania, wykraczający poza sferę normatywną, a odnoszący się do ocen etycznych. Różnorodne przejawy nieuczciwości administratora (m.in. zamierzone działania mające na celu wprowadzenie podmiotu danych w błąd, działania podstępne lub oszukańcze) powinny być uznawane za naruszenie omawianej zasady. Jednak ocena w tym zakresie powinna być dokonywana w każdym przypadku indywidualnie, z uwzględnieniem okoliczności faktycznych danej sprawy.

Literatura

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2015.

Barta P., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016.

Bygrave L.A., *Data protection law. Approaching Its Rationale, Logic and Limits*, Hague – London – New York 2002.

Carey P., *Data Protection. A Practical Guide to UK and EU Law*, Oxford 2004.

Datenschutz – Grundverordnung / BDSG. Kommentar, red. J. Kühling, B. Buchner, München 2018.

Datenschutz – Grundverordnung, red. B.P. Paal, D.A. Pauly, München 2017.

Drobek P., *Komentarz do art. 5* [w:] *RODO. Ogólne rozporządzenie o ochronie danych*. *Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Drozd A., *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2007.

Ehmann E., Helfrich M., *EG Datenschutzrichtlinie. Kurzkommentar*, Kolonia 1999.

Fajgielski P., *Zasady ogólne przetwarzania i ochrony danych osobowych* [w:] *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, red. G. Goździewicz, M. Szabłowska, Toruń 2008.

Handbook on European data protection law, Luksemburg 2014.

Ignatowicz J., Stefaniuk K., Wolter A., *Prawo cywilne. Zarys części ogólnej*, Warszawa 2017.

Jagielski M., *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010.

Jay R., Malcolm W., Parry E., Townsend L., Bapat A., *Guide to the General Data Protection Regulation. A Companion to Data Protection Law and Practice*, Thomson Reuters 2017.

Korff D., *EC study on implementation of data protection directive. Comparative study of national law*, Cambridge 2002.
Longchamps de Berier R., *Polskie prawo cywilne. Zobowiązania*, Lwów 1939, wydanie anastatyczne, Poznań 1999.
Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. M. Sakowska-Baryła, Warszawa 2018.
Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, red. P. Litwiński, Warszawa 2021.
RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.
The EU General Data Protection Regulation (GDPR). A Commentary, red. Ch. Kuner, L.A. Bygrave, Ch. Docksey, Oksford 2020.
Tinnefeld M.T., Ehmann E., *Einführung in das Datenschutzrecht*, Monachium 1998.

Streszczenie

Paweł Fajgielski

Rzetelność jako ogólna zasada przetwarzania danych osobowych

W artykule omówiona została zasada (wymóg) rzetelności przetwarzania danych osobowych. Zasada legalności, rzetelności i przejrzystości przetwarzania stanowi pierwszą i najważniejszą zasadę ogólną, w perspektywie której powinno być oceniane każde postępowanie administratora. Rzutuje ona nie tylko na sposób wykonywania konkretnych obowiązków nałożonych na administratora przepisami, ale także na interpretację pozostałych ogólnych zasad oraz podstaw dopuszczalności przetwarzania danych (w tym w szczególności zgody). W artykule zaprezentowana została teza, zgodnie z którą wymóg rzetelności przetwarzania stanowi swego rodzaju regułę naczelną, która pozostaje w ścisłym związku z innymi zasadami i wymogami nałożonymi na administratora i powinna wywierać istotny wpływ na sposób ich realizacji.

Przedstawione w artykule porównanie sformułowań wykorzystywanych w różnych wersjach językowych rozporządzenia 2016/679 na określenie omawianej zasady ukazuje różnorodność, a zarazem dużą pojemność znaczeniową wymogu rzetelności przetwarzania.

W artykule przywołane zostały różnorodne poglądy dotyczące rzetelności, prezentowane w literaturze zarówno na gruncie poprzednio obowiązujących przepisów (dyrektywy 95/46/WE oraz krajowych regulacji prawnych), jak i w oparciu o obowiązujący stan prawny (rozporządzenie 2016/679).

Z zaprezentowanych w artykule analiz wynika ogólny wniosek, że zasada rzetelności przetwarzania powinna być interpretowana szeroko. Obejmuje ona nie tylko wymóg starannego, należytego wypełniania przez administratora obowiązków nałożonych przepisami prawa, ale także wymóg uczciwości działania, wykraczający poza sferę normatywną, a odnoszący się do ocen etycznych. Różnorodne przejawy nieuczciwości administratora (m.in. zamierzone działania mające na celu wprowadzenie podmiotu danych w błąd, działania podstępne lub oszukańcze) powinny być uznawane za naruszenie omawianej zasady. Jednak ocena w tym zakresie powinna być dokonywana w każdym przypadku indywidualnie, z uwzględnieniem okoliczności faktycznych danej sprawy.

Słowa kluczowe: zasady przetwarzania danych osobowych; rzetelność przetwarzania; uczciwość przetwarzania; ogólne rozporządzenie o ochronie danych.

Summary

Paweł Fajgielski

Fair Processing as a General Principle of Personal Data Processing

The article discusses the requirement of fair processing of personal data. The principle of lawful, fair and transparent processing is the first and most important general principle against which each conduct of the controller should be assessed. It affects not only the manner of performing specific obligations imposed on the controller by regulations, but also the interpretation of other general principles and requirements for lawfulness of data processing (including in particular the data subjects consent). The article presents the thesis that the requirement of fair processing is a kind of supreme rule, which is closely related to other principles and requirements imposed on the controller and should have a significant impact on the manner of their implementation.

A comparison of the wording used in various language versions of GDPR to describe the discussed principle shows the diversity and, at the same time, a large semantic capacity of the requirement of fair processing.

The article cites various views on fairness presented in the literature, both on the basis of the previously applicable law (Directive 95/46/EC and national laws) and on the basis of the present legal regulation (GDPR). The analysis presented in the article leads to the conclusion that the principle of fair processing should be interpreted broadly. It includes not only the requirement of diligent and proper performance of the obligations imposed on the controller by law, but also the requirement of honesty, going beyond the normative sphere, and relating to ethical assessments. Various not fair actions of the controller (including deliberate actions aimed at misleading the data subject, deceptive or fraudulent actions) should be considered a breach of this principle. However, the assessment of fairness processing should be made on a case-by-case basis, taking into account the facts of the case.

Keywords: principles relating to personal data processing; fair processing; fairness; GDPR.

Dan Jerker B. Svantesson
Bond University, Australia
dasvante@bond.edu.au
ORCID: 0000-0003-2106-5594

https://doi.org/10.26881/gsp.2021.4.02

International Data Transfers post *Schrems* – Moving Towards Solutions

The statement that the modern world depends on international data transfers is difficult to dispute. However, the statement that international data transfers may undermine the protection of personal data is equally difficult to dispute. In this we see both a problem and a desired outcome. The problem we see is a clash between two important objectives. Or more precisely, we see a clash between, on the one hand, an important multifaceted objective and, on the other hand, the protection of a complex fundamental human right with implications going far beyond that right itself. The desired outcome we see is that we, somehow, must facilitate data privacy respecting international data transfers.

The above ought to be relatively uncontroversial. However, as soon as we move towards the obvious question that flows from the above – namely that of *how* we can facilitate data privacy respecting international data transfers – we enter a territory best described as a combination of a minefield and a quagmire. To make progress in such an environment we must proceed with caution and yet avoid getting bogged down in the unavoidable challenges, such as definitional challenges, we will face.

In this article, I will seek to canvass a selection of key considerations that ought to be kept in mind when we discuss approaches to international data transfers. However, to prepare ground for that discussion, I will first set the scene by examining the so-called *Schrems II* decision, its larger context and background, as well as some of the reactions we have seen to that decision.

Finally, by way of introduction, I wish to make clear that I have opted not to provide any overview of the applicable legal provisions as such.[1] Just restating – without any commentary – the relevant provisions (art. 44–50) of the General Data Protection Regulation[2] (GDPR) would have taken up just under 3,000 words, or approximately

[1] See instead: Ch. Kuner, *Articles 44–50 Chapter V* [in:] *The EU General Data Protection Regulation (GDPR): A Commentary*, eds *idem et al.*, Oxford University Press 2020, pp. 755–862.

[2] 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), OJ 2016 L 119/1.

50% of the space of this article. This illustrates the considerable complexity with which this area of law is associated.

1. Generally about international data transfers

Protecting privacy, including data privacy, is not optional. Rather it is necessary to always keep in mind that we are dealing with a fundamental human right. This, in itself, imposes limitations on what solutions can ever be regarded as acceptable. And as hinted at above, in the right to data privacy, we find a right that is complex – indeed, hard to define and delineate – and that is an important enabler of other human rights. Indeed, the protection of data privacy is an essential feature of any democratic form of governance.

The protection afforded by national data privacy laws is easily circumvented if the personal data they are meant to protect can be transferred to third countries without appropriate controls, safeguards and limitations. This is the most obvious and undisputable justification for the restrictions that data privacy laws commonly impose on international data transfers. At the same time, as observed already in the introduction, the societies we have built are now interacting to such a degree that crucial aspects would grind to a halt if personal data were not allowed to be transferred between countries. Writing an article in 2016 commenting on the *Schrems I* decision, I described this tension as the first of the many Gordian knots that characterise this area of law.[3]

The Covid-19 pandemic, that still holds the world in its grip at the time of writing, has showcased just how dependent we are on the Internet and its inherent cross-border data flows. However, this is of course by no means an issue specific to our online environment. International data transfers are also common – not to say essential – in many other settings such as international travel, international trade, employment records in multinationals, and in relation e.g., to research and health data.[4]

The need to strike a balance that upholds the right to privacy in an enforceable rather than symbolic manner, and that generates justified rather than blind trust is obvious.

[3] D. Svantesson, "Cross-border data transfers after the CJEU's Safe Harbour Decision – A tale of Gordian Knots," *Alternative Law Journal* 2016, no. 41(1), pp. 39–42.

[4] For a discussion of transborder health data flows, including research data, see e.g.: D. Mascalzoni, H.B. Bentzen *et al.*, "Are Requirements to Deposit Data in Research Repositories Compatible With the European Union's General Data Protection Regulation?," *Annals of Internal Medicine* 2019, no. 170(5), pp.332–334; and H.B. Bentzen, D. Svantesson, "Jurisdictional Challenges Related to DNA Data Processing in Transnational Clouds," [in:] *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, eds D. Svantesson, D. Kloza, Intersentia Ltd 2017, pp. 241–260.

2. Briefly about the lead up to *Schrems II*

The European Data Protection Supervisor (EDPS) has done us all a great favour by putting together and publishing its valuable "Case Law Digest" specifically on the topic of transfers of personal data to third countries.[5] This 10 June 2021 publication provides a structured and systematic overview of the case law developments that led us to where we are today.

I will not repeat that discussion here. Instead, I will limit myself to a very brief overview of the most important features of the three key cases that preceded *Schrems II* focusing on, and admittedly eclectic selection of issues I see as key to understanding this area.

2.1. Case C-101/01 *Lindqvist*

At the time of writing, the *Lindqvist* case is already turning 18 years old. However, conclusions reached in the case are still of significance. And since this matter dealt with issues somewhat different to those of the other authorities I will mention here, I will spend some time on this case. In *Lindqvist*, the Court concluded:

> There is no "transfer [of data] to a third country" […] where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.[6]

While this conclusion is interesting in its own right, it is also worthwhile to examine how the Court reached that conclusion. Having noted that "it is necessary to take account both of the technical nature of the operations thus carried out and of the purpose and structure of Chapter IV [GDPR Chapter V] of that directive where Article 25 appears,"[7] the Court made some observations as to the relevant technical setup. In particular it noted that, "Lindqvist's internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access to those pages."[8]

It is, of course, correct to note, as the Court did, that Lindqvist could not transfer the content of her website to an Internet user who was not connected to the Internet at the time, or who did not wish to take the steps necessary to visit her website. That is, however, equally true e.g., for TV broadcasts and the Court's justification of their approach, by reference to the relevant technology, is rather unconvincing. Further, we

---

5 European Data Protection Supervisor, *Case Law Digest: Transfers of personal data to third countries* (2021) https://edps.europa.eu/data-protection/our-work/publications/court-cases/case-law-digest-2021-transfers-personal-data_en [accessed: 2021.09.09].

6 Case C-101/01, *Bodil Lindqvist*, ECLI:EU:C:2003:596, p. 100.

7 *Ibidem*, par. 57.

8 *Ibidem*, par. 60.

may wonder how this relates to modern social media that indeed pushes content from one user to others who have the relevant app installed.

The Court then turned to the purpose of the relevant part of the Directive. In doing so, the Court observed that "Chapter IV of Directive 95/46 [GDPR Chapter V] contains no provision concerning use of the internet."[9] And went on to note that therefore "one cannot presume that the Community legislature intended the expression 'transfer [of data] to a third country' to cover" the type of Internet conduct in question.[10]

This conclusion is somewhat surprising. The fact that the Directive does not make specific mention of the Internet, suggests that it was drafted in technology-neutral language. Where that is the case, it cannot be assumed that the drafters did not intend the Directive to apply to Internet-related activities such as in the *Lindqvist* case. Rather, it seems at least equally likely that the technology-neutral language suggests that the application of the Directive should not be dependent on the technology in question.

Finally, and perhaps of broadest relevance, it is interesting to observe how the Court in the *Lindqvist* case, departed from a literal interpretation of the applicable law, and adopted a "consequence focused approach"[11] basing its decision in important respects on what would be the consequences of its decision:

> [i]f Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet.

As the Court noted, this would necessarily turn the special regime provided for by Chapter IV of the directive into a regime of general application, as regards operations on the Internet.[12] This consequence focused approach is of great use in the technology law field, it is far too rare, and it ought to be more broadly adopted by courts (and indeed more consistently adopted by the Court of Justice of the European Union – CJEU).

2.2. Case C-362/14 *Schrems I*

Through a decision of July 2000, the European Commission made a finding that the US Safe Harbour scheme met the required adequacy level. This decision opened the door for extensive transatlantic data transfers.

The Safe Harbour regime can be seen as a pragmatic structure that managed to combine European data privacy traditions with the US tradition of data privacy as a consumer right. However, it was a structure that was built on sand; in fact, as the CJEU's decision in *Schrems I* shows, it was a structure for which a building permit

---

9 *Ibidem*, par. 67.
10 *Ibidem*, par. 68.
11 See further: D. Svantesson, "What is 'Law', if 'the Law' is Not Something That 'Is'? A Modest Contribution to a Major Question", *Ratio Juris* 2013, no. 26(3), p. 456.
12 Case C-101/01…, par. 69.

should never have been granted. Thus, as the main outcome of *Schrems I*, the CJEU held the Commission's July 2000 adequacy finding to be invalid, and it was made clear that transfers could no longer be made in reliance on the Safe Harbour scheme. Importantly, the Court emphasised that:

> Article 25(6) of Directive 95/46 implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in point 139 of his Opinion, is intended to ensure that the high level of that protection continues where personal data is transferred to a third country.[13]

This highlights that the application of the provisions that regulate international data transfers is firmly guided by the EU Charter of Fundamental Rights (the Charter).[14] Furthermore, the CJEU ruled that a Commission adequacy finding:

> does not prevent a supervisory authority of a Member State [...] from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.[15]

Relatedly, the CJEU's judgment made clear that only the CJEU has jurisdiction to declare that a Commission adequacy finding is invalid. In addition, the judgment provided guidance as to the more precise meaning of a country providing an adequate level of protection:

> [T]he term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union.[16]

To conclude this section, it may be noted that, in *Schrems I*, the Court adopted a more formalistic approach to the law than it did in *Lindqvist*.

2.3. Opinion 1/15 *EU-Canada PNR Agreement*

The CJEU issued Opinion 1/15 in response to the European Parliament's request relating to an agreement envisaged between Canada and the European Union on the transfer and processing of Passenger Name Record data. The Court concluded that the draft agreement could not be concluded in its proposed form. Most importantly for our context, this conclusion was reached based on the observation that several of the agreement's provisions were incompatible with fundamental rights provided under the Charter. The Court referred to *Schrems I* and re-emphasised that the "right to

---

13 Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650, par. 72.
14 Charter of Fundamental Rights of the European Union, OJ 2000, C 364/01 and OJ 2010, C 83/389.
15 Case C-362/14…, par. 107.
16 *Ibidem*, par. 73.

the protection of personal data requires, inter alia, that the high level of protection of fundamental rights and freedoms conferred by EU law continues where personal data is transferred from the European Union to a non-member country."[17] Further, as noted by Kuner in his expert analysis of the matter, Opinion 1/15 indicates that the Court will hold international agreements to a strict standard of fundamental rights protection.[18]

3. Case C-311/18 *Schrems II* – overview, implications, and comments

When it became clear that the aftermath of the *Schrems I* case included a new mechanism – Privacy Shield – sharing many features with the abandoned Safe Harbour structure, the fact that there would be a *Schrems II* decision[19] was not surprising. Like the initial *Schrems I* matter, *Schrems II* was referred to the CJEU by the Irish High Court, and on this occasion the Irish court referred no less than 10 different questions to the CJEU.

In essence, the matter related to whether the US surveillance programmes interfered with the fundamental rights to privacy, to data protection and to effective judicial protection in such a manner as to render transfer of personal data to the US unjustifiable. To that end, the judgment addressed several issues. Importantly, the CJEU made clear that the GDPR:

> […] applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.[20]

Further, the Court held the Privacy Shield invalid, and concluded that: "data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union".[21]

The *Schrems II* decision resulted in intense academic debates.[22] From an international perspective, it is particularly interesting to note how the decision has been

---

17 *Ibidem*, par. 134.

18 Ch. Kuner, "International Agreements, Data Protection, and EU Fundamental Rights on the International State: Opinion 1/15, EU-Canada PNR," *Common Market Law Review* 2008, p. 55.

19 Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, ECLI:EU:C:2020:559.

20 *Ibidem*, par. 203.

21 *Ibidem*.

22 See e.g. Ch. Kuner, "Schrems II Re-Examined", *Verfassungsblog.de* 25 August 2020, https://verfassungsblog.de/schrems-ii-re-examined/ [accessed: 2021.09.09] and D. Korff, "Korff on Kuner: *Schrems II* Re-Examined," 3 September 2020, https://www.ianbrown.tech/2020/09/03/korff-on-kuner-schrems-ii-re-examined/ [accessed: 2021.09.09]; that purports to be a response to Kuner but that, in too large parts, rather appears intent on reading more into Kuner's statements than reasonable may be justified.

approached in the context of whether the conditions data privacy laws traditionally impose on transborder data transfers are properly viewed as measures imposing data localisation requirements. As to *Schrems II* Chander notes:

> I do not mean to suggest that *Schrems II* requires data localization or that it is even the recommended response. […] However, by failing to offer any guidance as to what such additional measures might be, it creates uncertainty. […] Thus, even while *Schrems II* does not establish a *de jure* requirement for data localization, its encumbrances on cross-border data flows to the United States, and to other foreign countries, seem to point many businesses to use data localization to solve the problems the decision poses.[23]

This is, of course, both an important and a correct observation. And perhaps it can be seen as a step back from Chander's earlier claim (with Le) as to data privacy laws: "While these laws are not explicitly designed to localize data, by creating significant barriers to the export of data, they operate as data localization measures."[24]

In my view, we gain nothing but confusion if we broaden the definition of data localisation so as to encompass by default the conditions data privacy laws traditionally impose on transborder data transfers. After all, there is a significant difference between something being banned and something only being allowed under stated conditions. More specifically in our context, there is a significant difference between a requirement mandating that data be stored or processed in a specific jurisdiction, on the one hand, and conditions being imposed on the transfer of data to another country, on the other hand. Thus, I have advanced the following, more narrow definition of data localisation: "'Data localisation' refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction."[25] With that definition in mind, I have recommended that "the conditions data privacy laws traditionally impose on transborder data transfers do not necessarily amount to data localisation."[26] I will have reason to return to the topic of data localisation in the below.

The CJEU's *Schrems II* decision has also led to intensive activity from the relevant European Union bodies.[27] At the time of writing, the most recent, development flowing from the *Schrems II* decision is the Commission's Decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. All these de-

---

[23] A. Chander, "Is Data Localization a Solution for Schrems II?", Georgetown Law Faculty Publications and Other Works 2020, 2300, p. 2, https://scholarship.law.georgetown.edu/facpub/2300 [accessed: 2021.09.09].

[24] A. Chander, U. Le, "Data Nationalism", *Emory Law Journal* 2015, vol. 64/3, p. 677, p. 718.

[25] D. Svantesson, "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", *OECD Digital Economy Papers* 2021, no. 301, OECD Publishing, Paris, p. 8, http://dx.doi.org/10.1787/7fbaed62-en [accessed: 2021.09.09].

[26] *Ibidem*, p. 26.

[27] See e.g.: EDPB – EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679.

velopments are deserving of detailed scrutiny. However, that goes beyond the scope of this article.

4. Selected key considerations as we move forward

So, are we stuck? The above might point to an impossible situation where there is no prospect of appropriate solutions that can both cater for international data transfers and at the same time, uphold a data privacy protection meeting the standards of the Charter. However, there are reasons to think that progress can, indeed, be made. Not least the old proverb that necessity is the mother of invention should give us hope. We quite simply must find solutions, and it would be useful for those solutions to be more long-term than was the temporary "patch" provided by the Privacy Shield.

In a publication stemming from my time in 2010 as a Visitor at the European University Institute, I explored options for reform in this field in some detail.[28] I will not repeat that discussion here. Rather, I will seek to bring attention to a range of considerations that ought to be kept in mind when we discuss approaches to international data transfers.

4.1. Identifying the "baseline" and the "zone of flexibility"

Discussions of balancing data privacy protection with other interest and rights are unpopular activities. And it is, of course, true that not all interests are equal and not everything is up for negotiation. Regardless of what trade advantages may be gained, data privacy cannot be traded away in a manner that undermines the data subjects' fundamental rights. In the immortal words of Spiros Simitis: "[t]his is not bananas we are talking about."[29] There is a "baseline" that must not be crossed.

At the same time, above this non-negotiable "baseline" set by human rights law, there is a "zone of flexibility". Within that zone we may pursue solutions that cater for all interests involved, and we may, indeed, pursue options that provide protection beyond the mentioned baseline, for example, by pursuing paths facilitating the adoption of privacy as a competitive advantage.

In my view, we need a more open discussion about what falls within the "baseline" and what fits within the "zone of flexibility".

4.2. The right level of granularity

As is clear already from this article, it is common practice to observe a tension between, on the one hand, the need for international data transfers, and, on the other

[28] D. Svantesson, "A legal method for solving issues of Internet regulation; applied to the regulation of cross-border privacy issues," *European University Institute Working Paper LAW* 2010, no.18.

[29] Cited by Lee Bygrave "International agreements to protect personal data" [in:] *Global Privacy Protection: The First Generationeds*, eds J. Rule, G. Greenleaf, Edward Elgar 2008, p. 15.

hand, the need for effective data privacy protection. However, in our context, that is perhaps an unhelpful "macro perspective". Perhaps we need to approach the considerations involved with greater granularity; that is, perhaps we are better served if we start analysing what types of international data transfers we are talking about, and what aspects of data privacy protection we are calling for.

Put simply, we can acknowledge the general value of international data transfers without assuming that all types of such transfers are of equal importance and value. Some such transfers – consider e.g., Opinion 1/15 – are important for the purpose of national security. Others are motivated by economic considerations such as "economies of scale". Yet others stem from technical structures that force us to consider whether it is current technological realities, or indeed the law, that is the proverbial "tail wagging the dog". It is not my aim here to assess how these grounds for international data transfers stack up when compared to data privacy interests. However, to me it seems crucial to acknowledge that not all current situations involving international data transfers are of equal importance.

Similarly, as alluded to, we must acknowledge the necessity of ensuring effective data privacy protection without assuming that all aspect of all data privacy laws are equally necessary for an adequate level of protection.

Admittedly, much work remains, and many severe challenges must be tackled along the way to solutions. For example, it may be noted that data typically is collected and transferred in bundles that contain both personal, and non-personal, data. This creates complications. However, already by moving into this greater granularity we ca move closer to a position in which the various objectives involved may be properly evaluated and either reconciled or at least balanced.

4.3. It takes two to tango

Where country A's data privacy law imposes conditions on international data transfers with the result that data cannot be transferred from country A to country B, it is commonplace to see country A's data privacy law as restrictive or even protectionist – it is country A's data privacy law that is blamed for the impossibility of the transfer. However, that is an unhelpful oversimplification. What we are faced with in any such a situation is a compatibility issue. Country A's and country B's laws are quite simply not compatible enough to facilitate the data transfer in question. Country B's inadequate data privacy protection is equally much the cause of the resulting barrier to data transfers. As the saying goes, 'it takes two to tango' and we will get no closer to solutions if we do not recognise this.

To my mind, this also has implications for discussions as to whether the restrictions data privacy laws commonly impose on international data transfers amount to 'data localisation'. If we recognise that the cause of the transfer being prevented is a compatibility issue, that lends support to the conclusion that the conditions data privacy laws traditionally impose on transborder data transfers do not necessarily amount to data localisation.

At any rate, if it is conceded that we are here dealing with a compatibility issue, we can usefully link into – and draw from – the discussion of "legal interoperability"[30] or the related concept of "jurisdictional interoperability".[31] Put simply, legal interoperability involves "the process of making legal norms work together across jurisdictions",[32] while the aim of jurisdictional interoperability is more modest and involves reaching a situation "where we have: (1) only a minimal level of serious jurisdictional clashes, and (2) an acceptable level of less serious jurisdictional clashes".[33] In a similar manner to how we now routinely work with privacy-by-design and security-by-design, perhaps the time has come to pursue "jurisdictional interoperability-by-design"?[34]

4.4. A "layered approach" facilitating interoperability

During the discussions that preceded that final version of the GDPR, I proposed what I termed a "layered approach" for the (territorial) scope determined in art. 3.[35] In essence my point was that, in the case of a diverse instrument such as the GDPR that contains both (virtually) globally accepted abuse-prevention provisions (the "abuse-prevention layer" e.g., Article 5), widely accepted rights (the "rights layer", e.g., Article 15), as well as bureaucratic administrative rules with few equivalents elsewhere (the "administrative layer" e.g., art. 37), it is inappropriate to apply the same threshold test for the applicability of all these rules to foreign parties. In other words, we need different tests regulating when such a party must comply with these rules, and we could cater for a lower threshold, and thus a wider reach for, the provisions of the "abuse-prevention layer" than for the other two layers. This thinking – if adopted in relation to application of the international data transfer rules – may have the potential to contribute towards the interoperability I discussed immediately above.

For example, in the context of any assessment of whether a foreign country's data privacy protection is "essentially equivalent to that guaranteed within the European Union", perhaps it is not necessary to take account of the entire GDPR in every situation? In a general sense, perhaps the administrative layer alluded to above is far less important than is the abuse-prevention layer and the rights layer, and indeed,

---

[30] See in particular: J. Palfrey, U. Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems*, Basic Books 2012; and R.H. Weber, "Legal Interoperability as a Tool for Combating Fragmentation" (2014) Global Commission on Internet Governance Paper Series No 4 (Centre for International Governance Innovation).

[31] See: D. Svantesson, "The holy trinity of legal fictions undermining the application of law to the global Internet," *International Journal of Law and Information Technology* 2015, vol. 23, no. 3 (2015); pp. 219–234. See further: D. Svantesson, *Solving the Internet Jurisdiction Puzzle*, Oxford 2017, pp. 113–121.

[32] J. Palfrey, U. Gasser, *Interop: The Promise*…, p.178.

[33] D. Svantesson, *Solving the Internet*…, p. 120.

[34] See further: D. Svantesson, "Internet & Jurisdiction Global Status Report 2019", Internet & Jurisdiction Policy Network 2019, Paris, p. 158.

[35] See: D. Svantesson, "A 'layered approach' to the extraterritoriality of data privacy laws," *International Data Privacy Law* 2013, no. 3(4); pp. 278–286. See further: D. Svantesson, *Solving the Internet*…, pp. 191–200.

the latter two may be much more palatable to a foreign country pursuing essentially equivalence. At least for those who are open to some form of compromises, this may represent one possible tool for increasing interoperability.

4.5. The problem of "mandate-driven compartmentalisation"

I suspect that a key reason why it often is so difficult to make progress on Internet regulation issues is found in what we may term "mandate-driven compartmentalisation"; that is, while there are many bodies that may develop useful regulatory approaches, they are all working within limited mandates preventing an effective, comprehensive, approach. In this context, it may be noted that the stakeholder survey of the Internet & Jurisdiction Global Status Report 2019[36] – the world's first comprehensive mapping of Internet jurisdiction-related policy trends, actors and initiatives – found that 79% of the surveyed experts do not think there is sufficient international coordination and coherence to address cross-border legal challenges on the Internet.[37]

The regulation of international data transfers is illustrative. Multiple bodies are working on international data transfers. Some do so exclusively from a trade perspective, others from a human rights perspective, yet others focus on law enforcement access to e-evidence etc. However, the problem is that all these issues are interlinked, and we may not be able to find appropriate solutions to any one unless we consider all at once.

4.6. The strong link between security and data privacy

Looking at decisions such as Opinion 1/15, *Schrems I*, and *Schrems II*, as well as cases not discussed above including *Digital Rights Ireland*,[38] *Google Spain*,[39] it is clear that the interest of national security and law enforcement may collide with the right of data privacy. However, it is also clear that those interest may pull in the same direction as data privacy in other instances.[40] In fact, the seemingly ever-increasing threat posed by cybercriminals targeting personal data means that we more and more frequently see clashes where the privacy interests of the suspect must be weighed against the privacy interests of the many victims of the criminal activity targeting personal data. In other words, we find ourselves in a privacy vs. privacy situation in which some privacy

---

36 The Report is based on a large-scale data contribution from 150 key stakeholders from the Internet & Jurisdiction Policy Network from: states, internet companies, technical operators, civil society, academia and international organisations. A full list of the contributing experts is provided in the Report (D. Svantesson, "Internet & Jurisdiction Global Status Report 2019", Paris, Internet & Jurisdiction Policy Network 2019, pp. 9–13).

37 D. Svantesson, "Internet & Jurisdiction Global…, p. 35.

38 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland & Seitlinger*, ECLI:EU:C:2014:238.

39 Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González*, ECLI:EU:C:2014:317.

40 This is discussed in some detail in: Radim Polčák, Dan Svantesson, *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*, Edward Elgar Publishing 2017.

interests – namely those of the victims – fall on the same side of the equation as does the interest of law enforcement. This is important. However, for anyone seeking solutions relating to international data transfers, there is another observation we can make that is even more significant.

Looking at the decisions mentioned above, it seems to me that we need to approach data privacy, and access to evidence by law enforcement and national security as a package. That is, the concerns about US access to EU personal data discussed in *Schrems II* cannot be overcome merely by focusing on data privacy law alone. Rather, we need to seek solutions that cater for the legitimate needs of law enforcement and national security without data protection being undermined by law enforcement and national security when personal data from the EU enters the US.

The Mutual Legal Assistance (MLA) structure is being improved.[41] Negotiations are in place in relation to improved mechanisms for direct request – across borders – to providers.[42] The Council of Europe's Budapest Convention is being amended by another Additional Protocol.[43] The United Nations Office on Drugs and Crime (UNODC), the United Nations Counter-Terrorism Committee Executive Directorate (CTED) and the International Association of Prosecutors (IAP), have jointly drafted and launched their updated 2021 *Practical Guide for Requesting Electronic Evidence Across Borders*,[44] and there is a forthcoming 2021 *Data Disclosure Framework*[45] that outlines practices developed by international service providers in responding to overseas government requests for data. These are all promising steps that together may create an environment in which it is sufficiently easy for US law enforcement to obtain data from Europe, in a human right respecting manner, for there to be no need for the type of privacy infringements of concern in the *Schrems II* matter.

Of course, I am not so naive as to think this will be an easy journey. Quite the contrary. However, I do think that it is a more plausible path forward than are the alternatives. The EU will not lower the "baseline" set by the Charter, and the US will not simply stop requiring data for law enforcement and national security.

4.7. The need for scalability

In international law, much weight is given to state practice.[46] This ought to create a strong incentive for countries to pursue scalable universal approaches given that a broad uptake of their approaches legitimacies those approaches. However, scalabil-

41 See further: D. Svantesson, "Internet & Jurisdiction Global…, pp. 104–105.

42 For an overview of the issues involved, see: Internet & Jurisdiction Policy Network Toolkit Cross-border Access to Electronic Evidence, 2021.

43 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, [accessed: 2021.09.09].

44 https://sherloc.unodc.org/cld/en/st/evidence/practical-guide.html [accessed: 2021.09.09].

45 https://sherloc.unodc.org/cld/en/st/evidence/ddf.html [accessed: 2021.09.09].

46 See in particular: art. 38(1)(b) Statute of the International Court of Justice.

ity does not seem to have been considered much in the context of international data transfers.

Rather, states base their approaches solely on domestic law and their needs with the occasional reference to vague principles of international law. *De lege ferenda*, they should also take into account what will be the effect if other countries adopt the same approach;[47] that is the question of scalability.

An illustrative example of the risks associated with ignoring the scalability issue is found in the "rep localisation" requirement found in art. 27 GDPR.[48] Rep localisation requirements mandate that foreign organisation maintain a physical representation in the country imposing the requirement.[49] Thus, organisations cannot access foreign markets without first establishing a physical presence there. This type of requirement has already been adopted into the data privacy laws of countries imitating the GDPR. One example of this is found in the Thai Personal Data Protection Act B.E. 2562 (2019).[50] The obvious question is whether EU-based organisations are going to established representatives in Thailand, and all the other countries that has adopted, and will adopt, rep localisation requirements. I imagine that once every organisation must have a representative in every country in which it has sales, we will see considerable discontent with this unscalable approach.

Where there is a failure to consider scalability, we end up with a widening of the harmful gap between those countries that are dominant in the online environment (typically richer more developed countries) and those that are struggling to reach their potential (typically poorer less developed countries). This is unacceptable.

Elsewhere,[51] I have argued that a scalability assessment is a part of any assessment of proportionality. For clarity and to provide emphasis, I have here rather approached it as a separate matter. The key thing is, of course, to ensure that scalability is considered.

4.8. The many roles of trust

Via the 2019 G20 meeting in Osaka, Japan gained support for the interesting notion of "transborder data flow with trust" earlier articulated at the January 2019 Davos World Economic Forum. In a sense, this concept is uncontroversial. We need transborder data

---

47 Compare to the "global south impact assessment" advocated in D. Svantesson, *Internet & Jurisdiction Global Status Report 2019*, Paris, Internet & Jurisdiction Policy Network 2019, p 64: "it is arguably reasonable to expect lawmakers in those countries that commonly influence policy and law developments globally to conduct what may be termed a 'global south impact assessment', assessing: (1) what impact their approaches will have in the global south, and (2) what will happen if the global south adopts their approaches."

48 For an analysis of art. 27, see further: C. Millard, D. Kamarinou, *Article 27* [in:] *The EU General Data Protection Regulation*, pp. 589–598.

49 See further: D. Svantesson, *Internet & Jurisdiction*…, pp.147–148.

50 Section 37(5).

51 D. Svantesson, "Data localisation trends and challenges: Considerations…, p. 28, http://dx.doi.org/10.1787/7fbaed62-en [accessed: 2021.09.09].

flow, but transborder data flow is only acceptable with trust. In my view, this trust must come in multiple forms. We need to see trust between states. Yet, trust between states is perhaps at a lower level now than it has been for quite some time. We also need trust between states and their citizens. But also this type of trust is low in many countries. In some countries this trust is lacking due to antidemocratic governments. But trust has also decreased in many democratic states as a result of measures imposed due to the pandemic. Furthermore, we need trust between states and companies. Again, this is a form of trust that has decreased over recent years, especially when it comes to the major tech companies. While states used to compete about being the best at accommodating the trendy new tech companies, those same companies are now constantly targeted with criticism. Finally, we need at least one other form of trust; that is, trust between companies and their customers. This form of trust seems to have largely followed the above-mentioned pattern of the trust between trust between states and companies and needs to be restored.

Much work is required to rebuild these forms of trust, and the required work demands a multistakeholder approach. Furthermore, it must be noted that all these forms of trust depend, and must be built on, enforceable legal rights. While many components (business, technical infrastructure etc.) are needed for productive transborder data flow, only adherence to the rule of law in the form of enforceable legal rights can facilitate the trust necessary for the international data transfers on which the world relies today more than ever.

5. Concluding remarks

The regulation of cross-border data flows goes back, at least, to the Swedish Data Act of 1973. Amongst other things, section 11 of that act made clear that:

> If there is reason to assume that personal data will be used for automatic data processing abroad, the data may be disclosed only after permission from the Data Inspection Board [Datainspektionen]. Such permission may be given only if it may be assumed that the disclosure of the data will not involve undue encroachment upon personal privacy.[52]

In other words, this is not a new issue. Yet, while the approach of imposing conditions on international data transfers has long history, the environment in which that approach is being applied has changed dramatically. In this new environment, it is more important than ever that solutions are found that cater for the important forms of international data transfers. As the case law has taught us, such transfers can only

[52] 11 par. Datalag (1973:289) (Swed.). Translation of: "Finns det anledning antaga att personuppgift skall användas för automatisk databehandling i utlandet, får uppgiften lämnas ut endast efter medgivande av Datainspektionen. Sådant medgivande får lämnas endast om det kan antagas att utlämnandet av uppgiften icke kommer att medföra otillbörligt intrång i personlig integritet." The translation was found at http://archive.bild.net/dataprSw.htm (no longer available) and verified by the author.

be accepted where the data subjects are afforded appropriate safeguards, enforceable rights and effective legal remedies.

While speaking of Sweden, I note the Swedish proverb "gör om, gör rätt." ("do it again, do it right"). Perhaps this is rather an apt proverb to guide our future direction in the field of international data transfers.

Literature

Bentzen H., Svantesson D., *Jurisdictional Challenges Related to DNA Data Processing in Transnational Clouds* [in:] *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, eds D. Svantesson, D. Kloza, Cambridge–Antwerpia–Portland 2017.

Bygrave L., *International agreements to protect personal data* [in:] *Global Privacy Protection: The First Generation*, eds J. Rule, G. Greenleaf, Cheltenham 2008, revised in 2017, available at SSRN: *https://ssrn.com/abstract=3072270* [accessed 2021.09.09].

Chander A., *Is Data Localization a Solution for Schrems II?*, "Georgetown Law Faculty Publications and Other Works" 2020, 2300, *https://scholarship.law.georgetown.edu/facpub/2300* [accessed: 2021.09.09].

Chander A., Le U., "Data Nationalism", *Emory Law Journal* 2015, vol. 64/3.

Korff D., "Korff on Kuner: *Schrems II* Re-Examined," 3 September 2020, *https://www.ianbrown.tech/2020/09/03/korff-on-kuner-schrems-ii-re-examined/* [accessed: 2021.09.09].

Kuner Ch., "*Schrems II* Re-Examined", Verfassungsblog.de 25 August 2020, *https://verfassungsblog.de/schrems-ii-re-examined/* [accessed: 2021.09.09].

Kuner Ch., "International Agreements, Data Protection, and EU Fundamental Rights on the International State: Opinion 1/15, EU-Canada PNR", *Common Market Law Review* 2018, no. 55.

Mascalzoni D., Bentzen H. *et al.*, "Are Requirements to Deposit Data in Research Repositories Compatible With the European Union's General Data Protection Regulation?", *Annals of Internal Medicine* 2019, no. 170(5).

Palfrey J., Gasser U., *Interop: The Promise and Perils of Highly Interconnected Systems*, New York 2012.

Polčák R., Svantesson D., *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*, Cheltenham 2017.

Svantesson D., "A 'layered approach' to the extraterritoriality of data privacy laws," *International Data Privacy Law* 2013, no. 3(4).

Svantesson D., "A legal method for solving issues of Internet regulation; applied to the regulation of cross-border privacy issues," *European University Institute Working Paper LAW* 2010, no. 18.

Svantesson D., "Cross-border data transfers after the CJEU's Safe Harbour Decision – A tale of Gordian Knots," *Alternative Law Journal* 2016, no. 41(1).

Svantesson D., "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines," *OECD Digital Economy Papers* 2020, no. 301, Paris, *http://dx.doi.org/10.1787/7fbaed62-en* [accessed: 2021.09.09].

Svantesson D., "The holy trinity of legal fictions undermining the application of law to the global Internet," *International Journal of Law and Information Technology* 2015, vol. 23, no. 3.

Svantesson D., "What is 'Law', if 'the Law' is Not Something That 'Is'? A Modest Contribution to a Major Question", *Ratio Juris* 2013, no. 26(3), p. 456.

Svantesson D., *Solving the Internet Jurisdiction Puzzle*, Oxford 2017.

The EU General Data Protection Regulation (GDPR): A Commentary, eds Ch. Kuner *et al.*, Oxford 2020.

Trans-Atlantic Data Privacy Relations as a Challenge for Democracy, eds D. Svantesson, D. Kloza, Cambridge–Antwerpia–Portland 2017.

Weber R.H., "Legal Interoperability as a Tool for Combating Fragmentation," *Global Commission on Internet Governance Paper Series Centre for International Governance Innovation* 2014, no 4.

Summary

Dan Jerker B. Svantesson

International Data Transfers post *Schrems* – Moving Towards Solutions

International data transfers are both essential for the modern world and a major source of risks to the protection of personal data. In this, we can speak of a clash between an important multi-faceted objective and the protection of a complex fundamental human right with implications going far beyond that right itself.

The goal must be to facilitate data privacy respecting international data transfers. However, agreement on this goal – even if widespread – does not necessarily signal agreement on how we reach that goal. To make progress, we must proceed with caution and yet avoid getting bogged down in the unavoidable challenges, such as definitional challenges, we will face.

This article canvasses a selection of key considerations that ought to be kept in mind when we discuss approaches to international data transfers. However, to prepare ground for that discussion, it first sets the scene by examining the so-called Schrems II decision, its larger context and background, as well as some of the reactions we have seen to that decision.

Keywords: transfer of data to third country; adequacy; standard contractual clauses; GDPR.

Streszczenie

Dan Jerker B. Svantesson

Międzynarodowy transfer danych po sprawach Schremsa – ku rozwiązaniom

Ponadgraniczny transfer danych jest niezbędny współczesnemu światu, stanowiąc jednocześnie znaczące źródło zagrożeń dla ochrony danych osobowych. W tym kontekście możemy mówić o konflikcie pomiędzy ważnym, wieloaspektowym zadaniem do zrealizowania a ochroną złożonego, podstawowego prawa człowieka, którego skutki wykraczają daleko poza samo prawo.

Celem musi być ułatwienie ochrony prywatności danych przy poszanowaniu potrzeby ponadgranicznego przekazywania danych. Jednak zgoda co do określenia celu – nawet jeśli powszechna – niekoniecznie oznacza porozumienie co do sposobu jego osiągnięcia. Aby poczynić postępy, musimy postępować ostrożnie, a jednocześnie unikać ugrzęźnięcia w gąszczu nieuniknionych wyzwań, z którymi przyjdzie nam się zmierzyć, takich jak choćby wyzwania terminologiczne.

W niniejszym artykule przedstawiono wybrane kluczowe kwestie, o których należy pamiętać, gdy dyskutujemy o naszym podejściu do ponadgranicznego przekazywania danych. Nim ta dyskusja się rozwinie, należy przygotować do niej grunt scenę poprzez zbadanie tzw. orzeczenia *Schrems II*, jego szerszego kontekstu, tła, a także niektórych reakcji, z jakimi mieliśmy do czynienia w związku z tym orzeczeniem.

Słowa kluczowe: transfer danych do państw trzecich; adekwatność; standardowe klauzule umowne; RODO.

Agnieszka Grzelak
Akademia Leona Koźmińskiego
agrzelak@alk.edu.pl
ORCID: 0000-0002-5867-8135

https://doi.org/10.26881/gsp.2021.4.03

Przyszłość współpracy UE z państwami trzecimi w sprawie przekazywania danych pasażerów lotniczych. O skutkach opinii Trybunału Sprawiedliwości nr 1/15 dla wymiany danych PNR

1. Wprowadzenie

Problematyka przetwarzania danych PNR (*Passenger Name Record*) jest przedmiotem badań naukowych i praktyki od lat. Instrumenty PNR są bowiem doskonałym przykładem dychotomii między prywatnością a bezpieczeństwem publicznym[1]. Jest to również atrakcyjny instrument zwalczania terroryzmu i poważnej przestępczości, stąd też nie dziwi, że zawarciem umów pozwalających na przetwarzanie danych jest zainteresowanych szereg państw, a prace nad wypracowaniem standardów prowadzą organizacje międzynarodowe[2].

Dane PNR to zbiór danych o podróży każdego pasażera linii lotniczych, który zawiera informacje niezbędne, aby umożliwić przetwarzanie i weryfikowanie rezerwacji przez przewoźników lotniczych obsługujących lot w odniesieniu do każdego przelotu zarezerwowanego przez jakąkolwiek osobę lub w jej imieniu. Dane te są przekazywane przez pasażerów przewoźnikom lotniczym podczas dokonywania rezerwacji na lot[3]. Dane PNR należy przy tym odróżnić od tzw. danych API (*Advance Passenger*

[1] H. Hijmans, *PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators*, „European Data Protection Law Review" 2017, nr 3, s. 406.

[2] Poza UE należy do nich chociażby International Civil Aviation Organisation ICAO, która już w 2010 r. przyjęła wytyczne: Guidelines on Passenger Name Record (PNR) Data, doc. 9944 https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_en.pdf [dostęp: 25.11.2021]. Od marca 2019 r. trwają prace nad nowym dokumentem ICAO. Również Rada Bezpieczeństwa ONZ w 2017 r. uchwalił rezolucję, która zobowiązuje państwa do rozwoju systemu przetwarzania danych PNR: United Nations Security Council Resolution 2396 (2017).

[3] Zob. m.in. definicję danych PNR zawartą w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz. Urz. UE L 119, s. 132).

Information), czyli danych biograficznych pobranych z części paszportu możliwej do automatycznego odczytu, która obejmuje imię i nazwisko, miejsce zamieszkania, miejsce urodzenia i obywatelstwo osoby. Wykorzystanie danych PNR znacząco różni się od sposobu wykorzystywania danych API – dane PNR są raczej narzędziem służącym walce z przestępczością, a nie weryfikacji tożsamości w związku z przekroczeniem granicy. Dane PNR służą do oceny ryzyka związanego z przelotem pasażera, czy też do identyfikacji osób, które mogą być podmiotem zainteresowania organów ścigania, a także osób powiązanych z osobą podejrzewaną o popełnienie przestępstwa[4].

W ostatnim dziesięcioleciu na forum UE podjęto działania zmierzające po pierwsze, do uregulowania zasad przekazywania danych PNR z UE do państw trzecich, jak również do stworzenia wewnątrzunijnej regulacji dotyczącej PNR. Jednocześnie bardzo w tych latach wzmocnił się poziom ochrony prawa do prywatności i prawa do ochrony danych osobowych, co bez wątpienia miało wpływ nie tylko na działania Komisji Europejskiej, ale przede wszystkim znalazło swój wyraz w orzeczeniach Trybunału Sprawiedliwości (TS, Trybunał)[5]. Wejście w życie Traktatu z Lizbony nie tylko wiązało się z przyznaniem mocy prawnej równej traktatom: Karcie Praw Podstawowych UE (KPP), wprowadzeniu do Traktatu o funkcjonowaniu Unii Europejskiej nowego art. 16 TFUE[6], ale także oznaczało zmianę procedury zawierania umów międzynarodowych tego typu (konieczność uzyskania zgody Parlamentu Europejskiego)[7]. Przypomnienie tych

[4] Ciekawego podsumowania definicji i znaczenia danych PNR dokonuje T. Maruhashi, *Japan-EU Passenger Name Record Negotiations and Their Implications* [w:] *Human-Centric Computing in a Data-Driven Society. 14th IFIP TC 9 International Conference on Human Choice and Computers*, red. D. Kreps, T. Komukai, T.V. Gopal, K. Ishii, HCC14 2020, Tokyo, Japan, September 9–11, 2020, Proceedings, Springer 2020, s. 100 i n.

[5] Wystarczy tu wspomnieć o tych orzeczeniach, które będą punktem wyjścia dla TS w sprawie opinii 1/15: wyrok Trybunału (wielka izba) z dnia 8 kwietnia 2014 r. w sprawach połączonych C-293/12 i C-594/12 *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in.* oraz *Kärntner Landesregierung i in.*, ECLI:EU:C:2014:238; dalej: wyrok w sprawie DRI; wyrok Trybunału (wielka izba) z dnia 6 października 2015 r. w sprawie C-362/14 *Maximillian Schrems przeciwko Data Protection Commissioner*; dalej: wyrok w sprawie Schrems I, ECLI:EU:C:2015:650 czy wyrok TS z dnia 21 grudnia 2016 r. w sprawach połączonych C-203/15 i C-698/15, *Tele2 Sverige AB przeciwko Post- och telestyrelsen* oraz *Secretary of State for the Home Department przeciwko Tomowi Watsonowi, Peterowi Brice'owi, Geoffrey'owi Lewisowi*, EU:C:2016:970 Nie można jednak zapominać o najnowszych orzeczeniach z dnia 6 października 2020 r. w sprawach C-623/17, *Privacy International przeciwko Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*, EU:C:2020:790, dalej: wyrok C-623/17, *Privacy International*; wyrok TS z dnia 6 października 2020 r., sprawy połączone C-511/18, C-512/18 i C-520/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net przeciwko Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées oraz Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX przeciwko Conseil des ministres*, EU:C:2020:791; dalej: wyrok w sprawach połączonych C-511/18, C-512/18 i C-520/18, *La Quadrature du Net*.

[6] Na ten temat szerzej A. Grzelak, *Prawo do ochrony danych osobowych a konieczność walki z przestępczością. Uwagi na tle art. 16 traktatu o funkcjonowaniu Unii Europejskiej* [w:] *Prawo Unii Europejskiej a prawo konstytucyjne państw członkowskich*, red. S. Dudzik, N. Półtorak, Warszawa 2013, s. 407–434.

[7] Por. obecny art. 218 ust. 6 TFUE.

działań będzie przedmiotem pierwszego fragmentu niniejszego artykułu. Przyjmowanie kolejnych aktów prawnych wiązało się jednak z szeregiem wątpliwości i zastrzeżeń dotyczących poziomu ochrony praw podstawowych, w szczególności prawa do prywatności i prawa do ochrony danych osobowych. Zasadnicze uwagi zgłaszane były przez Europejskiego Inspektora Ochrony Danych (EDPS) czy też przez organizacje pozarządowe. Szereg z tych problemów stało się przedmiotem analizy Trybunału Sprawiedliwości w jednym z najważniejszych orzeczeń z tej dziedziny w ostatnich latach, a mianowicie w opinii 1/15 dotyczącej projektowanej umowy w sprawie przekazywania danych PNR, która miała być zawarta z Kanadą[8]. Te problemy będą przedmiotem analizy w następnej części opracowania, a opinia 1/15 powinna stać się kluczowym punktem odniesienia dla wszelkich dalszych analiz. Podstawowym jednak zagadnieniem, które jest przedmiotem niniejszego tekstu będzie próba odpowiedzi na pytanie o znaczenie opinii 1/15 dla dalszych prac nad systemem PNR i przyszłość współpracy z państwami trzecimi w tym obszarze, ale także jej znaczenie dla całego systemu ochrony danych osobowych w Unii Europejskiej.

2. Ewolucja prac nad systemem PNR w kontekście zewnętrznym i wewnętrznym w Unii Europejskiej – krótkie przypomnienie

Zanim przedstawione zostaną podstawowe problemy związane z uregulowaniem zasad przekazywania danych PNR do państw trzecich, określone w orzecznictwie Trybunału, warto krótko uporządkować ewolucję prac nad systemem PNR zarówno w kontekście zewnętrznym (negocjacji z państwami trzecimi), jak i wewnętrznym (stworzeniem systemu EU-PNR).

Komisja Europejska rozpoczęła prace nad uregulowaniem zasad gromadzenia danych PNR przez przewoźników i przekazywania ich właściwym organom odpowiedzialnym za zwalczanie przestępczości, wnosząc w roku 2003[9] o ustanowienie bezpiecznych pod względem prawnym ram dla przekazywania PNR do Departamentu Bezpieczeństwa Wewnętrznego USA (*Department of Homeland Security* – DHS) oraz do przyjęcia wewnętrznej polityki w zakresie PNR. Konieczność podjęcia działań w tym zakresie była związana z polityką wewnętrzną USA, gdzie krótko po wydarzeniach z 11 września 2001 r. wprowadzono regulacje zobowiązujące przewoźników lotniczych (w tym unijnych) do przekazywania danych władzom amerykańskim[10]. Pracom nad umową z USA towarzyszyły zastrzeżenia Parlamentu Europejskiego (PE) i Grupy Roboczej Art. 29, która wnosiła o zapewnienie adekwatnego poziomu ochrony w USA[11].

[8] Opinia Tybunału (wielka izba) 1/15 z dnia 26 lipca 2017 r., ECLI:EU:C:2017:592; dalej: opinia 1/15.

[9] Komunikat do Rady i Parlamentu w sprawie przekazywania danych dotyczących przelotu pasażera (PNR): globalne podejście UE, COM(2003) 826.

[10] P.M. Schwartz, *The EU-US Privacy Collission: A Turn to Institutions and Procedures*, Harvard Law Review 2013, s. 1973–1979.

[11] Negocjacje rozpoczęte z USA zakończyły się zawarciem umowy przez Radę pomimo tego, że Parlament Europejski chciał opinii TS dotyczącej podstawy prawnej porozumienia. Ostatecznie jednak

Odpowiednie skargi trafiły do Trybunału Sprawiedliwości i w 2006 r. TS unieważnił decyzję Rady dotyczącą zawarcia umowy oraz decyzję Komisji o adekwatnym poziomie ochrony[12], przy czym powodem nie były kwestie merytoryczne (TS nie dokonywał analizy), lecz wybór niewłaściwej podstawy prawnej. Dalsze negocjacje doprowadziły do podpisania przez UE umowy ze Stanami Zjednoczonymi Ameryki o przekazywaniu danych PNR w interesie walki z terroryzmem i poważną przestępczością transgraniczną, która to umowa zapewnia przekazywanie danych PNR, przy jednoczesnej ochronie danych osobowych[13]. W tym okresie podpisane zostały również umowy z Kanadą i Australią (które ostatecznie były stosowane tymczasowo)[14].

Kolejny komunikat dotyczący globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim Komisja przedstawiła w 2010 r.[15], proponując dalsze działania w odpowiedzi na ataki terrorystyczne w Stanach Zjednoczonych, w Madrycie i Londynie, a także w związku z potrzebą wzmocnienia poszanowania praw podstawowych. Komisja zaprezentowała w nim globalne podejście do transferów danych PNR do państw trzecich, ustanawiając zestaw kryteriów, które muszą być spełnione odnośnie do zasad i gwarancji bezpieczeństwa danych. W efekcie, w wymiarze zewnętrznym obecnie stan umów i etapy negocjacyjne prezentują się następująco[16]:

---

wycofał swój wniosek o zbadanie treści umowy, a zamiast tego wniósł o stwierdzenie nieważności decyzji Rady o zawarciu umowy. Na ten temat szerzej: E. Guild, E. Brouwer, *The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief July 2006, nr 109 oraz M. Mendez, *Passenger Name Record Agreement*, European „Constitutional Law Review" 2007, vol. 3, nr 1, s. 127, a także V. Papakonstantinou, P. de Hert, *The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic*, „Common Market Law Review" 2009, s. 885.

[12] Wyrok Trybunału (wielka izba) z dnia 30 maja 2006 r. w połączonych sprawach Parlament Europejski przeciwko Radzie Unii Europejskiej (C-317/04) i Komisji Wspólnot Europejskich (C-318/04), Zb. Orz. 2006, I-04721, ECLI:EU:C:2006:346. Trybunał Sprawiedliwości uniknął odpowiedzi na pytania co do zgodności umowy z zasadami ochrony danych osobowych, stwierdzając jedynie, że nieprawidłowo wskazano podstawę prawną decyzji Rady, co w efekcie naruszało uprawnienia Parlamentu. Co zaskakujące, w opinii rzecznika generalnego porozumienie zostało uznane za zgodne ze standardem wynikającym z art. 8 EKPC. Zob. opinię z 22.11.2005 r., ECLI:EU:C:2005:710.

[13] Decyzja Rady 2007/551/WPZiB/WSiSW z dnia 23 lipca 2007 r. w sprawie podpisania, w imieniu Unii Europejskiej, Umowy między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (DHS) (Umowa PNR z 2007 r.) oraz Umowa między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (DHS) (Umowa PNR z 2007 r.), Dz. Urz. L 204, s. 16 i s. 18.

[14] Dz. Urz. UE L 91 z 2006 r., s. 53, s. 49; Dz. Urz. UE L 82 z 2006 r., s. 15 oraz Dz. Urz. UE L 213 z 2008 r., s. 49.

[15] Zob. komunikat Komisji z 21.09.2010 r. w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, COM(2010) 492 final.

[16] Stan na dzień: 18.06.2021 r.

Tab. 1. Umowy zawarte między UE a państwami trzecimi – obowiązujące

Państwo	Data podpisania umowy	Data wejścia w życie	Dodatkowe raporty lub informacje
Australia[17]	29 września 2011 r.	1 czerwca 2012 r.	sprawozdanie z 2014 r.[18] sprawozdanie z 2021 r.[19]
USA	14 grudnia 2011 r.[20]	1 lipca 2012 r.	sprawozdanie z 2017 r.[21] sprawozdanie z 2021 r.[22]

Źródło: Opracowanie własne.

Tab. 2. Trwające negocjacje

Państwo	Data rozpoczęcia negocjacji	Aktualna sytuacja
Kanada	25 czerwca 2014 r. – podpisanie umowy	w świetle opinii TSUE 1/15 umowa w tej formie nie może być zawarta
	czerwiec 2018 r.	rozpoczęcie negocjacji nad nową umową
Meksyk	2015 r.[23]	negocjacje zawieszone
Japonia	18 lutego 2020 r.	decyzja Rady o rozpoczęciu negocjacji[24]

Źródło: Opracowanie własne.

[17] Umowa między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej i granicznej danych dotyczących przelotu pasażera (danych PNR) (Dz. Urz. UE L 186 z 2012 r., s. 4.).

[18] Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie wspólnego przeglądu realizacji Umowy między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej i granicznej danych dotyczących przelotu pasażera (danych PNR), COM(2014) 458 final.

[19] Report from the Commission to the European Parliament and the Council: On the joint review of the implementation of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, COM(2021) 19 final.

[20] Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (Dz. Urz. UE L 215 z 2012 r., s. 5).

[21] Report from the Commission to the European Parliament and the Council: On the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security COM(2017) 29 final.

[22] Report from the Commission to the European Parliament and the Council on the joint evaluation of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, COM(2021) 18 final.

[23] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_15_5374 [dostęp: 25.11.2021].

[24] https://www.consilium.europa.eu/pl/press/press-releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations/ [dostęp: 25.11.2021].

Równolegle rozpoczęto prace nad stworzeniem europejskiego systemu przekazywania danych PNR (tzw. EU-PNR), najpierw przedstawiając projekt decyzji ramowej Rady[25], a następnie – w związku z wejściem w życie Traktatu z Lizbony – projekt dyrektywy, nad którą prace zakończyły się w 2016 r. przyjęciem dyrektywy 2016/681 (dyrektywa EU-PNR)[26]. Dyrektywę przyjęto, chociaż opinia Europejskiego Inspektora Ochrony Danych (EDPS) była w tym zakresie negatywna – w jego ocenie zachodziła sprzeczność proponowanych przepisów ze standardem wynikającym z Karty Praw Praw Podstawowych (KPP, Karta)[27]. Dyrektywa definiuje zadania państw członkowskich w zakresie przetwarzania danych PNR, wymagając od nich m.in. ustanowienia jednostek odpowiedzialnych za zbieranie, przechowywanie i przetwarzanie danych (tzw. jednostki PIU – *passenger information units*) oraz do przyjęcia listy organów właściwych do wnioskowania o dostęp i otrzymywania danych PNR. Zasady określone w dyrektywie stosuje się w odniesieniu do lotów z państw trzecich do UE, jednak państwa członkowskie UE mogą podjąć decyzję o zastosowaniu ich również w odniesieniu do lotów wewnątrzunijnych[28]. W dniu 24 lipca 2020 r. Komisja przestawiła Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące przeglądu dyrektywy 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania[29]. Ogólna ocena dotycząca pierwszych miesięcy stosowania przepisów jest pozytywna, działania państw w kierunku jej implementacji ogólnie zadowalajace, a dyrektywa nie wymaga na tym etapie żadnych zmian. Tymczasem ocena poszczególnych rozwiązań i sposobu ich wdrożenia do prawa krajowego przez badaczy do takich entuzjastycznych wniosków już nie prowadzi, o czym jeszcze będzie mowa w dalszej części tekstu.

Wydanie przez Trybunał Sprawiedliwości wspomnianej we wprowadzeniu do niniejszego tekstu opinii 1/15, która będzie jeszcze przedmiotem analizy w dalszej części, zdecydowanie przyhamowało proces negocjowania i zawierania umów z państwami trzecimi i wymusiło na Komisji konieczność przedstawienia nowego podejścia i dostosowania się do wymogów wynikających z orzecznictwa. Komisja w dniu

[25] W 2007 r. Komisja przedstawiła wniosek dotyczący projektu decyzji ramowej regulującej omawiane zagadnienia, COM(2007) 654 final.

[26] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz. Urz. UE L 119, s. 132; dalej: dyrektywa EU-PNR albo dyrektywa 2016/681).

[27] Opinia EDPS 5/2015 z dnia 24 września 2015 r., https://edps.europa.eu/sites/default/files/publication/15-09-24_pnr_en.pdf [dostęp: 25.11.2021].

[28] Zob. zaktualizowaną listę państw członkowskich, które podjęły decyzję o stosowaniu dyrektywy w sprawie wykorzystywania danych PNR do lotów wewnątrzunijnych zgodnie z art. 2 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz. Urz. UE C 358 z 2020 r., s. 7). Na tej liście znajduje się Polska.

[29] COM(2020) 305 final.

24 lipca 2020 r. opublikowała zatem tzw. mapę drogową[30], w której podsumowała rozwój sytuacji dotyczącej stosowania danych PNR na świecie od 2010 r., a także dokonała próby określenia polityki dotyczącej przekazywania danych PNR państwom spoza UE. Podstawowym problemem, jaki zarysował się w ostatnim dziesięcioleciu były bowiem różnice w standardzie ochrony danych osobowych i prywatności pomiędzy Unią Europejską (zwłaszcza w związku z reformą dokonaną w 2016 r.) a państwami trzecimi[31].

3. Prace nad umową z Kanadą i wniosek Parlamentu Europejskiego do TSUE

Pierwsza umowa z Kanadą została zawarta już w 2005 r. pomimo tego, że już na tym etapie pojawiały się wątpliwości dotyczące standardu ochrony prawa do prywatności i danych osobowych[32]. W dniu 18 lipca 2005 r. Rada przyjęła decyzję 2006/230/WE w sprawie zawarcia umowy pomiędzy Wspólnotą Europejską a rządem Kanady o przetwarzaniu danych API/PNR[33], którą zatwierdziła tę umowę. Zgodnie z preambułą, została ona zawarta z uwzględnieniem wymogu rządu Kanady, który to wymóg dotyczył przekazywania przez przewoźników lotniczych właściwym władzom Kanady informacji o pasażerach oraz zapisu danych dotyczących nazwiska pasażera (danych „API/PNR") w zakresie, w jakim są one zbierane i zawarte w automatycznych systemach rezerwacji oraz odprawy, należących do przewoźników. Celem tej umowy było zapewnienie, by dane API/PNR były przekazywane przy pełnym poszanowaniu podstawowych praw i wolności, w szczególności prawa do prywatności.

W dniu 6 września 2005 r. Komisja przyjęła decyzję 2006/253/WE w sprawie odpowiedniej ochrony danych osobowych zawartych w Imiennym Rejestrze Pasażerów linii lotniczych, przekazanym do Agencji Służb Granicznych Kanady (CBSA)[34]. Zgodnie z tą decyzją, CBSA miała zapewnić odpowiedni poziom ochrony danych PNR przekazywanych z Unii Europejskiej w związku z lotami do Kanady, zgodnie wymogami określonymi w załączniku do decyzji. Decyzja ta miała obowiązywać przez trzy lata i sześć miesięcy od daty podania jej do wiadomości – przy czym do przedłużenia obowiązywania

30 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12531-External-dimension-of-the-EU-policy-on-Passenger-Name-Records-_pl [dostęp: 14.06.2021].

31 Zob. w szczególności wyrok Trybunału Sprawiedliwości w sprawie *Schrems II*: wyrok z 16.07.2020 w sprawie C-311/18 *Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillianowi Schremsowi*, ECLI:EU:C:2020:559.

32 Na jej temat zob. bardzo szeroko P. Hobbing, *Tracing Terrorists: The EU-Canada Agreement in PNR Matters* CEPS Special Report, September 2008 Revised version 17.11.2008, http://aei.pitt.edu/11745/1/1704.pdf [dostęp: 18.06.2021]. Zob. również opinię Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego decyzji Rady w sprawie zawarcia porozumienia pomiędzy Wspólnotą Europejską a Rządem Kanady w sprawie przetwarzania zaawansowanych informacji na temat pasażerów (API) oraz danych dotyczących nazwy rekordu pasażera (PNR) (COM(2005) 200 wersja ostateczna), Dz. Urz. UE C 218 z 2005 r., s. 6.

33 Dz. Urz. UE L 82 z 2006 r., s. 14.

34 Dz. Urz. UE L 91 z 2006 r., s. 49.

tej decyzji nie doszło. Okres obowiązywania umowy z 2006 r. był zgodnie z art. 5 ust. 1 i ust. 2 związany był z okresem obowiązywania decyzji 2006/253, a zatem termin obowiązywania tej umowy upłynął we wrześniu 2009 r. i pojawiła się potrzeba rozpoczęcia rozmów na temat nowej umowy.

W dniu 5 maja 2010 r. Parlament Europejski przyjął rezolucję dotyczącą rozpoczęcia negocjacji w sprawie umów dotyczących rejestru nazwisk pasażerów (PNR) ze Stanami Zjednoczonymi, Australią i Kanadą[35], zaś pół roku później Rada przyjęła decyzję upoważniającą Komisję do rozpoczęcia w imieniu Unii negocjacji z Kanadą w sprawie umowy o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera w celu zapobiegania terroryzmowi i innych poważnych przestępstw międzynarodowych oraz ich zwalczania, a także wytyczne negocjacyjne w tej sprawie. Umowa została parafowana w dniu 6 maja 2013 r. W dniu 5 grudnia 2013 r. Rada przyjęła decyzję w sprawie podpisania umowy między Kanadą a Unią Europejską o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera. Przewidywana umowa została podpisana w dniu 25 czerwca 2014 r., a kilka dni później Rada zwróciła się do PE o wyrażenie zgody na projekt decyzji Rady w sprawie zawarcia przewidywanej umowy.

W dniu 25 listopada 2014 r. Parlament Europejski przyjął rezolucję w sprawie zasięgnięcia opinii Trybunału Sprawiedliwości na temat zgodności z traktatami umowy między Kanadą a Unią Europejską w sprawie przekazywania i przetwarzania danych dotyczących przelotu pasażera[36]. Wniosek PE o wydanie opinii dotyczył zarówno zgodności przewidywanej umowy z prawem pierwotnym Unii, jak i właściwej podstawy prawnej decyzji Rady dotyczącej zawarcia przewidywanej umowy i miał następujące brzmienie:

„Czy projekt przewidywanej umowy jest zgodny z postanowieniami traktatów (art. 16 TFUE) i Kartą praw podstawowych Unii Europejskiej (art. 7, 8 i art. 52 ust. 1) w zakresie prawa osób fizycznych do ochrony danych osobowych?

Czy art. 82 ust. 1 lit. d) oraz art. 87 ust. 2 lit. a) TFUE stanowią właściwą podstawę prawną aktu Rady dotyczącego zawarcia przewidywanej umowy, czy też akt ten należy oprzeć na podstawie prawnej z art. 16 TFUE?".

W ten sposób, na podstawie art. 218 ust. 11 TFUE, umowa z Kanadą trafiła do Trybunału Sprawiedliwości, który miał wypowiedzieć się na temat jej zgodności z przepisami TFUE i KPP UE. Zanim zapadł wyrok, opinię w tej sprawie przedstawił rzecznik generalny Paolo Mengozzi, który zaproponował, by Trybunał uznał część przepisów umowy za niezgodne z art. 7, 8 i 52 ust. 1 KPP ze względu na wykroczenie poza to, co ściśle konieczne, brak precyzji, naruszenie zasady celowości i zbyt długi okres retencji danych[37].

---

[35] Dz. Urz. UE C 81 z 2011 r., s. 70.

[36] Dz. Urz. UE C 289 z 2016 r., s. 2.

[37] Opinia rzecznika generalnego P. Mengozziego przedstawiona 8.09.2016 r. w sprawie 1/15, EU:C:2016:656.

4. Opinia 1/15 Trybunału Sprawiedliwości

Trybunał Sprawiedliwości swoją opinię przedstawił 26 lipca 2017 r. W pierwszej kolejności Trybunał Sprawiedliwości zajął się problemem właściwej podstawy prawnej dla zawarcia umowy, a konkretniej pominięciem art. 16 ust. 2 TFUE. Trybunał przypomniał zasadnicze wymogi: wybór podstawy prawnej aktu UE, w tym aktu przyjętego w celu zawarcia umowy międzynarodowej, musi opierać się na obiektywnych czynnikach, które mogą zostać poddane kontroli sądowej, a do których należą w szczególności cel i treść tego aktu[38]. Oceniając cel i treść porozumienia, Trybunał – podobnie jak uczynił to rzecznik generalny P. Mengozzi w swojej opinii – doszedł do wniosku, że umowa zawiera dwa elementy składowe – pierwszy dotyczy konieczności zapewnienia bezpieczeństwa publicznego, a drugi – ochrony danych PNR. Tym samym, decyzja Rady w sprawie zawarcia umowy powinna opierać się zarówno na art. 16 ust. 2 TFUE, jak i na art. 87 ust. 2 lit. a TFUE, o ile procedura wynikająca z obu podstaw jest zgodna[39]. W tym konkretnym przypadku decyzja Rady w sprawie zawarcia przewidywanej umowy powinna – w ocenie Trybunału – opierać się łącznie na art. 16 ust. 2 TFUE i na art. 87 ust. 2 lit. a TFUE[40]. Przypomnieć przy tym należy, że wybór właściwej podstawy prawnej ma znaczenie konstytucyjne, ponieważ posiadając tylko kompetencje powierzone, UE musi powiązać przyjmowane akty z postanowieniem traktatu, które ją do tego przyjęcia skutecznie upoważniają, a zastosowanie błędnej podstawy prawnej może przesądzić o nieważności samego aktu zawarcia, a tym samym – o wadliwości zgody UE na związanie umową, którą podpisała. W tym konkretnym przypadku przywołanie właściwej podstawy prawnej nie miało znaczenia dla wyboru właściwej procedury – we wszystkich przypadkach zastosowanie znajduje zwykła procedura prawodawcza, natomiast wskazanie art. 16 ust. 2 TFUE jako podstawy powinno mieć znaczenie dla oceny celu umowy i jej priorytetów. Przyznanie pierwszeństwa podstawom z tytułu V części III TFUE wskazywałoby na przyznanie przewagi walorowi bezpieczeństwa, co mogłoby też rzutować na sposób interpretacji przepisów umowy[41]. Dobrze zatem, że Trybunał wyjaśnił tę kwestię w swojej opinii.

O wiele istotniejsze dla przyszłych porozumień i dla prawa ochrony danych osobowych w UE są te rozważania, w których Trybunał dokonał szczegółowej analizy umowy, zakończonej wnioskiem o jej niezgodności z art. 7, art. 8[42], art. 21 i art. 52 ust. 1

---

38 Opinia 1/2015, pkt 76. Zob. wyroki: z dnia 6 maja 2014 r., Komisja/Parlament i Rada, C-43/12, EU:C:2014:298, pkt 29; a także z dnia 14 czerwca 2016 r., Parlament/Rada, C-263/14, EU:C:2016:435, pkt 43 i przytoczone tam orzecznictwo.

39 Wyrok z dnia 6 listopada 2008 r. Parlament/Rada, C-155/07, EU:C:2008:605, pkt 37 i przytoczone tam orzecznictwo.

40 Pkt 105–118 opinii 1/15.

41 Autorka pisała o tych dylematach w kontekście RODO. Zob. A. Grzelak, *Główne cele ogólnego rozporządzenia o ochronie danych* [w:] M. Kawecki, T. Osiej, *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, Warszawa 2017, s. 11–25.

42 Należy przy tym zauważyć, że Trybunał ograniczył się wyłącznie do analizy art. 8 KPP, pomijając szczegółową analizę art. 16 ust. 1 TFUE i wskazując, że art. 8 KPP określa jednak bardziej szczegółowe wymagania, od jakich zależy dopuszczalność przetwarzania danych osobowych.

Karty Praw Podstawowych w zakresie, w jakim nie wyklucza przekazywania z Unii Europejskiej do Kanady danych szczególnie chronionych oraz wykorzystywania i zatrzymywania tych danych. Co do zasady Trybunał uznał, że przekazanie i przetwarzanie danych PNR, dotyczących zidentyfikowanych osób, narusza prawo podstawowe do ochrony prywatności (art. 7 KPP) oraz prawo do ochrony danych osobowych (art. 8 KPP). Istotą analizy jest jednak uzasadnienie tego naruszenia, w kontekście wymogów określonych w art. 8 ust. 2 oraz art. 52 ust. 1 KPP. Jednocześnie, w związku z tym, że celem umowy jest zapewnienie bezpieczeństwa publicznego poprzez przekazywanie danych PNR do Kanady i wykorzystywanie ich w ramach zwalczania przestępstw terrorystycznych i innych poważnych przestępstw, zatem ingerencja może być uzasadniona celem ogólnym UE. Ochrona bezpieczeństwa publicznego przyczynia się przecież do ochrony praw i wolności innych osób, a art. 6 KPP gwarantuje każdemu prawo nie tylko do wolności, ale też bezpieczeństwa osobistego[43]. Takie stwierdzenie Trybunału nie jest zaskakujące – było to już bowiem przedmiotem szerszych analiz, chociażby we wspomnianej wcześniej sprawie DRI.

Podstawowym problemem, jaki doprowadził do uznania niezgodności umowy z przepisami Karty było niespełnienie wymogu „konieczności" związanego z tym, że naruszenie musi być ograniczone wyłącznie do tego, co jest ściśle niezbędne. Trybunał zidentyfikował przy tym szereg problemów.

Po pierwsze, Trybunał stwierdził, że dane PNR, które miały być przekazywane, nie są wystarczająco jasno i precyzyjnie zdefiniowane. O ile 19 rubryk danych PNR, figurujących w załączniku do umowy, odpowiada zasadniczo wymogom wytycznych Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO), o tyle należy podkreślić, że są też takie, które wzbudzają wątpliwości. Wśród nich TSUE wskazał na „dostępne informacje dotyczące programów dla stałych klientów (*frequent flier*) i dotyczące korzyści (darmowe bilety, zamiana klasy biletu na wyższą itd.)" oraz „wszelkie dostępne informacje kontaktowe (w tym informacje na temat jednostki, która utworzyła dane)", bowiem one nie określają w sposób wystarczająco jasny i precyzyjny danych PNR podlegających przekazaniu[44]. W tym przypadku Trybunał uznał, że użyte sformułowania nie wyznaczają w sposób wystarczający zakresu danych podlegających przekazaniu. Warto przy tym nadmienić, że podobne sformułowania użyte w innych przypadkach (np. „wszelkie dostępne informacje o płatnościach") już takich zastrzeżeń nie budziły, bowiem ich interpretacja spełniała wymogi jasności i precyzji. Za nieprecyzyjne uznano też „uwagi ogólne, w tym inne informacje dodatkowe (OSI), informacje o usługach specjalnych (SSI) i o prośbach o usługi specjalne (SSR)". Przy tym te dane uznane zostały za potencjalnie ujawniające dane sensytywne, które mogłyby być przetwarzane w sposób sprzeczny z art. 21 KPP (zakaz dyskryminacji), a tym samym legalność ich przetwarzania wymagałaby precyzyjnego i szczególnie solidnego uzasadnienia,

[43] Pkt 148–151 opinii 1/15.
[44] Pkt 156 opinii 1/15.

opartego na przesłankach innych niż ochrona porządku publicznego, czego w tym przypadku zabrakło[45].

Po drugie, TS przyjrzał się kwestii zautomatyzowanego przetwarzania danych PNR. Dane PNR przekazywane do Kanady powinny być zasadniczo analizowane w sposób zautomatyzowany, a tymczasem ocena ryzyka stwarzanego przez pasażerów lotniczych dla bezpieczeństwa ruchu lotniczego jest przeprowadzana przed przybyciem pasażerów do Kanady, co naturalnie może być obarczone błędem. Zatem każdy wynik pozytywny powinien być poddany indywidualnej ocenie przeprowadzanej w sposób niezautomatyzowany[46].

Trzeci analizowany problem dotyczył celów przetwarzania danych. Zdefiniowanie pojęć „przestępstwo terrorystyczne" czy „poważne przestępstwo międzynarodowe" uznane zostało przez TS za wystarczające[47]. Trybunał uznał jednak, że umożliwienie przetwarzania danych „w poszczególnych przypadkach" w celach, odpowiednio, „zapewnienia nadzoru nad administracją publiczną lub jej odpowiedzialności" oraz „dostosowania się do wydanego wezwania do stawiennictwa w sądzie lub też nakazu lub zarządzenia wydanego przez sąd" nie spełnia wymogów jasności i precyzji[48].

Czwarty problem dostrzeżony przez Trybunał dotyczył zatrzymania i wykorzystywania danych PNR. Trybunał przypomniał warunki, na jakich organy kanadyjskie mogą mieć dostęp do danych i je zatrzymywać, podkreślając, że uregulowania muszą spełniać obiektywne kryteria ustanawiające związek między danymi osobowymi podlegającymi zatrzymaniu a zamierzonym celem[49]. Cele te umowa określa w art. 3, a Trybunał przeanalizował je w kontekście różnych momentów przetwarzania danych. Uznał, że w przypadku zatrzymywania danych PNR i ich wykorzystywania do chwili opuszczenia Kanady przez pasażerów lotniczych oraz podczas pobytu pasażerów lotniczych w Kanadzie, zatrzymanie i wykorzystanie danych może być uzasadnione i nie wykracza poza granice tego, co ściśle konieczne, bowiem może pojawić się konieczność wykorzystania danych w celu zwalczania terroryzmu i poważnych przestępstw międzynarodowych. Jednak w przypadku danych wpuszczonych już do Kanady, przetwarzanie danych PNR powinno opierać się na innych okolicznościach uzasadniających ich wykorzystanie, przy czym oczywiście potrzeba zwalczania terroryzmu i poważnych przestępstw może to uzasadniać. W takich przypadkach jednak co do zasady przetwarzanie danych powinno być uzależnione od uprzedniej kontroli dokonywanej bądź przez sąd bądź przez inny niezależny organ administracyjny[50]. Jednak w sytuacji, w której pasażerowie opuścili terytorium Kanady należy przyjąć, że nie stanowią już zagrożenia w zakresie terroryzmu lub poważnych przestępstw międzynarodowych, skoro ani kontrole graniczne przy wjeździe i opuszczeniu kraju, ani też inne weryfikacje podczas

45 Pkt 165 opinii 1/15.
46 Pkt 168–174 opinii 1/15.
47 Pkt 175–178 opinii 1/15.
48 Pkt 179–181 opinii 1/15.
49 Tu TS odwołał się w szczególności do wyroków w sprawie *Schrems I* oraz w sprawie *Tele2 Sverige i Watson*.
50 Pkt 202 opinii 1/15.

pobytu nie wykazały obiektywnych przyczyn do dalszego przetwarzania danych. Zatem w takim przypadku, nie istnieje chociażby pośredni związek między danymi PNR osób, które opuściły terytorium Kanady, a celem umowy. Co do zasady zatem, trwałe przechowywanie danych PNR ogółu pasażerów lotniczych po opuszczeniu przez nich Kanady nie może zostać uznane za konieczne. Jednak może się okazać, że w indywidualnych przypadkach osoby, które wyjeżdżają, takie zagrożenie stwarzają, i wówczas przetwarzanie danych może być uzasadnione, przy czym – znów – powinno podlegać uprzedniej kontroli sądu lub niezależnego organu administracyjnego.

Piąty problem zdefiniowany w opinii 1/15 dotyczył udostępniania danych. Trybunał Sprawiedliwości nie zgodził się, by dane były przekazywane przez organy kanadyjskie władzom państw trzecich, co do których poziom ochrony zapewnianej w tych państwach byłby oceniany przez organy kanadyjskie. Przypomniał w szczególności wymogi wynikające z orzeczenia w sprawie *Schrems I*: przekazywanie danych osobowych z UE do państwa trzeciego może mieć miejsce wyłącznie wówczas, gdy państwo to zapewnia poziom ochrony podstawowych praw i wolności zasadniczo równoważny poziomowi gwarantowanemu w UE. Ten sam wymóg dotyczy przypadków udostępniania danych PNR z Kanady do innych państw trzecich – tak, by nie obchodzić wymogów wynikających z prawa UE. By możliwe było przekazanie danych PNR do państwa trzeciego, konieczne byłoby zawarcie umowy między UE a państwem trzecim albo decyzji Komisji, przyjętej na podstawie stosownych przepisów (w ówczesnym stanie prawnym TSUE wskazał na art. 25 ust. 6 dyrektywy 95/46/WE)[51]. Podobnie, umowa nie określała żadnych szczegółów, które pozwoliłyby uznać, że udostępnianie danych podmiotom prywatnym będzie dopuszczalne (ani kręgu beneficjentów, ani sposobu, w jaki informacje mogłyby zostać wykorzystane), w tym nie wymagała, by udostępnienie danych PNR pozostawało w związku z celem umowy.

Trybunał podniósł także inne zastrzeżenia, w tym wskazał na brak obowiązku notyfikacji podmiotu danych o ich wykorzystaniu lub udostępnieniu na warunkach wynikających z umowy[52]. Wreszcie przypomniał znaczenie niezależnego nadzoru nad przestrzeganiem zasad przetwarzania danych i uznał, że dopuszczenie, by nadzór sprawował nie tylko „niezależny organ publiczny", lecz również „inny organ ustanowiony środkami administracyjnymi (…), który sprawuje swoją funkcję w sposób bezstronny i działa w sposób niezależny, co można potwierdzić". Takie sformułowanie, w ocenie TSUE, budzi wątpliwości, czy faktycznie taki organ nie będzie podporządkowany innemu, który może wpływać na jego decyzje[53].

[51] Pkt 212–215 opinii 1/15.
[52] Pkt 221–225 opinii 1/15.
[53] Pkt 228–231 opinii 1/15.

5. Konsekwencje opinii 1/15 dla systemu PNR i ochrony danych osobowych w Unii Europejskiej

5.1. Przede wszystkim należy stwierdzić, że stanowisko Trybunału nie było zaskakujące. Trybunał Sprawiedliwości w dużej mierze oparł się na swoich wcześniejszych orzeczeniach, w tym na wspomnianych już ustaleniach w sprawach DRI czy *Schrems I*. Nie odszedł od swojego stanowiska, chociaż niektóre państwa członkowskie w trakcie postępowania argumentowały (do czego szerzej odniósł się w swojej opinii rzecznik generalny), że instytucje powinny mieć dalej idące uprawnienia, a standard ochrony powinien być nieco niższy w przypadku aktów wchodzących w zakres relacji zewnętrznych. Trybunał zastosował identyczną miarę wobec zarówno umów międzynarodowych zawieranych przez UE, jak i aktów skierowanych do wewnątrz UE.

Słusznie zauważają Martyna Kusak i Paweł Wiliński[54], że Trybunał wskazał wyraźnie, że stosowanie środków polegających na nieukierunkowanym i nieograniczonym gromadzeniu danych jest nieproporcjonalną ingerencją w prawa podstawowe, a w efekcie jest niezgodne z prawem UE. Marcin Rojszczak zauważa, że wniosek ten jest aktualny wobec każdego działania, którego skutkiem jest zatrzymywanie danych, zatem dotyczy również metadanych[55], a także działań organów zajmujących się bezpieczeństwem publicznym. Trzeba jednak pamiętać, że zarówno opinia 1/15, jak i późniejsze orzecznictwo TS dowodzi, że dzieje się tak wyłącznie wówczas, gdy nie jest wykazana konieczność i proporcjonalność działań, wyrażające się w realizacji wymogów określonych w tych orzeczeniach. Trybunał ustanowił bardzo wysoki standard ochrony danych osobowych[56].

To z kolei może budzić wątpliwości podniesione przez niektórych ekspertów, którzy postawili pytanie, czy takie rygorystyczne stanowisko nie doprowadzi do trudności w negocjacjach z państwami trzecimi, które mając wiedzę o tym, że wynegocjowana umowa może zostać zakwestionowana następczo przez Trybunał, nie będą chciały podejmować takich wysiłków i inwestować swojego czasu i energii w negocjacje[57]. To z kolei otwiera dyskusję w sprawie w ogóle zasadności wypowiadania się przez TSUE odnośnie do umów, które nie weszły jeszcze w życie – przy czym należy przychylić się do stanowiska Mario Mendeza, który zasadnie wskazuje, że przecież właśnie ten

---

[54] M. Kusak, P. Wiliński, *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Warszawa 2020, s. 89 i n.

[55] M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019, s. 476–477.

[56] W. Wiewiórowski, *Surveillance for public security purposes. Four pillars of acceptable interference with the fundamental right to privacy* [w:] *Data Protection and Privacy under Pressure*, red. G. Vemueulen, E. Lievens, Maklu 2017, s. 185–189.

[57] Ch. Kuner, *Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15*, Verfassungsblog, 26 July 2017, verfassungsblog.de [dostęp: 25.11.2021]. Autor wskazuje m.in. że zarówno rzecznik generalny, jak i TSUE dokonali bardzo szczegółowej analizy umowy, kwestionując m.in. użycie skrótu „itd." w załączniku określającym wykaz przetwarzanych danych (zob. pkt 157 wyroku). Autor podkreśla również, że TSUE nie wyjaśnił dokładnie, na jakich źródłach opierał się, oceniając umowę.

moment umożliwia zapobieżenie wejściu w życie umowy, która nie spełnia podstawowych wymogów odnośnie do zgodności z traktatami[58]. Hielke Hijmans uważa, że Trybunał wręcz przejął rolę współprawodawcy – fakt, że Trybunał dokonał bardzo dogłębnej analizy porozumienia pozwala uzasadnić takie stanowisko, chociaż oczywiście, zgodnie z art. 218 ust. 11 TFUE, Trybunał Sprawiedliwości jest uprawniony do kontrolowania wynegocjowanej już umowy[59]. Bez wątpienia jednak takie podejście Trybunału może utrudniać jakiekolwiek dalsze rozmowy i negocjacje, powodując, że negocjatorzy unijni mają związane ręce.

5.2. W opinii 1/15 Trybunał Sprawiedliwości nie zakwestionował w ogóle systemu PNR, uznając go za potrzebny i przydatny do zwalczania terroryzmu i poważnej przestępczości. Trybunał zasadniczo zgodził się ze stanowiskiem, że zatrzymywanie danych PNR i ich wykorzystywanie do chwili opuszczenia Kanady przez pasażerów lotniczych jest co do zasady dopuszczalne, bowiem pozwala na ułatwienie kontroli bezpieczeństwa i kontroli granicznych. Zatrzymywanie i wykorzystywanie danych PNR w tym celu z samej swej istoty nie może być ograniczone do określonego kręgu pasażerów lotniczych, ani podlegać uprzedniej zgodzie sądu lub niezależnego organu administracyjnego. Tymczasem w sprawie *Tele2/Watson* Trybunał uznał, że niedopuszczalna jest uogólniona i niezróżnicowana retencja danych. W opinii 1/15 Trybunał nie wyjaśnił, czym różni się retencja danych PNR od tych, o których mowa w sprawie *Tele2/Watson* – można jedynie domyślać się tak, jak czyni to Lorna Woods, że chodzi o charakter danych[60.] Trybunał stwierdził jedynie, że przetwarzanie danych w ramach umowy było ograniczone wyłącznie do niektórych aspektów życia prywatnego, „w szczególności dotyczących podróży lotniczych między Kanadą a Unią Europejską"[61.].W istocie, można było oczekiwać od Trybunału bardziej dokładnego wyjaśnienia i wskazania tych elementów, które ukazywałyby niezbędność i proporcjonalność masowego i rutynowego przetwarzania danych osób, które zasadniczo nie są o nic podejrzewane, do celów walki z przestępczością[62]. Tym samym, Trybunał zaakceptował co do zasady przetwarzanie danych PNR, o ile spełnione zostaną warunki i ograniczenia wskazane w opinii 1/15, przy czym szczególnie jest to istotne w kontekście tych przepisów, które miałyby zezwalać na przekazywanie danych PNR do państw trzecich[63].

---

58 M. Mendez, *Opinion 1/15: The Court of Justice Meets PNR Data (Again!)*, „European Papers" 2017, vol. 2, nr 3, s. 812. Zob. również *idem*, *Constitutional Review of Treaties: Lessons for Comparative Constitutional Design and Practice*, „International Journal of Constitutional Law" 2017, p. 84.

59 H. Hijmans, *PNR Agreement EU-Canada*…, s. 410.

60 L. Woods, *Transferring Personal Data Outside the EU: Clarification from the ECJ?*, EU Law Analysis, 4 August 2017, eulawanalysis.blogspot.co.uk [dostęp: 25.11.2021].

61 Pkt 150 opinii 1/15.

62 Tak w swojej opinii wskazywał m.in. EDPS. Zob. cytowaną już opinię 5/2015 z 24.09.2015 r. w sprawie umowy z Kanadą.

63 Na to zwraca uwagę Ch. Kuner, *Court of Justice International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, „Common Market Law Review" 2018, vol. 55, nr 3, s. 857–882.

5.3. Dla samej umowy z Kanadą opinia 1/15 Trybunału Sprawiedliwości miała fundamentalne znaczenie, bowiem – zanim mogłaby zostać zawarta – musiałaby zostać istotnie zmieniona. To zaś oznacza otwarcie negocjacji na nowo. Zgodnie z art. 218 ust. 11 TFUE, w przypadku negatywnej opinii Trybunału przewidywana umowa nie może wejść w życie, chyba że nastąpi jej zmiana lub rewizja Traktatów. Do rewizji traktatów nie dojdzie w tym względzie oczywiście, zatem konieczne było podjęcie dalszych negocjacji. Jeszcze w 2017 r. Komisja przesłała Radzie zalecenie dotyczące rozpoczęcia negocjacji[64], które zainicjowano w czerwcu 2018 r. W lipcu 2019 r. zarówno UE, jak i Kanada we wspólnym oświadczeniu wypowiedziały się w sprawie konieczności szybkiego sfinalizowania prac nad umową[65]. Taka umowa, której treści do dnia dzisiejszego nie znamy, mogłaby stanowić swoisty wzór – modelowe rozwiązanie dla przyszłych umów z państwami trzecimi. W negocjowanych umowach z Japonią czy Meksykiem, ewentualnie z innymi państwami trzecimi, szczególnie rygorystycznie powinno podejść się do problemu konieczności i proporcjonalności systemu PNR, a także do praktycznego wdrażania zasady celowości dotyczącej wykorzystywania przekazanych danych PNR.

5.4. Większy problem dotyczy tego, jak opinia 1/15 wpływa na obowiązujące umowy z USA i Australią. Pomijając problem podstawy prawnej (porozumienia zostały zawarte na tej samej podstawie prawnej, którą zakwestionował TSUE w opinii 1/15), należy stwierdzić, że to obydwie umowy zawierają merytoryczne rozwiązania równoważne tym, które TSUE podniósł jako niezgodne z KPP i TFUE w opinii dotyczącej umowy z Kanadą[66]. Umowy te zawarte były w stanie prawnym poprzedzającym wyrok TSUE w sprawach *DRI* czy *Tele 2/Watson*.

Do najważniejszych problemów występujących w obu umowach zaliczyć należy ten sam zakres danych (nieprecyzyjny), jak w przypadku Kanady, a także niedopuszczalność przekazywania danych sensytywnych bez wyraźnego i bardzo dokładnego uzasadnienia. W obu porozumieniach występują problemy dotyczące zasady celowości, zwłaszcza że w przypadku umowy z USA chodzi nie tylko o przestępczość terrorystyczną, ale również o wiele szerzej – o „przestępstwa powiązane" (*related crimes*), zaś „przestępstwa transgraniczne" są bardzo szeroko zdefiniowane. Dane PNR, o ile zajdzie konieczność, mogą być wykorzystywane i przetwarzane w indywidualnych przypadkach, gdy jest to niezbędne z uwagi na poważne zagrożenie, oraz w celu ochrony żywotnych interesów jakiejkolwiek osoby fizycznej, lub jeżeli nakaże tak sąd (art. 4 ust. 2 umowy z USA). Departament Bezpieczeństwa Wewnętrznego USA może także wykorzystywać i przetwarzać dane PNR w celu identyfikacji osób, które po przyjeździe do Stanów Zjednoczonych lub przed opuszczeniem tego państwa zostałyby

[64] Komisja Europejska, Zalecenie w sprawie decyzji Rady upoważniającej do rozpoczęcia negocjacji w sprawie Umowy między Unią Europejską a Kanadą o przekazywaniu i wykorzystywaniu danych dotyczących przelotu pasażera (PNR) w celu zapobiegania terroryzmowi i innym poważnym przestępstwom o charakterze międzynarodowym oraz walki z nimi, COM(2017) 605 final.

[65] Zob. pkt 11 Canada – EU Summit Joint Declaration, July 17–18, 2019, Montreal, https://www.consilium.europa.eu/media/40403/final-2019-joint-declaration-final.pdf [dostęp: 25.11.2021].

[66] Analizy dokonał M. Mendez, *Opinion 1/15*…, s. 815–818.

poddane dokładniejszemu przesłuchaniu lub sprawdzeniu, lub w przypadku których może zachodzić konieczność dalszego sprawdzenia (art. 4 ust. 3 umowy z USA)[67]. Żadna z umów nie dokonuje rozróżnienia między danymi osób, które przybyły już i przebywają na terytorium państwa trzeciego i osób, które z niego wyjechały. Obie umowy przewidują również przekazywanie danych PNR do państw trzecich – co zgodnie z opinią 1/15 – wymagałoby porozumienia między UE a państwem trzecim lub decyzji o adekwatności poziomu ochrony.

Jasno zatem widać, że obie umowy nie są zgodne z KPP oraz TFUE w podobnym zakresie, w jakim za niezgodną uznał TSUE umowę z Kanadą. Jednak obie umowy obowiązują i nie ma obecnie prawnej możliwości ich unieważnienia w trybie określonym w art. 218 czy art. 263 TFUE. Otwarte pozostaje pytanie, czy takiej oceny ważności nie mógłby dokonać Trybunał Sprawiedliwości w odpowiedzi na pytanie prejudycjalne sądu krajowego[68]. Umowa z USA, która weszła w życie w 2012 r., zgodnie z art. 26 pozostaje w mocy przez okres siedmiu lat od dnia jej wejścia w życie, a po upływie tego termin i wszelkich kolejnych okresów – jest przedłużana na okres kolejnych siedmiu lat, o ile jedna ze stron nie powiadomi drugiej strony drogą dyplomatyczną, z co najmniej dwunastomiesięcznym wyprzedzeniem, o zamiarze nieprzedłużania umowy. Takiego zamiaru dotychczas nie wyrażono, a Komisja nie podjęła działań zmierzających do renegocjacji umowy, co według M. Mendeza, mogłoby być nawet podstawą do wszczęcia postępowania przeciwko Komisji (skarga na bezczynność) na podstawie art. 265 TFUE[69], skoro Komisja ma świadomość niezgodności postanowień obu umów z traktatami i KPP. Rówież Christopher Kuner stawia pytania o działania instytucji UE, zastanawiając się, jak to jest możliwe że Komisja i Rada wynegocjowały i zaakceptowały tekst, który następnie został uznany przez TS za posiadający tak istotne wady, jeśli chodzi o poziom ochrony praw podstawowych. Christopher Kuner przypomina przy tym, że przecież Kanada ma długą historię współpracy z UE w dziedzinie ochrony danych osobowych, i że prawo tego państwa jest stosunkowo bliskie rozwiązaniom unijnym – jak w tym świetle przedstawia się możliwość wynegocjowania satysfakcjonującego tekstu z państwami charakteryzującymi się o wiele niższym standardem ochrony?[70]

5.5. Wreszcie, opinia 1/15 powinna mieć znaczenie dla systemu EU-PNR, prowadząc nie tylko do zmian w jego funkcjonowaniu, ale przede wszystkim w regulacjach[71].

---

[67] Zob. również art. 4 ust. 3 umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (Dz. Urz. L 215 z 2012 r., s. 5).

[68] Takiej oceny dokonywał TSUE w odpowiedzi na pytania prejudycjalne sądu krajowego w odniesieniu do ważności porozumienia o partnerstwie w sektorze rybołówstwa pomiędzy Wspólnotą Europejską a Królestwem Marokańskim (Dz. Urz. L 141 z 2006 r., s. 4). Zob. wyrok TSUE w sprawie C-266/16 *Western Sahara Campaign UK*, z dnia 27 lutego 2018 r., ECLI:EU:C:2018:118.

[69] M. Mendez, *Opinion 1/15*…, s. 816.

[70] Ch. Kuner, *Court*…, s. 857–882.

[71] Geneza i przyczyny przyjęcia dyrektywy 2016/681 – zob. D. Lowe, *The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit for Purpose?*, „International Criminal Law Review" 2016,

Chociaż Komisja Europejska w chwili obecnej takiej potrzeby nie dostrzega[72], to jednak wątpliwości może wzbudzać w szczególności zakres gromadzonych danych (w tym przede wszystkim „uwagi ogólne")[73]. Ostateczna ocena co do tego, czy ograniczenia praw podstawowych określonych w dyrektywie EU-PNR są dopuszczalne, wymaga analizy pod kątem konieczności i proporcjonalności. W szczególności, brak jakiejkolwiek wzmianki o ochronie praw podstawowych w dyrektywie EU-PNR może budzić obawy co do jej rzeczywistego wpływu na prawa podstawowe i stawiać pod znakiem zapytania kwestię, czy taki program jest rzeczywiście niezbędny do skutecznego zwalczania poważnej przestępczości oraz terroryzmu, chociaż oczywiście fakt, że walka z międzynarodowym terroryzmem i utrzymanie międzynarodowego pokoju i bezpieczeństwa, a także zapewnienia bezpieczeństwa publicznego stanowi cel interesu ogólnego wynika z dotychczasowego orzecznictwa[74]. W literaturze podkreśla się też, że wątpliwości może budzić kwestia celowości (art. 7 ust. 5 dyrektywy EU-PNR), zakres gromadzonych danych, okres zatrzymania danych, nieprecyzyjne gwarancje procesowe i wreszcie przyznanie prawa do porównywania danych PNR z danymi zgromadzonymi w bazach prowadzonych do innych celów[75]. Ta ostatnia kwestia była podnoszona przez Europejskiego Inspektora Ochrony Danych, który – w przypadku umowy z Kanadą – krytykował regulowane porównywanie danych PNR z nieograniczoną liczbą niezdefiniowanych baz, uznając, że jest to nadmierne i nieproporcjonalne[76]. Dyrektywa musi ustanawiać jasne i precyzyjne reguły co do zakresu i stosowania transferu danych oraz regulować minimalne zabezpieczenia i gwarancje skutecznej

---

nr 16, s. 856–884. Autor uważa, że dyrektywa dobrze realizuje założenia prawa do prywatności i nie wzbudza większych zastrzeżeń. W świetle pytań prejudycjalnych skierowanych przez sądy krajowe do TSUE takie stanowisko może jednak się nie utrzymać. Innego zdania jest zdecydowanie S. Roda, która przedstawia swoją analizę, z której wynika, że część przepisów dyrektywy wymaga zmiany. Zob. *eadem*, *Shortcomings of the Passenger Name Record Directive in Light of Opinion 1/15 of the Court of Justice of the European Union*, „European Data Protection Law Review" 2020, nr 1, s. 66 i n. Zob. też S. Fantin, P. Vogiatzoglou, P. Dewitte, K. Quezada Tavárez, *From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives*, „Journal of Intellectual Property" 2020 nr 11, https://ssrn.com/abstract=3777074 [dostęp: 25.11.2021]. Z kolei wątpliwości co do uregulowania kwestii profilowania w dyrektywie EU PNR wyrażali również V. Papakonstantinou, P. De Hert, *Repeating the Mistakes of the Past Will Do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling*, „New Journal of European Criminal Law", 2015 nr 2, s. 160, ale także np. J. Wojnowska-Radzińska, która wyjaśnia też założenia dyrektywy, zob. *eadem*, *Legitimizing Pre-Emptive Data Surveillance under EU Law – the case of the PNR Directive*, RPEiS 2021, z. 1, https://doi.org/10.14746/rpeis.2021.83.1.9. [dostęp: 25.11.2021].

[72] Zob. wnioski płynące ze sprawozdania zawartego w sprawozdaniu COM(2020) 305 final.

[73] Autorka niniejszego opracowania również przedstawiała wątpliwości na etapie prac nad projektem dyrektywy. Zob. w szczególności: A. Grzelak, *Opinia dotycząca projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania*, „Zeszyty Prawnicze Biura Analiz Sejmowych" 2011, nr 2, s. 39–52.

[74] Zob. w szczególności wyrok w sprawie *Kadi*, ECLI:EU:C:2008:461, pkt 363; *Al-Aqsa* (ECLI:EU:C:2012:711), pkt 130); *Tsakouridis* (ECLI:EU:C:2010:708), pkt 46 i 47.

[75] S. Roda, *Shortcomings of the Passenger Name Record Directive*…, s. 77–78.

[76] Opinia EIOD 5/2015 z 24.09.2013, pkt 37.

ochrony danych osobowych przed ryzykiem nadużycia oraz przed wszelkim niezgodnym z prawem dostępem i wykorzystaniem tych danych. Oceny tego, czy tak rzeczywiście jest, może dokonać Trybunał Sprawiedliwości, jednak dotychczasowa wykładnia art. 7, art. 8 i art. 52 ust. 1 Karty oraz art. 16 TFUE może prowadzić do oczekiwania, że dyrektywa EU-PNR powinna zostać zmieniona.

Trzeba przy tym zauważyć, że w chwili obecnej trwają analizy zgodności dyrektywy EU-PNR z wymogami wynikającymi z traktatu i KPP, bowiem w trybie art. 267 TFUE, przed Trybunałem zawisło kilka postępowań, w których sądy krajowe proszą o ocenę ważności dyrektywy lub o wykładnię jej przepisów:

1) C-486/20 – pytanie sądu słoweńskiego z 1.10.2020 r. w sprawie *Varuh človekovih pravic Republike Slovenije (Rzecznik Praw Obywatelskich Słowenii)* – dotyczy pkt 8 i pkt 12 załącznika do dyrektywy 2016/681 i oceny zgodności z art. 7 i art. 8 oraz z art. 52 ust. 1 KPP;
2) C-222/20 – pytanie z 27.05.2020 r. niemieckiego Verwaltungsgericht Wiesbaden w sprawie *OC / Bundesrepublik Deutschland* – sąd krajowy sformułował kilka pytań, dotyczących przede wszystkim wykładni art. 7 i art. 8 KPP w związku z krajowymi przepisami wdrażającymi dyrektywę 2016/681;
3) C-215/20 – pytanie z 19.05.2020 r. niemieckiego Verwaltungsgericht Wiesbaden, który sformułował bardzo ważne pytanie ogólne plus pytania szczegółowe, zmierzające do ustalenia, czy dyrektywa 2016/681 jest zgodna z art. 7, art. 8 i art. 52 Karty;
4) trzy sprawy z identycznymi pytaniami:
   a) C-148/20 – pytanie z 16.03.2020 r. sądu niemieckiego w sprawie *AC / Deutsche Lufthansa AG*;
   b) C-149/20 – pytanie z 16.03.2020 r. sądu niemieckiego w sprawie *DF / Deutsche Lufthansa AG*;
   c) C-150/20 – pytanie z 17.03.2020 r. sądu niemieckiego w sprawie *BD / Deutsche Lufthansa AG*.
5) C-817/19 – pytanie z 31.10.2019 r. belgijskiego Cour constitutionnelle (Belgia) w sprawie *Ligue des droits humains / Conseil des ministers* – w tym przypadku, poza pytaniami dotyczącymi samej dyrektywy 2016/681, jest również pytanie odnoszące się do zakresu stosowania RODO w kontekście przepisów krajowych wdrażających dyrektywę.

Wszystkie te sprawy są w toku i w żadnej nie przedstawiono jeszcze opinii rzecznika generalnego.

5.6. Problem wyważenia między prawem do prywatności a porządkiem publicznym i bezpieczeństwem pojawił się również we wspomnianych już sprawach *Privacy International* oraz *La Quadrature du Net i in.*[77] Trybunał Sprawiedliwości w tych sprawach

[77] Wyroki te wymienione zostały w przypisie 5. Na temat tych wyroków zob. też A. Grzelak, K. Zielińska, *Między prawem do prywatności i ochrony danych osobowych a zapewnieniem bezpieczeństwa publicznego i walką z przestępczością. Problemu retencji danych ciąg dalszy – glosa do wyroków Trybunału*

analizował możliwość zastosowania dyrektywy o e-prywatności do działalności związanej z bezpieczeństwem narodowym i zwalczaniem terroryzmu, a także zakres, w jakim państwa członkowskie mogą dokonać ograniczenia prawa do prywatności i ochrony danych osobowych dla celów związanych z bezpieczeństwem narodowym i zwalczaniem terroryzmu. Trybunał dokonał też analizy art. 6 Karty, ponieważ jest wykorzystywany jako argument przez państwa członkowskie do uzasadnienia ingerencji w prawo do prywatności. Wyroki i opinie rzeczników generalnych w tych sprawach są bardzo obszerne, jednak niektóre wnioski można odnieść również do systemu PNR, bowiem w sprawie *Privacy International* głównym problemem było masowe gromadzenie danych i zautomatyzowane przetwarzanie w celu ochrony bezpieczeństwa narodowego przez krajowe agencje wywiadowcze, z kolei w sprawie *La Quadrature du Net* Trybunał analizował uogólnione i niedyskryminacyjne zatrzymywanie danych oraz legalność procedur retencji danych (problem powiadamiania podmiotu danych), a także rozważał, czy poza uzasadnieniem, jakim jest walka z bezpieczeństwem narodowym, zwalczaniem terroryzmu i poważnej przestępczości, również bezpieczeństwo terytorium, porządek publiczny i inne podobne argumenty uzasadniają dopuszczalność przetwarzania danych, i czy taki obowiązek nie wynika przy okazji z art. 4 i 6 KPP. I chociaż dotyczą one bardziej relacji wewnętrznych UE, i w tym aspekcie stanowisko TS jest nieco bardziej zniuansowane, to jednak zasadnicze poglądy wyrażane w wyrokach DRI i późniejszych zostało utrzymane.

5.7. Na poziomie ogólniejszym można zastanawiać się nad istotą prawa do ochrony prywatności i prawa do ochrony danych osobowych. Christopher Kuner zauważa, że w ostatnich latach TS kilkakrotnie wypowiadał się na ten temat, wskazując, iż – po pierwsze – masowa retencja danych nie wpływa na istotę prawa do prywatności zgodnie z art. 7 KPP, bowiem nie prowadzi do wyjawienia treści komunikacji elektronicznej[78]; po drugie – nie narusza istoty prawa do ochrony danych osobowych określonego w art. 8 KPP, bowiem dostawcy usług muszą przestrzegać stosownych przepisów[79]; po trzecie – przyjęte rozwiązania prawne są wyrazem kompromisu wobec treści art. 7 KPP[80]; i wreszcie – gwarantuje prawa osobom, których dane są przetwarzane, w tym prawo dostępu[81]. W opinii 1/15 TSUE również nie uznał, by doszło do naruszenia istoty prawa do prywatności i prawa do ochrony danych osobowych, bowiem przekazywane dane były ograniczone wyłącznie do pewnego wycinka prywatności, związanej z podróżami lotniczymi. Słusznie wskazuje Christopher Kuner, że potrzeba jasności i przewidywalność sprawia, iż ważne jest opracowanie ram normatywnych – do tej pory Trybunał nie chciał się wypowiedzieć na temat samych kryteriów, co byłoby istotne zwłaszcza ze względu na to, że sama prywatność jest pojmowana kontekstowo i defi-

---

Sprawiedliwości z 6.10.2020 r.: C-623/17, Privacy International, oraz w sprawach połączonych C-511/18, C-512/18, C-520/18, La Quadrature du Net i in., EPS 2021, nr 8, s. 28.

78 Wyrok ws. DRI, pkt 39.

79 *Ibidem*, pkt 40.

80 Wyrok ws. *Schrems I*, pkt 94.

81 *Ibidem*, pkt 95.

niowana na podstawie indywidualnych przypadków. Być może, jak uważa Maja Brkan, nie ma po prostu możliwości określenia abstrakcyjnie tego, co stanowi istotę praw podstawowych[82]. Być może w istocie tak jest, ale jednak z orzecznictwa TS wynika, że naruszenie istoty prawa podstawowego jest nielegalne i nie jest przedmiotem testu proporcjonalności, co wiązałoby się z koniecznością podjęcia próby zdefiniowania tego pojęcia.

6. Wnioski

Opinia 1/15 jest wyrazem troski Trybunału o wysoki standard ochrony prywatności i danych osobowych i stanowi kontynuację stanowiska wyrażanego w sprawach DRI, *Schrems I*, *Tele2/Watson* czy *Schrems II*. Trybunał po raz kolejny udowodnił, że nie pozwoli na obchodzenie i obniżanie standardów w relacjach zewnętrznych, w tym w zawieranych przez UE umowach bilateralnych. Pozostaje otwartą kwestia, czy Komisja Europejska będzie w stanie i czy będzie próbować przekonać państwa trzecie o konieczności przestrzegania wymogów wynikających z opinii 1/15. Pewne wątpliwości budzi fakt, że problem ten nie stał się jeszcze przedmiotem rozmów z USA i Australią, zaś dyrektywa 2016/681 w ocenie Komisji nie wymaga zmian.

Ostatecznie Trybunał nie odrzucił systemu PNR w całości, tworząc jednak tzw. checklistę wymogów proceduralnych, które muszą być spełnione, by uznać dopuszczalność stosowania tych rozwiązań. Spełnienie wymogów wskazanych przez Trybunał jest trudne, co – biorąc pod uwagę, jak spowolnione zostały rozmowy w sprawie systemów PNR – oznacza, że w praktyce kontynuowanie umów jest bardzo utrudnione[83]. I chociaż – patrząc przez pryzmat praw podstawowych – można zarzucać Trybunałowi, że opowiedział się za dopuszczalnością uogólnionego i niedyskryminacyjnego systemu inwigilacji podróżujących, to jednak w istocie Trybunał zmiękczył bardzo swoje stanowisko, wprowadzając liczne wymogi proceduralne, które mają chronić prawa podstawowe[84].

Trybunał w opinii 1/15 przedstawił wyważone stanowisko, ponieważ nie posunął się za daleko i zasadniczo dał zielone światło systemom PNR. Jednakże Trybunał tak szczegółowo zbadał istotę umowy, że może to mieć i zapewne ma kłopotliwe konsekwencje dla stosunków międzynarodowych UE. Nie wiadomo jeszcze, czy Komisja będzie w stanie przekonać państwa trzecie o konieczności spełnienia wysokich

---

[82] M. Brkan, *In Search of the Concept of Essence of EU Fundamental Rights Through the Prism of Data Privacy*, „Maastricht Faculty of Law Working Paper" 2017 nr 1, 16.01.2017. *Eadem*, *The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, „German Law Journal" 2019, nr 20, s. 864–883.

[83] E. Guild, E. Mendos Kuşkonmaz, *EU Exclusive jurisdiction on surveillance related to terrorism and serious transnational crime: case review on Opinion 1/15*, „European Law Review" 2018, vol. 43, nr 4, s. 583–597.

[84] A. Vedaschi, *The European Court of Justice on the EU-Canada Passenger Name Record Agreement*, „European Constitutional Law Review" 2018, vol. 14, nr 2, s. 410–429.

standardów określonych w opinii 1/15, przy czym Stany Zjednoczone są bez wątpienia najtrudniejsze do przekonania, biorąc pod uwagę ich rozbieżne podejście do prywatności. W każdym razie pozostaje jeszcze do odrobienia lekcja związana z koniecznością zmiany dyrektywy UE w sprawie PNR – standard unijny nie może być niższy niż ten, który przedstawiono w opinii 1/15. Niezależnie od tego, czy mamy do czynienia z wewnętrznym systemem PNR w UE, czy z umowami PNR z państwami trzecimi, szczególnie trudnym wyzwaniem będzie opracowanie systemów, które będą w stanie wprowadzić w życie zaproponowane przez Trybunał rozróżnienia dotyczące zatrzymywania i wykorzystywania danych PNR przed przylotem pasażerów lotniczych, podczas ich pobytu i odlotu oraz po ich odlocie.

Trybunał Sprawiedliwości w swoich orzeczeniach konsekwentnie pokazuje również, że w walce UE z terroryzmem, prywatność i ochrona danych nie zeszły na dalszy plan w stosunku do inicjatyw w zakresie bezpieczeństwa, czego dowodzi nie tylko opinia 1/15, ale także seria orzeczeń w sprawach *Schrems*, w których TS konsekwentnie sprzeciwia się asymetrycznym relacjom między UE a USA, z bardziej dominującą pozycją USA. Jeśli Trybunał dostrzega naruszenia prawa UE, nie ma oporów przed podejmowaniem decyzji, które prowadzą do niezawarcia ważnych umów czy unieważnienia podstaw prawnych współpracy. Trybunał pokazuje przy tym, że interesy bezpieczeństwa i prywatności nie wykluczają się wzajemnie i powinny się przeplatać i uzupełniać.

Literatura

Brkan M., *In Search of the Concept of Essence of EU Fundamental Rights Through the Prism of Data Privacy*, „Maastricht Faculty of Law Working Paper", 2017 nr 1.

Brkan M., *The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, „German Law Review German Law Journal" 2019, nr 20

Fantin S., Vogiatzoglou P., Dewitte P., Quezada Tavárez K., *From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives*, „Journal of Intellectual Property" 2020, nr 11.

Grzelak A., *Główne cele ogólnego rozporządzenia o ochronie danych* [w:] M. Kawecki i T. Osiej, *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, Warszawa 2017.

Grzelak A., *Opinia dotycząca projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania*, „Zeszyty Prawnicze Biura Analiz Sejmowych" 2011, nr 2

Grzelak A., *Prawo do ochrony danych osobowych a konieczność walki z przestępczością. Uwagi na tle art. 16 traktatu o funkcjonowaniu Unii Europejskiej* [w:] *Prawo Unii Europejskiej a prawo konstytucyjne państw członkowskich*, red. S. Dudzik, N. Półtorak, Warszawa 2013.

Grzelak A., Zielińska K., *Między prawem do prywatności i ochrony danych osobowych a zapewnieniem bezpieczeństwa publicznego i walką z przestępczością. Problemu retencji danych ciąg dalszy - glosa do wyroków Trybunału Sprawiedliwości z 6.10.2020 r.: C-623/17, Privacy International, oraz w sprawach połączonych C-511/18, C-512/18, C-520/18, La Quadrature du Net i in.*, EPS 2021, nr 8.

Guild E., Brouwer E., *The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief, July 2006, nr 109.

Guild E., Mendos Kuşkonmaz E., *EU Exclusive jurisdiction on surveillance related to terrorism and serious transnational crime: case review on Opinion 1/15*, „European Law Review" 2018, vol. 43, nr 4.

Hijmans H., *PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators*, „European Data Protection Law Review" 2017, nr 3.

Hobbing P., *Tracing Terrorists: The EU-Canada Agreement in PNR Matters*, CEPS Special Report, September 2008, revised version 17.11.2008, http://aei.pitt.edu/11745/1/1704.pdf [dostęp: 18.06.2021].

Kuner Ch., *Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15* [w:] Verfassungsblog, 26 July 2017, verfassungsblog.de [dostęp: 25.11.2021].

Kuner Ch., *Court of Justice International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, „Common Market Law Review" 2018, vol. 55, nr 3.

Kusak M., Wiliński P., *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Warszawa 2020.

Lowe D., *The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit for Purpose?*, „International Criminal Law Review" 2016, nr 16.

Maruhashi T., *Japan-EU Passenger Name Record Negotiations and Their Implications* [w:] *Human-Centric Computing in a Data-Driven Society. 14th IFIP TC 9 International Conference on Human Choice and Computers*, red. D. Kreps, T. Komukai, T.V. Gopal, K. Ishii, HCC14 2020, Tokyo, Japan, September 9–11, 2020, Proceedings, Springer 2020.

Mendez M., *Constitutional Review of Treaties: Lessons for Comparative Constitutional Design and Practice*, „International Journal of Constitutional Law" 2017.

Mendez M., *Opinion 1/15: The Court of Justice Meets PNR Data (Again!)*, „European Papers" 2017 vol. 2, nr 3.

Mendez M., *Passenger Name Record Agreement*, „European Constitutional Law Review" 2007, vol. 3, nr 1.

Papakonstantinou V., De Hert P., *Repeating the Mistakes of the Past Will Do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling*, „New Journal of European Criminal Law" 2015, nr 2.

Papakonstantinou V., De Hert P., *The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic*, „Common Market Law Review" 2009.

Roda S., *Shortcomings of the Passenger Name Record Directive in Light of Opinion 1/15 of the Court of Justice of the European Union*, „European Data Protection Law Review 2020", nr 1

Rojszczak M., *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019.

Schwartz P.M., *The EU-US Privacy Collission: A Turn to Institutions and Procedures*, „Harvard Law Review" 2013.

Vedaschi A., *The European Court of Justice on the EU-Canada Passenger Name Record Agreement*, „European Constitutional Law Review" 2018, vol. 14, nr 2.

Wiewiórowski W., *Surveillance for public security purposes. Four pillars of acceptable interference with the fundamental right to privacy* [w:] *Data Protection and Privacy under Pressure*, red. G. Vemueulen, E. Lievens, Maklu 2017.

Wojnowska-Radzińska J., *Legitimizing Pre-Emptive Data Surveillance under EU Law – the case of the PNR Directive*, RPEiS 2021, z. 1.
Woods L., *Transferring Personal Data Outside the EU: Clarification from the ECJ?,* EU Law Analysis, 4 August 2017, eulawanalysis.blogspot.co.uk [dostęp: 25.11.2021].

Streszczenie

Agnieszka Grzelak

Przyszłość współpracy UE z państwami trzecimi w sprawie przekazywania danych pasażerów lotniczych. O skutkach opinii Trybunału Sprawiedliwości nr 1/15 dla wymiany danych PNR

System przekazywania danych pasażerów linii lotniczych właściwym organom państwowym do celów związanych z walką z terroryzmem i poważną przestępczością zaczął się w Unii Europejskiej rozwijać, odkąd Stany Zjednoczone zaczęły się domagać takich informacji. W efekcie, Unia Europejska rozpoczęła proces przygotowania umów z państwami trzecimi, które pozwalałyby na przekazywanie takich danych, jak i tworzenia wewnątrzunijnego systemu wymiany danych. W opinii 1/15 dotyczącej umowy z Kanadą, która miała być zawarta przez Unię, Trybunał Sprawiedliwości wyraźnie dopuścił tworzenie systemów wymiany danych PNR, jednakże obwarował to istotnymi ograniczeniami i gwarancjami, które miałyby zapewnić wysoki poziom ochrony prywatności i danych osobowych obywateli UE. W efekcie, do zawarcia umowy z Kanadą nie doszło, negocjacje z innymi państwami zostały wstrzymane. Jednocześnie umowy UE z USA i Australią obowiązują mimo tego, że zawierają sformułowania analogiczne do tych, które uznane zostały przez TSUE za niezgodne z Kartą Praw Podstawowych Unii Europejskiej i Traktatem o funkcjonowaniu Unii Europejskiej. Celem artykułu jest zarówno dokonanie przeglądu tej sytuacji, jak i próba spojrzenia na skutki opinii 1/15 dla systemu wymiany danych PNR w Unii Europejskiej.

Słowa kluczowe: dane PNR; zwalczanie terroryzmu; opinia 1/15; ochrona danych osobowych; RODO.

Summary

Agnieszka Grzelak

The Future of EU Cooperation with Third Countries on the Transfer of Passenger Names Records. On the Effects of the Opinion No. 1/15 of the Court of Justice of the EU on the Exchange of PNR Data

The system for transferring passenger data to the competent state authorities for the purpose of combating terrorism and serious crime began to develop in the European Union after the United States had requested such information from the air carriers. As a result, the European Union started the process of preparing agreements with third countries that would allow the transfer of such data, as well as setting up an intra-EU system for the exchange of data. In the Opinion 1/15 on the agreement with Canada, which was to be concluded by the European

Union, the Court of Justice explicitly allowed for setting up PNR data exchange systems, but subjected this to important limitations and guarantees that would ensure a high level of protection of the privacy and personal data of EU citizens. As a result, the agreement with Canada has not been concluded and negotiations with other countries have been put on hold. At the same time, EU agreements with the US and Australia remain in force, despite the fact that they contain provisions analogous to those found by the CJEU to be incompatible with the Charter of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union. The aim of this article is to review this situation, but also to analyze the implications of the Opinion 1/15 for the system of PNR data exchange in the European Union.

Keywords: PNR data; combating terrorism; Opinion 1/15; personal data protection; GDPR.

Dominik Lubasz
Lubasz i Wspólnicy – Kancelaria Radców Prawnych
dominik.lubasz@lubasziwspolnicy.pl
ORCID: 0000-0001-9716-5802

https://doi.org/10.26881/gsp.2021.4.04

Warunki wyrażania zgody jako przesłanki legalizującej przetwarzanie danych osobowych

1. Wprowadzenie

Zgoda podmiotu danych jest jedną z przesłanek legalizacyjnych przetwarzania danych osobowych zarówno zwykłych, jak i szczególnych kategorii, sformułowanych odpowiednio w art. 6 oraz 9 RODO[1]. Katalog przesłanek legalizacyjnych danych osobowych zwykłych i szczególnych kategorii ma charakter zamknięty, zaś same przesłanki mają charakter autonomiczny i równoprawny[2].

Autonomiczność przesłanek przetwarzania powoduje, że z perspektywy legalizacji procesu przetwarzania wystarczające jest spełnienie warunków jednej z nich[3]. Nie jest jednak wykluczone, że w danym stanie faktycznym w konkretnym procesie przetwarzania będzie spełniona więcej niż jedna przesłanka legalizacyjna, np. przesłanka wykonania umowy i realizacji obowiązku prawnego ciążącego na administratorze[4]. W kontekście zgody autonomiczność ta doznaje pewnych ograniczeń w tym sensie, że w sytuacji gdy podmiot danych odmówił zgody na przetwarzanie jego danych oso-

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1 ze zm.; dalej: RODO, rozporządzenie 2016/679). Na temat rozróżnienia podstaw przetwarzania danych zwykłych i wrażliwych oraz charakteru regulacji w dotychczasowym stanie prawnym – zob. P. Litwiński, P. Barta, *Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2016, s. 224–225; A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2001, s. 49 i s. 81 oraz por. np. wyrok NSA z dnia 11 kwietnia 2003 r., II SA 412/02, niepubl.

[2] D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 347; a także wyrok WSA w Warszawie z dnia 1 grudnia 2005 r., II SA/Wa 917/05, LEX nr 189823; wyrok WSA w Warszawie z dnia 31 marca 2006 r., II SA/Wa 2395/04, LEX nr 197601.

[3] Zob. D. Lubasz, D. Sęczkowski, *Nowe europejskie przepisy o ochronie danych osobowych – przygotowania do wdrożenia czas zacząć*, „Compliance. Magazyn Fachowy Instytutu Compliance" 2016, nr 3.

[4] P. Litwiński, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, komentarz do art. 6, Legalis; oraz P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 161 i n.

bowych, okoliczność ta będzie negatywnie oddziaływała na możliwości skorzystania przez administratora np. z przesłanki uzasadnionego interesu (art. 6 ust. 1 lit f RODO). Z tej perspektywy uprzedni wybór przesłanki legalizacyjnej w zakresie, w jakim jest to dopuszczalne prawnie, ma kluczowe znaczenie dla skutków w obszarze praw podmiotów danych, jak i konsekwencji dla administratora w zakresie skorzystania z nich, przez osobę której dane dotyczą.

Równoprawność przesłanek legalizacyjnych oznacza z kolei, że żadna z przesłanek nie ma charakteru uprzywilejowanego w stosunku do pozostałych. Wynika z tego przede wszystkim konstatacja, że przypisywanie przesłance zgody, co w obrocie jest dość często spotykane, wiodącego znaczenia – nie znajduje uzasadnienia i nie jest poprawne. Przesłanka ta nie zastępuje innych, a wręcz pozyskiwanie przez administratora zgody w sytuacji równoczesnego występowania innej przesłanki legalizacyjnej jest nieprawidłowe i może powodować naruszenie dobrowolności i odwoływalności takiej zgody.

Przesłanki legalizacyjne uszczegóławiają i nadają skonkretyzowaną normatywną treść sformułowanej w art. 5 lit. a RODO zasadzie zgodności z prawem[5], co w konsekwencji przesądza o tym, że ich wykładnia nie może być wyabstrahowana od relacji do zasad przetwarzania danych z art. 5 RODO i musi uwzględniać ograniczenia z nich płynące. Ma to istotne znaczenie również w przypadku zgody jako przesłanki legalizacyjnej, wyznaczającej najdalej idącą autonomię podmiotu danych w zakresie decydowania o przetwarzaniu jego danych osobowych, w tym w kontekście art. 7 i 8 Karty praw podstawowych UE[6], a mimo to niemogącej być podstawą procesów przetwarzania kolidujących z zasadami przetwarzania, w szczególności z zasadą minimalizacji danych.

2. Zgoda jako przesłanka legalizacyjna – zagadnienia ogólne

Pojęcie zgody zdefiniowane zostało w art. 4 pkt 11 RODO i oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Pojęcie to jest kluczowe dla weryfikacji spełnienia przesłanki legalizacyjnej przetwarzania danych osobowych zwykłych oraz szczególnych kategorii danych w myśl, odpowiednio, art. 6 ust. 1 lit. a i art. 9 ust. 2 lit. a RODO, ale także dopuszczenia zautomatyzowanego podejmowania decyzji w stosunku do podmiotu danych, w tym profilowania, o którym mowa w art. 22 ust. 1 w zw. z ust. 2 lit. c RODO, oraz legitymizowania transferu danych do państwa trzeciego, zgodnie z art. 49 ust. 1 lit. a RODO.

Wymogi dotyczące zgody sformułowane w przepisie art. 4 pkt 11 RODO, uzupełniane są dodatkowo regulacją szczegółową przepisu art. 7 określającego szczególne warunki wyrażania zgody oraz art. 8 wskazującym warunki wyrażenia zgody przez

[5] Zob. P. Drobek [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*…, s. 327 i n.
[6] Dz. Urz. C 326 z 2012 r., s. 391.

dziecko w przypadku usług społeczeństwa informacyjnego, a ponadto wyjaśniane w motywach 32, 33, 42 i 43 dotyczących sposobu działania administratora, w celu spełnienia głównych elementów skutecznej zgody.

Koncepcja zgody w rozporządzeniu 2016/679, zachowująca zasadniczą konstrukcję regulacyjną, przyjętą uprzednio w dyrektywie 95/46/WE[7], opartą na autonomii podmiotu danych, jej aktywnym działaniu oraz odwracalności decyzji o wyrażeniu zgody, uległa jednak pewnemu uelastycznieniu, zwłaszcza w zestawieniu z rozwiązaniami przyjętymi w nie obowiązującej już ustawie o ochronie danych osobowych z 1997 r.[8], implementującej do polskiego porządku prawnego dyrektywę 95/46/WE[9]. Dopuszczone zostało bowiem, obok oświadczenia (wyraźnego), złożenie zgody przez jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie wyraźnego działania potwierdzającego przyzwala na przetwarzanie dotyczących jej danych osobowych. Regulacja ta otwiera drogę do akceptacji jako skutecznej zgody działań konkludentnych, które były wykluczone w dotychczasowym stanie prawnym, jako sposobu udzielania zgody. W każdym jednak przypadku zgoda musi być związana z aktywnym działaniem podmiotu danych, a zatem musi być oparta na modelu *opt-in*[10]. Takiej kwalifikacji nie będzie można przypisać biernemu zachowaniu, w tym milczeniu, zgodom predefiniowanym, opartym na domyślnych ustawieniach, czy też zawartym w niewyodrębnionych w zakresie akceptacji postanowieniom regulaminu itp[11]. W tym ostatnim kontekście zwłaszcza podkreśla się konieczność zapewnienia odrębności zgody od innych konwencjonalnych zachowań. Dla swej skuteczności zgoda

---

[7] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (uchylona) (Dz. Urz. L 281, s. 31).

[8] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922).

[9] W art. 7 pkt 5 u.o.d.o. z 1997 r. zgoda jest definiowana jako „oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie". W polskiej doktrynie prawa wskazywano, że poprzez odwołanie się w tej definicji do pojęcia oświadczenia woli należy przy jego wykładni stosować przepisy kodeksu cywilnego, dotyczące definicji oświadczenia woli, kwalifikujące jako takie oświadczenie każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli w postaci elektronicznej (art. 60 k.c.); zob. P. Barta, P. Litwiński, *Ustawa*…, komentarz do art. 23, nt 8. Zastrzegane jednak w przepisie art. 60 k.c. odmienności regulacyjne skłaniały niektórych autorów do uznania, w związku z zakazem zgody domniemanej czy dorozumianej w myśl przepisu art. 7 pkt 5 u.o.d.o. z 1997 r., że wykluczone jest wyrażenie zgody w sposób konkludentny; zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona*…, komentarz do art. 7, nt 33.

[10] Wyrażenie zgody zarówno przez oświadczenie, jak i wyraźne działanie potwierdzające oparto zatem jak dotychczas na systemie *opt-in*, wymagającym od podmiotu danych określonej akcji o określonym natężeniu jednoznaczności i wyraźności. Wykluczono w konsekwencji wszelkie modele *opt-out*, wykorzystujące bierność, milczenie osoby, której dane dotyczą, lub też jej nieuwagę lub bezwolność, a także ustawienia domyślne, domyślnie zaznaczone pola zgód itp.

[11] Tak też L.A. Bygrave, L.Tosoni [w:] Ch. Kuner, L.A. Bygrave, Ch. Docksey, *The EU General Data Protection Regulation (GDPR), A Commentary*, s 184 i s. 185; P. Litwiński, Ogólne *rozporządzenie o ochronie danych, Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021, s. 139 i n; P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 161 i n., zob. również wyrok TSUE w sprawie *Planet49*, C-673/17.

musi być czynnością wyseparowaną[12]. Na gruncie rozporządzenia ogólnego czynność udzielenia zgody może polegać np. na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych[13].

Prawodawca unijny nie sformułował natomiast wymogów co do formy udzielenia zgody. Dokonując odformalizowania, równocześnie obok zasady rozliczalności sformułowanej w art. 5 ust. 2, prawodawca unijny zdecydował się w art. 7 ust. 1 RODO podkreślić, że jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

Ponadto, w niektórych jednak przypadkach, kierując się potrzebą zapewniania podwyższonego standardu ochronnego, w tym poprzez mechanizmy rozliczalności, przewidziane zostały dodatkowe wymogi dotyczące relewantnej aktywności podmiotu danych, z której można wywodzić dozwolenie na przetwarzanie. Dotyczy to przepisów art. 9 ust. 2 lit. a, art. 22 ust. 1 w zw. z ust. 2 lit. c, a także przesłanek legalizujących transfer danych do państwa trzeciego zgodnie z art. 49 ust. 1 lit. a RODO[14]. W tych bowiem wypadkach wymagana jest zgoda wyraźna, co wyklucza możliwość w tych sytuacjach kwalifikacji jako zgody działania konkludentnego.

3. Elementy ważności zgody

W definicji wyróżniono kumulatywne relewantne elementy ważności zgody:
a) dobrowolność;
b) konkretność;
c) świadomość;
d) jednoznaczność.

Wskazane kryteria ważności zgody należy interpretować w sposób ścisły[15]. Wynika to z konsekwentnie przyjmowanego – również na gruncie rozporządzenia 2016/679 – stanowiska[16], zaprezentowanego przez Grupę Roboczą Art. 29 w opinii 15/2011[17]

[12] Na konieczność osobnej w kontekście niełączenia oraz odseparowanej optycznie zgody, zwracał uwagę w swej opinii rzecznik generalny M. Szpunar w sprawie *Planet49*, C-673/17, pkt 68.
[13] D. Lubasz [w:] M. Jagielski, *Dokumentacja ochrony danych osobowych ze wzorami*, Warszawa 2019, s. 203 i n.
[14] D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*…, s. 242–243.
[15] L.A. Bygrave, L. Tosoni [w:] Ch. Kuner, L.A. Bygrave, Ch. Docksey, *The EU General Data*…, s. 181.
[16] Tak Europejska Rada Ochrony Danych w wytycznych dotyczących zgody – zob. wytyczne EROD 05/2020 dotyczące zgody, na mocy rozporządzenia 2016/679, s. 5, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pl.pdf, [dostęp: 19.11.2021]; dalej: wytyczne 05/2020.
[17] Opinia 15/2011, dotycząca definicji zgody (WP 187), s. 8.

w sprawie zgody, że zwracanie się do osób o wyrażenie zgody na czynność przetwarzania danych powinno podlegać rygorystycznym wymogom, ponieważ dotyczy praw podstawowych osób, których dane dotyczą, a administrator pragnie przeprowadzić operację przetwarzania, która byłaby niezgodna z prawem bez zgody podmiotu danych. Pomimo pewnej problematyczności tego stanowiska w kontekście istnienia innych podstaw legalizacyjnych przetwarzania danych osobowych stanowi ono dowód na ścisłe podejście organów nadzorczych do kwestii interpretacji wymogów formalnych ważności zgody[18].

4. Dobrowolność zgody

Wymóg dobrowolności zgody oznacza, że podmiot danych powinien mieć zapewnioną autonomię przy podejmowaniu decyzji nie tylko co do udzielenia zgody, ale także co do odmowy jej udzielania oraz jej wycofania bez niekorzystnych konsekwencji[19]. Co do zasady zatem zgoda może być właściwą, legalną podstawą wyłącznie wówczas, gdy podmiotowi danych, zapewnia się kontrolę oraz rzeczywistą możliwość wyboru w odniesieniu do przyjęcia lub odrzucenia zaoferowanych warunków lub odrzucenia ich bez niekorzystnych konsekwencji[20].

Konkretyzacja wymogu dobrowolności następuje w art. 7 ust. 4 RODO, w którym podkreślono, że oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy m.in. od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy[21].

Jak wskazuje Europejska Rada Ochrony Danych (EROD), przywołana regulacja obejmuje co do zasady nie tylko relację pomiędzy zgodą a wykonaniem umowy, ale także wszelkie inne elementy niewłaściwej presji lub niewłaściwego wpływu na podmiot danych, mogący się przejawiać na wiele rożnych sposobów i uniemożliwiający mu, swobodne okazanie woli[22].

Na ocenę spełnienia przesłanki dobrowolności zgody wpływał będzie negatywnie również wyraźny brak równowagi między podmiotem danych a administratorem. W motywie 43 jako przykład wskazano te sytuacje, gdy administrator jest organem

[18] Zob. też: L.A Bygrave, L. Tosoni [w:] Ch. Kuner, L.A. Bygrave, Ch. Docksey, *The EU General Data*…, s. 181.

[19] Zob. Wytyczne Grupy Roboczej Art. 29 dotyczące zgody, (WP259), s. 7, a także motywy 42, 43 RODO oraz opinia 15/2011 w sprawie definicji zgody (WP187), s. 12.

[20] Wytyczne 05/2020, s. 5; A. Mednis, *Cechy zgody na przetwarzanie danych osobowych w opinii Grupy Roboczej Art. 29 dyrektywy 95/46 Nr 15/2011 (WP 187)* [w:] *Aktualne problemy prawnej ochrony danych osobowych 2012*, MoP 2012, nr 7, dodatek, s. 25; P. Litwiński, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021, s. 137; D. Lubasz, *Ochrona danych osobowych*, Warszawa 2020, s. 122

[21] D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, komentarz do art. 7.

[22] Wytyczne 05/2020, s. 8.

publicznym. Zdaniem EROD, w większości takich przypadków podmiot danych nie będzie miał realnej alternatywy wobec zaakceptowania warunków przetwarzania zaproponowanych przez tego administratora. Ponadto, jak podkreśla, istnieją inne zgodne z prawem podstawy, które są co do zasady właściwsze w przypadku działalności organów publicznych.[23] We wcześniejszych wytycznych Grupy Roboczej Art. 29 jako przypadek nierównowagi wskazano także relację pracodawca – pracownik[24], lecz nie wykluczono możliwości udzielenia zgody przez pracownika, jednak jedynie wtedy, gdy może uczynić to rzeczywiście dobrowolnie[25]. Prawodawca unijny w motywie 155 wprost dopuścił, by państwa członkowskie, na podstawie art. 88 RODO, przewidziały przypadki, w których wyrażenie zgody przez pracownika będzie dopuszczalne. Z możliwości tej skorzystał polski ustawodawca, wprowadzając do kodeksu pracy[26] w art. 22^{1a} regulację, na mocy której zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez pracodawcę, równocześnie formułując warunki jej dopuszczalności. Zgodnie z art. 22^{1a} § 2 k.p., aby zgoda pracownika była ważna i nie naruszała przesłanki dobrowolności, odmowa jej udzielenia oraz jej wycofanie nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę. Ponadto w przypadku przetwarzania danych osobowych szczególnych kategorii ważność zgody zależy dodatkowo od tego, czy inicjatywa przetwarzania tych danych przez pracodawcę pochodziła osoby ubiegającej się o zatrudnienie lub pracownika.

W doktrynie wskazuje się także, że przypadkiem braku równowagi stron, zaburzającym dobrowolność wyrażenia zgody, będzie legalizowanie przetwarzania danych w kontekście badań klinicznych[27]. Potwierdza to także EROD w opinii 3/2019 wskazując, że zależnie od okoliczności badania klinicznego może wystąpić brak równowagi sił między sponsorem/badaczem a uczestnikami, co może być związane

---

[23] *Ibidem*.

[24] Grupa Robocza Art. 29, *Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 (WP 259)*, 8, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849 [dostęp: 19.11.2021]. W zakresie relacji pracodawca – pracownik i braku stanu równowagi wypowiadał się także TSUE m.in. w wyrokach w połączonych sprawach C-379/01 do C-403/01, dopuszczając w kontekście prawa pracy możliwości swobodnego podejmowania w określonych przypadkach decyzji przez pracowników.

[25] Szerzej na temat zgody pracownika na przetwarzanie jego danych osobowych – zob. P. Zawadzka-Filipczyk [w:] E. Jagiełło-Jaroszewska, D. Jarmużek, P. Zawadzka-Filipczyk, *RODO. Ochrona danych osobowych w stosunkach pracy*, Warszawa 2018, s. 58 i n.; J. Czerniak-Swędzioł, K. Kulikowska [w:] *RODO. Ochrona danych osobowych w zatrudnieniu*, red. M. Mędrala, s. 173 i n.; M. Wujczyk [w:] *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, red. D. Dorre-Kolasa, s. 74; G. Sibiga, *Przetwarzanie i ochrona danych osoby ubiegającej się o zatrudnienie w świetle przepisów prawa pracy*, „Radca Prawny" 2005, nr 2, s. 70. Zob. także: P. Fajgielski, *Ogólne rozporządzenie*…, s. 127 i s. 128; M. Garwoński, M. Sztąberek [w:] *RODO. Przewodnik ze wzorami*, red. M. Gawroński, s. 84.

[26] Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (tekst jedn.: Dz. U. z 2020 r., poz. 1320 ze zm.).

[27] L.A. Bygrave, L. Tosoni [w:] Ch. Kuner, L.A. Bygrave, C. Docksey, *The EU General Data*…, s 182.

z okolicznościami dotyczącymi potencjalnego uczestnik badań, w tym np. jego sytuacji ekonomicznej, statusu społecznego, zależności instytucjonalnej lub hierarchicznej, która mogłaby w niewłaściwy sposób wpłynąć na jego decyzję o udziale (pkt 19)[28]. Z kolei w wytycznych 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19, podając przykład nieinterwencyjnego badania danej populacji, przeprowadzania na podstawie ankiet dotyczących objawów i postępu choroby, w którym przetwarzanie następowałoby na podstawie zgody uczestnika, EROD nie dostrzega „wyraźnego braku równowagi sił", o którym mowa w motywie 43, przy założeniu oczywiście, że podmiot danych nie był poddawany naciskom, ani nie grożono mu negatywnymi konsekwencjami, gdyby nie udzielił zgody[29].

Typowe naruszenia przesłanki dobrowolności, niezależne od braku równowagi stron, związane są z kolei np. z żądaniem administratora wyrażenia zgody przez podmiot danych na przetwarzanie jego danych w celu realizacji umowy czy też uzależnienie spełnienia świadczenia oznaczanego jako bezpłatne od wyrażenia zgody na informację handlową. W pierwszym przypadku naruszenie polega na sprzeczności z zasadą autonomiczności przesłanek legalizacyjnych, w takiej bowiem sytuacji zgoda nie będzie dobrowolna z uwagi na brak rzeczywistej możliwości jej cofnięcia, jako że nawet dokonanie tej czynności przez podmiot danych nie spowoduje zaprzestania przetwarzania przez administratora na podstawie przesłanki z art. 6 ust. 1 lit. b, a w drugim – z uwagi na sprzeczność wprost z powołanym już art. 7 ust. 4 RODO.

Zgody nie uważa się za dobrowolną, także jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne. Ten element przesłanki dobrowolności EROD określa jako szczegółowość, która odnosi się do zapewnienia podmiotom danych swoboda wyboru celu, który akceptują, zamiast obowiązku wyrażenia zgody na szereg celów przetwarzania jednocześnie[30]. Jeżeli administrator połączył kilka celów przetwarzania i nie zwrócił się o osobną zgodę na każdy z tych celów, podmiot danych zostaje pozbawiony swobody wyboru, a w konsekwencji nie jest spełniona przesłanka dobrowolności. Element szczegółowości jest ściśle związany również z przesłanką konkretności zgody, o czym w dalszej części artykułu.

Przesłanka dobrowolności zgody w tym kontekście analizowana była także w orzecznictwie sądów administracyjnych, wprawdzie w odniesieniu do dotychczasowego stanu prawnego, jednakże rozważania te zachowują swą aktualność. Między

[28] Opinia EROD nr 3/2019 w sprawie pytań i odpowiedzi dotyczących wzajemnych zależności między rozporządzeniem w sprawie badań klinicznych (RBK) a ogólnym rozporządzeniem o ochronie danych (RODO), (art. 70 ust. 1 lit. b), s. 6, https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_pl.pdf, [dostęp: 19.11.2021].

[29] Wytyczne 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19, s. 7, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_pl.pdf, [dostęp: 19.11.2021].

[30] Wytyczne 05/2020, s. 13.

innymi w orzeczeniu Naczelnego Sądu Administracyjnego, III OSK 161/21[31], stwierdzono, że na gruncie przepisów o ochronie danych osobowych istnieje wymóg zapewnienia, aby decyzja w sprawie wyrażenia zgody na przetwarzanie danych osobowych w określonym celu była podjęta swobodnie i miała charakter samodzielny, musi ona być przejawem wolnej i nieskrępowanej woli danej osoby, to znaczy nie może być wymuszona przez konieczność złożenia innych oświadczeń woli. Z tym założeniem konstrukcyjnym orzekający w sprawie sąd konfrontował zagadnienie łączenia zgód w różnych celach przetwarzania, w tym konkretnym przypadku w zakresie dotyczącym marketingu produktów i usług własnych administratora danych oraz produktów i usług innych nieokreślonych jednostkowo podmiotów. Rozważając przesłankę dobrowolności doszedł do wniosku, że tak łączone zgody nie pozwalają podmiotowi danych na podjęcie dobrowolnej decyzji, jako że nie ma w istocie wyboru poza wyborem ograniczającym się do opcji *take it or leave it*, który nie spełnia kryterium dobrowolności.

5. Konkretność zgody

Konkretność zgody odnosi się do celu i zakresu przetwarzania. Pozostaje w ścisłym związku z regulacją art. 6 ust. 1 lit. a i art. 9 ust. 2 lit. a RODO. Zgodnie z przywołanymi przepisami, podmiot danych musi mieć możliwość wyrażenia zgody „w jednym lub większej liczbie określonych celów" oraz przysługuje mu możliwość wyboru w odniesieniu do każdego z nich[32]. Zgoda zatem, aby była konkretna, musi określać w sposób zrozumiały, wyraźnie i precyzyjnie cel oraz zakres przetwarzania i pozwalać podmiotowi danych w ten sposób na kontrolę nad jego danymi[33]. Oznacza to, że wymóg ten nie będzie spełniony, jeśli zgoda nie będzie zawierać informacji na temat celu przetwarzania lub czynić to w sposób ogólny, blankietowy czy też odnosić się do otwartego zbioru czynności przetwarzania.

Wymóg konkretności nie ogranicza się tylko do wskazania celu przetwarzania, ale dotyczy także innych jego aspektów powiązanych z celem, w szczególności zakresu przetwarzania i zakresu danych, i pod tym względem jest powiązany z przesłanką świadomości zgody obejmującej m.in. skonkretyzowanie ram przetwarzania[34].

---

[31] Wyrok NSA z dnia 20 kwietnia 2021 r., III OSK 161/21, https://orzeczenia.nsa.gov.pl/doc/524FC93261 [dostęp: 19.11.2021].

[32] Wytyczne 05/2020, s. 14.

[33] Grupa Robocza Art. 29 wskazuje dodatkowo, że w zgodzie powinny być określone również konsekwencje przetwarzania – Grupa Robocza Art. 29, opinia 15/2011 w sprawie definicji zgody, przyjęta 13.07.2011 r. (WP 187), s. 18, http://www.giodo.gov.pl/pl/file/5341 [dostęp: 21.01.2018]. Zob. także: A. Mednis, *Cechy zgody na przetwarzanie danych osobowych w opinii Grupy Roboczej Art. 29 dyrektywy 95/46 Nr 15/2011 (WP 187)* [w:] *Aktualne problemy prawnej ochrony danych osobowych 2012*, red. G. Sibiga, M. Praw. 2012, nr 7 – dodatek, s. 26.

[34] D. Lubasz [w:] M. Jagielski, *Dokumentacja ochrony*…, Warszawa 2019, s. 203 i n.

Określoność celu jest jednak kluczowa i podkreślana w motywie 43 RODO, w tym nie tylko z perspektywy przesłanki dobrowolności, ale i konkretności zgody[35]. Zgodnie z przywołanym motywem, zgodę należy wyrażać z osobna nie tylko na różne cele, ale i na różne operacje przetwarzania. Z tego wymogu w wytycznych dotyczących zgody EROD wywodzi, że aby zapewnić zgodność, administrator musi zastosować:

- określenie celu jako zabezpieczenie przed zmianą celu co jest zgodne z realizacją zasady ograniczenia celu określone w art. 5 ust. 1 lit. b, która wyznacza pozostałe parametry przetwarzania;
- szczegółowość w zapytaniach o zgodę oraz
- wyraźne oddzielenie informacji związanych z uzyskaniem zgody na działania w zakresie przetwarzania danych od informacji dotyczących innych kwestii[36].

W odniesieniu do dwóch ostatnich zagadnień wymóg konkretności zgody pozostaje w bliskiej korelacji z wymogiem świadomej zgody, a także elementem dobrowolności zgody, jakim jest jej szczegółowość.

Przesłanka konkretności zgody była przedmiotem analizy TSUE w wyroku *Planet49* C-673/17, w którym trybunał podkreślił, że przesłanka konkretności na gruncie analogicznej definicji pojęcia zgody w art. 2 lit. h dyrektywy 95/46/WE, oznacza, że zgoda odnosić się musi do określonego przetwarzania danych i nie może zostać wywnioskowane z treści wyrażenia woli mającego inny cel (pkt 58).

6. Świadomość zgody

Oświadczenie o wyrażeniu zgody musi być świadome. Świadomość zgody jest nierozerwalnie związana z przejrzystością przetwarzania, będącą zasadą przetwarzania danych, o której mowa w art. 5 ust. 1 lit. a RODO[37].

W przypadku zgody, realizacja zasady przejrzystości nakierowana jest przede wszystkim na zapewnienie podmiotom danych jak najpełniejszej kontroli nad danymi, przez zapewnienie wiedzy na temat celu, zakresu i kontekstu przetwarzania danych. Elementy te są niezbędne do umożliwienia im podejmowania świadomych decyzji, zrozumienia, na co wyrażają zgodę oraz wykonania prawa wycofania zgody[38].

Wyraźnie podkreślono to w motywie 39, zgodnie z którym celem regulacji jest zapewnienie osobie, której dane dotyczą, transparentności w zakresie tego, że jej dane

---

[35] Zob. także motyw 32 RODO, zgodnie z którym jeżeli przetwarzanie ma służyć różnym celom, potrzebna jest zgoda na każdy z tych celów. Związane to jest także z realizacją zasady ograniczonego celu z art. 5 ust. 1 lit. b RODO, zgodnie z którą dane muszą być „zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami". Na temat znaczenia ograniczonego celu pod kątem możliwości łączenia w oświadczeniu o zgodzie różnych celów zob. D. Lubasz [w:] *RODO*…, s. 357.

[36] Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 (WP 259), s. 14.

[37] Szerzej na temat zasady przejrzystego informowania, zob. J. Łuczak [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 406 i n.

[38] Wytyczne 05/2020, s. 16.

osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. A zatem w celu zapewnienia podmiotowi danych świadomości w zakresie zgody administrator w chwili zwracania się o zgodę powinien przedstawić wszystkie niezbędne informacje o istotnych aspektach przetwarzania. Występuje tu więc oczywista korelacja z obowiązkami informacyjnymi sprecyzowanymi w art. 13 RODO[39].

Jak wynika z motywu 42 RODO, że aby wyrażenie zgody było świadome, podmiot danych powinien znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych[40]. W konkretnych przypadkach może być jednak wymagane podanie więcej informacji, aby umożliwić podmiotowi danych zrozumienie istoty przetwarzania[41], i w tym zakresie istotnie następuje korelacja z wymogami informacyjnymi z art. 13 lub 14 RODO.

Europejska Rada Ochrony Danych w wytycznych dotyczących zgody sformułowała minimalne wymogi zapewniające świadomość zgody obejmujące obowiązek podania następujących informacji:

1) tożsamości administratora;
2) celu każdej operacji przetwarzania, w odniesieniu do której prosi się o zgodę;
3) o zakresie danych, które będą gromadzone i wykorzystywane;
4) o prawie do wycofania zgody;
5) dotyczących wykorzystywania danych do celów zautomatyzowanego podejmowania decyzji zgodnie z art. 22 ust. 2 lit. c w stosownych przypadkach; oraz
6) dotyczących możliwych zagrożeń związanych z przekazywaniem danych w związku z brakiem decyzji stwierdzającej odpowiedni stopień ochrony oraz odpowiednich zabezpieczeń, zgodnie z art. 46[42].

Warto jednak podkreślić, że powyższe informacje nie muszą znaleźć się w samej formule zgody lub zapytaniu o nią, lecz muszą być przekazane w trakcie procedury pozyskiwania danych i odbierania zgody w sposób towarzyszący tej procedurze w sposób jasny, zrozumiały i dostępny dla podmiotu danych.

W przepisach rozporządzenia nie określono wprawdzie formy przekazywania informacji ani ich kształtu w celu spełnienia wymogu świadomej zgody. Oznacza to, że ważne informacje mogą być przekazane na różne sposoby, np. w formie pisemnych lub ustnych oświadczeń bądź wiadomości dźwiękowych lub wiadomości wideo.

---

[39] Wykonywanie obowiązków informacyjnych nie daje jednak gwarancji pełnej świadomości, zwłaszcza w przypadkach, gdy administrator występuje o zgodę w związku z rozszerzeniem celów przetwarzania, a pozostałych obowiązków już nie realizuje. Stanowisko takie, w szczególności wobec braku wyrażonej *expressis verbis* w ustawie o ochronie danych osobowych przesłanki świadomości w definicji zgody, prezentował A. Mednis [w:] *idem*, *Cechy*…, s. 27.

[40] Brytyjski Information Commissioner's Office wskazuje, że minimalny standard powinien obejmować również informację o prawie do odwołania zgody w każdym czasie; zob. projekt wytycznych Information Commissioner's Office, *Consultation: GDPR consent guidance*, s. 22, https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf [dostęp: 19.11.2021].

[41] Grupa Robocza Art. 29, *Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679*…, s. 14.

[42] Wytyczne 05/2020, s. 16–17.

W przepisie art. 7 ust. 2 oraz pomocniczo w motywie 42 RODO sformułowano natomiast wymogi dotyczące świadomej zgody, co miało zapewnić wyższy standard jasności i dostępności informacji[43]. Standard jakości informacji odnosi się do sposobu przedstawienia informacji (w postaci zwykłego, zrozumiałego, widocznego tekstu, bez żargonu); sposób ten zależy od kontekstu, przy czym informacje muszą być zrozumiałe dla przeciętnego użytkownika. Standard dostępności z kolei nakierowany jest na odpowiednią widoczność informacji i ich kompleksowość[44]. W przywołanym motywie wskazano na występującą korelację z dyrektywą 93/13/EWG[45], i w tym zakresie formułując wymogi, by oświadczenie o wyrażeniu zgody przygotowane przez administratora miało zrozumiałą i łatwo dostępną formę, było sformułowane jasnym i prostym językiem i nie zawierało nieuczciwych warunków.

6. Jednoznaczność zgody

Regulacją dotyczącą przesłanki jednoznaczności zgody na gruncie rozporządzenia ogólnego wprowadza się najdalej idącą zmianę w stosunku do dotychczasowego stanu prawnego.

W myśl definicji pojęcia zgody, jak stanowi art. 4 pkt 11 RODO, jednoznaczność zgody powiązana została ze sposobami wyrażania woli, a zatem z jednej strony – z oświadczeniem, z drugiej zaś – z wyraźnym działaniem potwierdzającym. Jak podkreśla się nadto w motywie 32 RODO, „zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia".

Przesłanka jednoznaczności jest cechą okazania woli przesądzającą, że w konkretnej sytuacji udzielania zgody nie może powstawać wątpliwość co do intencji osoby ją wyrażającej. Oznacza to, że zachowanie danej osoby wyrażającej przyzwolenie na przetwarzanie musi niedwuznacznie określać jej zamiar. Akceptacja przez prawodawcę unijnego działań konkludentnych jako skutecznej zgody, nie zmniejsza istoty tego wymogu. Zarówno w przypadku okazania woli w formie oświadczenia, jak i wyraźnego działania potwierdzającego nie może być mowy o wątpliwościach co do intencji podmiotu danych. Okazanie woli musi być świadomie aktywnym działaniem podmiotu danych i odrębnym od innych czynności, w tym np. zawierania umowy, przyjmowania oferty czy akceptacji regulaminu[46].

---

[43] Wytyczne 05/2020, s. 17.

[44] A. Mednis, *Cechy*…, s. 27.

[45] Dyrektywa Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (Dz. Urz. L 95, s. 29).

[46] D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*…, s. 256.

7. Dodatkowe wymogi zgody w przypadkach szczególnych

W art. 9 ust. 2 lit. a RODO dotyczącym zgody jako przesłanki legalizacyjnej przetwarzania szczególnych kategorii danych, w art. 22 ust. 1 w zw. z ust. 2 lit. c RODO, przy dopuszczeniu zautomatyzowanego podejmowania decyzji w stosunku do podmiotu danych, w tym profilowania, a także w art. 49 ust. 1 lit. a RODO, przy legitymizowaniu transferu danych do państwa trzeciego, prawodawca unijny, kierując się potrzebą zapewniania podwyższonego standardu ochronnego, sformułował dodatkowy wymóg zgody, jakim jest jej wyraźny charakter.

Wyraźność zgody nie jest zatem wymogiem o charakterze ogólnym, i została ograniczona do przypadków szczególnych, wymagających szczególnej ochrony i zapewnienia rozliczalności.

W tych wypadkach nie jest dozwolone kwalifikowanie jako zgody wyraźnego działania potwierdzającego. Termin „wyraźna" jako element zgody odnosi się do sposobu, w jaki zgoda ma być wyrażana przez osobę, której dane dotyczą. Oznacza to, że podmiot danych musi wyrazić oświadczenie zgody i nie może mieć ono formy działania konkludentnego[47]. Stanowisko to potwierdza EROD w wytycznych 05/2020 dotyczących zgody[48]. Do zachowania określonego w ten sposób podwyższonego standardu zgody niezbędne jest zatem okazanie woli poprzez złożenie oświadczenia sformułowanego z użyciem słów[49]. W dalszym ciągu nie ma jednak znaczenia forma takiego oświadczenia. Może być ono sformułowane pisemnie, w formie dokumentowej lub ustnie, aczkolwiek zarówno Grupa Robocza Art. 29, jak i EROD, ze względów dowodowych sugeruje nieograniczanie się przez administratorów do formy ustnej odbierania takiej zgody[50]. Jednocześnie jednak EROD wskazuje, że możliwe jest odebranie wyraźnej zgody podczas rozmowy telefonicznej, pod warunkiem że informacje dotyczące wyboru są uczciwe, zrozumiałe i jasne, i że administrator zwraca się do podmiotu danych o konkretne potwierdzenie (np. naciśniecie przycisku lub ustne potwierdzenie)[51], co ma być gwarancją aktywnej zgodny. W kontekście dowodowym natomiast środkami zapewniającymi rozliczalność mogłyby być w tym wypadku logi lub nagranie samej rozmowy.

W kontekście cyfrowym z kolei forma ustna jest mało użyteczna i może zostać zastąpiona elektronicznym formularzem, wiadomością e-mail czy skanem oświadczenia[52]. Zapewnienie wyraźności zgody może również zapewniać procedura *double opt-in* w komunikacji z wykorzystaniem poczty elektronicznej.

---

47 Grupa Robocza Art. 29, *Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679*…, s. 23.

48 Wytyczne 05/2020, s. 22.

49 Analogiczne stanowisko zajmuje brytyjski Information Commissioner's Office w projekcie wytycznych dotyczących zgody – https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf [dostęp: 19.11.2021].

50 Grupa Robocza Art. 29, *Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679*…, s. 23; wytyczne 05/2020, s. 22 i 23.

51 Wytyczne 05/2020, s. 23

52 Grupa Robocza Art. 29, *Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679*…, s. 24.

8. Dodatkowe wymogi dotyczące zgody pisemnej

W art. 7 ust. 2 RODO sformułowane zostały dodatkowe wymogi dotyczące zgody udzielanej w formie pisemnej, która stanowi autonomiczne pojęcie prawa unijnego. W zakres tego pojęcia wchodzą zarówno przypadki obejmujące formę pisemną w rozumieniu kodeksu cywilnego, czyli formę, w której utrwalone oświadczenie opatrzone jest podpisem własnoręcznym, jak i formę bliską formie tekstowej z niemieckiego kodeksu cywilnego (por. art. 126b BGB). W tym kontekście warto zauważyć, że rozporządzenie 2016/679 zrównuje w pewnym sensie formę pisemną z formą elektroniczną, wymieniając tę ostatnią jako podtyp formy pisemnej (zob. art. 28 ust. 9, art. 30 ust. 3 RODO).

Wynikające z art. 7 ust. 2 RODO wymogi dotyczące pisemnego, w rozumieniu rozporządzenia, zapytania, a w konsekwencji i samej zgody, stanowią wyraźne ujęcie zasady przejrzystości i wskazanie określonego sposobu komunikacji pomiędzy administratorem a podmiotem danych. Administrator, uwzględniając wymaganie zrozumiałej formy oraz użycia jasnego i prostego języka, powinien formułować zapytanie lub oświadczenie w sposób prosty semantycznie i jednoznaczny, a użycie pojęć technicznych ograniczyć do sytuacji, w których jest to niezbędne, tak aby komunikat został zrozumiany zgodnie z jego wolą przez odbiorcę. Jest to standard jasności komunikacji wyznaczony regulacją dyrektywy 93/13/EWG, na co wskazuje motyw 42. Ocena zatem, czy forma komunikatu jest zrozumiała, dokonywana jest przez pryzmat podmiotów, które mają udzielić zgody. Inne wymogi w tym zakresie będą formułowane, jeśli odbiorcą mają być dzieci, inaczej będzie w przypadku osób starszych, a jeszcze inaczej – specjalistów z danej dziedziny.

Szczegółowe wymogi dla pisemnej w rozumieniu art. 7 ust. 2 RODO zgody, nie oznaczają oczywiście, że oświadczenia, w innej formie niż pisemna, nie muszą być sformułowane w zrozumiałej formie, jasnym i prostym językiem. Wymogi w tym zakresie wynikają bowiem z przesłanki świadomości zgody oraz zasady przejrzystości uregulowanej w art. 5 ust. 1 lit. a RODO.

Na mocy przepisu art. 7 ust. 2 RODO zapytanie o zgodę, a także samo oświadczenie, musi zostać ponadto przedstawione „w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii". Wymóg ten nie tworzy jednak dodatkowej jakości normatywnej, jako że odseparowanie zgody od innych treści, wywodzone jest już z samej definicji pojęcia zgody[53].

[53] Zob. przykładowo opinię rzecznika generalnego M. Szpunara w sprawie C-673/17 *Planet49*, pkt 68 i n., https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX:62017CC0673 [dostęp: 29.11.2021].

9. Forma zgody

Jako że jednym z celów rozporządzenia było odformalizowanie i zniesienie zbędnych obciążeń administracyjnych, konsekwentnie w zakresie zgody nie zostały sformułowane wymogi co do formy i wybór jej dotyczący został pozostawiony administratorom, którzy kierować się muszą wynikającą art. 5 ust. 2 zasadą rozliczalności, nakładającą na nich obowiązek wykazania zgodności, także co do legalizacji procesów przetwarzania danych. W przypadku zgody, obowiązek wykazania rozliczalności dodatkowo *expressis verbis* sformułowany został w art. 7 ust. 1 stanowiącym, że jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

Brak wymogów co do formy zgody wynika także z faktu, że oprócz oświadczenia w ogólnym rozporządzeniu o ochronie danych, dopuszcza się również udzielenie zgody w postaci wyraźnego działania potwierdzającego[54], czyli poprzez działania konkludentne[55], co z natury jest działaniem odformalizowanym.

10. Ciężar dowodu – rozliczalność

Z odformalizowaniem zgody jako przesłanki legalizacyjnej wiąże się, jak już wskazano, przeniesienie ciężaru na kwestie rozliczalności, a zatem wykazania przez administratora, że podmiot danych udzielił mu przyzwolenia na przetwarzanie jego danych osobowych. Podkreśla to prawodawca unijny w motywie 42, zaznaczając, że jeżeli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania. W szczególności w przypadku pisemnego oświadczenia składanego w innej sprawie powinny istnieć gwarancje, że osoba, której dane dotyczą, jest świadoma wyrażenia zgody oraz jej zakresu.

Rozliczalność zgody dotyczy zarówno samego faktu jej udzielenia, jak i poszczególnych jej elementów, tj. dobrowolności, konkretności, świadomości i jednoznaczności. Szczególną rolę pełni sposób sformułowania zapytania i oświadczenia o zgodzie oraz zakres informacji przekazywanych przy tej okazji przez administratora, które mają zapewnić pełną swobodę decyzyjną podmiotu danych.

---

[54] Na temat wyraźnego działania potwierdzającego zob. szerzej D. Lubasz [w:] *RODO*…, komentarz do art. 4 pkt 11, nt 26.

[55] Stanowisko takie wyrażane było zwłaszcza w polskiej doktrynie prawa i orzecznictwie – zob. P. Barta, P. Litwiński, *Ustawa*…, komentarz do art. 23, nt 7; J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona*…, s. 485; wyrok NSA z dnia 4 kwietnia 2003 r., II SA 2135/02, „Wokanda" 2004, nr 6, s. 30; B. Kaczmarek-Templin, *Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych – wybrane zagadnienia* [w:] *Polska i europejska reforma ochrony danych osobowych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016, s. 104–105. Szerzej na ten temat zob. D. Lubasz [w:] *RODO*…, komentarz do art. 4 pkt 11, nt 27.

Dostrzegając wagę zagadnienia rozliczalności w zakresie dotyczącym zgody, w art. 7 ust. 1, w uzupełnieniu zasady rozliczalności przewidzianej w art. 5 ust. 2 RODO, nałożono na administratorów wyraźny obowiązek wykazania, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. O ile zatem uelastyczniono sposób zbierania zgód oraz nie narzucono określonej formy dla oświadczenia o zgodzie[56], o tyle wybierając określony model pozyskiwania zgód, administrator musi jednak pamiętać o utrwaleniu faktu uzyskania przyzwolenia podmiotu danych w celu wykazania, w szczególności przed organem nadzorczym, ale też przed samym podmiotem danych, że otrzymał zgodę na przetwarzanie danych osobowych.

Jak podkreśla Grupa Robocza Art. 29 oraz EROD, administratorzy mają swobodę opracowywania metod zapewnienia zgodności z tym wymogiem rozliczalności, a zatem doboru sposobów wykazania uzyskania zgody podmiotu danych[57]. Kluczowe jest przy tym jednak, by obowiązek wykazania, że zgoda została uzyskana przez administratora w sposób ważny, nie powinien sam w sobie prowadzić do nadmiernego dodatkowego przetwarzania danych. Oznacza to, że administratorzy, kierując się wymogami *data protection by design*[58] oraz zasadą minimalizacji danych, powinni zachowywać tylko taką ilość danych, aby móc wykazać zgodność, ale nie powinni gromadzić więcej danych niż to konieczne[59]. Obowiązek dowodowy trwa, zgodnie ze stanowiskiem EROD, dopóty istnieje obowiązek wykazania prawidłowo wyrażonej zgody. Po zakończeniu czynności przetwarzania dowód na wyrażenie zgody nie powinien być przechowywany dłużej niż jest to bezwzględnie konieczne do wywiązania się z prawnego obowiązku lub do ustalenia, dochodzenia lub obrony roszczeń, zgodnie z art. 17 ust. 3 lit. b i e RODO[60].

11. Wycofanie zgody

Ocena ważności wyrażenia zgody, jako autonomicznej decyzji podmiotów danych dotyczącej dozwolenia na przetwarzanie ich danych osobowych, związana jest nie tylko z procesem jej udzielania, ale także jej odwoływalnością bez niekorzystnych konsekwencji[61].

---

[56] Zob. szerzej: D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*…, s. 257.

[57] Grupa Robocza Art. 29, *Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679*…, s. 25; wytyczne 05/2020, s. 24.

[58] Zobacz szerzej wymogi art. 25 ust. 1 RODO.

[59] Grupa Robocza Art. 29, *Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679*…, s. 25.. Przykładowo, administrator może prowadzić rejestr oświadczeń o wyrażeniu zgody, aby móc wykazać, w jaki sposób uzyskano zgodę, kiedy uzyskano zgodę i jakie informacje przekazano osobie, której dane dotyczą, w momencie uzyskania zgody. Jako na niewystarczające z kolei wskazuje grupa robocza ograniczenie się administratora do informacji o konfiguracji strony WWW, jeśli za jej pośrednictwem zbierane są zgody, bez utrwalenia informacji o konkretnym procesie jej udzielenia.

[60] Wytyczne 05/2020, s. 24.

[61] Zob. Grupa Robocza Art. 29, *Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679*…, s. 7; a także motywy 42, 43 RODO oraz opinia 15/2011 w sprawie definicji zgody (WP187), s. 12.

Uprawnienie do wycofania zgody uregulowane zostało w art. 7 ust. 3 RODO, zgodnie z którym podmiot danych ma nie tylko prawo w dowolnym momencie wycofać zgodę, co nie powinno wpływać na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem, ale także musi być o tym informowany, zanim wyrazi zgodę. W ten sposób skodyfikowane zostały wytyczne Grupy Roboczej Art. 29, zawarte w opinii 15/2011.

Ponadto, prawodawca unijny wprowadził wymóg, który określa, że wycofanie zgody musi być równie łatwe jak jej wyrażenie, choć nie przesądza, że ma to następować w ten sam sposób co udzielenie zgody. Jak podkreśla jednak EROD w wytycznych 5/2020 dotyczących zgody, tam, gdzie zgoda jest uzyskiwana za pomocą interfejsu użytkownika specyficznego dla danej usługi za pośrednictwem strony internetowej, witryny aplikacji, konta logowania, interfejsu urządzenia IoT (*Internet of Things*) lub za pomocą e-maila, nie ma wątpliwości, że osoba, której dane dotyczą, musi mieć możliwość wycofania zgody za pośrednictwem tego samego interfejsu elektronicznego, gdyż przejście na inny interfejs, jedynie w celu wycofania zgody, wymagałoby zbędnego wysiłku[62].

Warto jednocześnie zwrócić uwagę, że z łatwością wycofywania zgody łączony jest wymóg, by wycofanie zgody następowało bez uszczerbku dla podmiotu danych. Oznacza to w szczególności, że administrator musi umożliwić wycofanie zgody bezpłatnie lub bez obniżenia poziomu usługi[63].

Polski ustawodawca zdecydował się na dodatkowe podkreślenie tego wymogu w kontekście pracowniczym w art. 22^{1a} § 2 k.p. Stanowi on, że aby zgoda pracownika była ważna i nie naruszała przesłanki dobrowolności, odmowa jej udzielenia oraz jej wycofanie nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę.

Konsekwencją wycofania zgody jest co do zasady obowiązek usunięcia danych przez administratora, przy założeniu nie ma innych celów uzasadniających dalsze ich przechowywanie, które są realizowane na odrębnej podstawie prawnej. Naruszenie tego obowiązku aktualizuje podmiotowi danych prawo żądania usunięcia danych na podstawie art. 17 ust. 1 lit. a, jedynie poza sytuacją, którą przewidziano w art. 17 ust. 1 lit. b RODO.

Zapewnienie odwoływalności zgody jest wymogiem konstrukcyjnym systemu ochrony danych osobowych w rozumieniu art. 24 RODO w związku z wymogami przejrzystości z art. 5 ust. 1 lit. a i z art. 12 RODO. Zobowiązanie administratora do ułatwiania realizacji praw podmiotów danych na podstawie art. 12 ust. 2 RODO rozciąga się bowiem również na uprawnienie podmiotów danych z art. 7 ust. 3 RODO. Aspekty te pokreślone zostały w decyzji Prezesa UODO z dnia 16 października 2019 r.

---

62 Grupa Robocza Art. 29, *Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679*…, s. 9.

63 *Ibidem*, s. 10.

ZSPR.421.7.2019, w której podstawą nałożenia administracyjnej kary pieniężnej było m.in. niewdrożenie odpowiednich środków technicznych i organizacyjnych, które umożliwiałyby podmiotowi danych łatwe i skuteczne wycofanie zgody na przetwarzanie swoich danych osobowych oraz realizację prawa do żądania niezwłocznego usunięcia swoich danych osobowych.

Literatura

Bielak-Jomaa E., Lubasz D., *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016.

Bielak-Jomaa E., Lubasz D., *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Czerniak-Swędzioł J., Kulikowska K., *Zgoda na przetwarzanie danych osobowych pracownika* [w:] *RODO. Ochrona danych osobowych w zatrudnieniu*, red. M. Mędrala, Warszawa 2018.

Doerre-Kolasa D., *Pozyskiwanie danych osobowych osoby ubiegającej się o zatrudnienie i pracownika na podstawie przepisów KP* [w:] *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, red. *eadem*, Warszawa 2020.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Gawroński M., *RODO. Przewodnik ze wzorami*, Warszawa 2018.

Jagielski M., *Dokumentacja ochrony danych osobowych ze wzorami*, Warszawa 2019.

Jagiełło-Jaroszewska E., Jarmużek D., Zawadzka-Filipczyk P., *RODO. Ochrona danych osobowych w stosunkach pracy*, Warszawa 2018.

Kaczmarek-Templin B., *Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych – wybrane zagadnienia* [w:] E. Bielak-Jomaa, D. Lubasz, *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016.

Litwiński P., Barta P., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016.

Litwiński P., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Legalis.

Lubasz D., Sęczkowski D., *Nowe europejskie przepisy o ochronie danych osobowych – przygotowania do wdrożenia czas zacząć*, „Compliance. Magazyn Fachowy Instytutu Compliance" 2016, nr 3.

Mednis A., *Cechy zgody na przetwarzanie danych osobowych w opinii Grupy Roboczej Art. 29 dyrektywy 95/46 Nr 15/2011 (WP 187)* [w:] G. Sibiga, *Aktualne problemy prawnej ochrony danych osobowych 2012*, M. Praw. 2012, nr 7 – dodatek.

Mednis A., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2001.

Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, red. P. Litwiński, Warszawa 2021.

RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. D. Lubasz, E. Bielak-Jomaa, Warszawa 2018.

Sibiga G., Przetwarzanie i ochrona danych osoby ubiegającej się o zatrudnienie w świetle przepisów prawa pracy, „Radca Prawny" 2005, nr 2.

The EU General Data Protection Regulation (GDPR). A Commentary, red. Ch. Kuner, L.A. Bygrave, Ch. Docksey, Oksford 2020.

Streszczenie

Dominik Lubasz

Warunki wyrażania zgody jako przesłanki legalizującej przetwarzanie danych osobowych

Zgoda podmiotu danych jest jedną z przesłanek legalizacyjnych przetwarzania danych. Koncepcja zgody w rozporządzeniu 2016/679 zachowała zasadniczą konstrukcję regulacyjną, przyjętą uprzednio w dyrektywie 95/45/WE, opartą na autonomii podmiotu danych, jej aktywnym działaniu oraz odwracalności decyzji o wyrażeniu zgody, jednakże uległa również pewnemu uelastycznieniu. W artykule poddane zostają analizie zarówno warunki skutecznego wyrażenia zgody, dodatkowe wymogi w sytuacjach szczególnych, jak również interakcje pomiędzy regulacją dotyczącą zgody a innymi obowiązkami nakładanymi na administratorów, w tym w szczególności w zakresie dotyczącym transparentności przetwarzania.

Słowa kluczowe: zgoda; przesłanki legalizacyjne; dobrowolność zgody; świadomość zgody; konkretność zgody; jednoznaczność zgody; wyraźne działania potwierdzające; wycofanie zgody; forma zgody; rozliczalność; RODO.

Summary

Dominik Lubasz

Conditions of Consent as a Legal Basis for Processing of Personal Data

The consent of the data subject is one of the legal basis for data processing. The concept of consent in Regulation 2016/679 has retained the basic regulatory design previously adopted in Directive 95/45/EC, based on the autonomy of the data subject, his or her active action and the revocability of the consent, but it has also been made somewhat more flexible. The article analyses the conditions for valid consent, additional requirements in specific situations, as well as the relation between the regulation of consent and other obligations imposed on controllers, including in particular as regards the transparency of processing.

Keywords: consent; lawfulness of processing; voluntariness of consent; awareness of consent; concreteness of consent; unambiguity of consent; clear affirmative action; withdrawal of consent; form of consent; accountability; GDPR.

Grzegorz Sibiga
Instytut Nauk Prawnych Polskiej Akademii Nauk
gsibiga@inp.pan.pl
ORCID: 0000-0002-4721-8272

https://doi.org/10.26881/gsp.2021.4.05

Publiczna dostępność na podstawie przepisów o dostępie do informacji publicznej informacji i dokumentów dotyczących stosowania RODO przez administratora w orzecznictwie sądów administracyjnych

Wprowadzenie

Zagadnienie powszechnej (publicznej) dostępności, czy jeszcze szerzej – transparentności – informacji i dokumentów dotyczących stosowania ogólnego rozporządzenia o ochronie danych (RODO)[1], czyli materialnych efektów tego procesu, ma co najmniej dwa wymiary normatywne. Pierwszy z nich jest wpisany w samo RODO, ponieważ zawiera ono – poza uprawnieniami podmiotów danych i obowiązkami administratora związanymi z transparentnością przetwarzania danych osobowych konkretnych osób fizycznych (art. 12 ust. 1, art. 13–15) – także wymagania wobec administratora upublicznienia informacji o stosowaniu RODO lub przynajmniej przekazania określonych informacji podmiotom danych, co też może nastąpić poprzez ich publikację. Przykładowo, można wskazać, że do pierwszej grupy zalicza się obowiązek administratora (podmiotu przetwarzającego) publikacji danych kontaktowych inspektora ochrony danych (art. 37 ust.7 RODO). Natomiast do drugiej grupy – obowiązek współadministratorów przekazania osobom, których dane dotyczą zasadniczej treści uzgodnień między nimi (art. 26 ust. 2 zdanie drugie RODO), który zdarza się, że jest również realizowany poprzez zamieszczenie tych uzgodnień w serwisach internetowych współadministratorów[2], a niektórzy z nich decydują się nawet na ujawnienie w ten sposób pełnej treści uzgodnień[3].

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1).

[2] Zob. np. „Treść zasadniczych uzgodnień pomiędzy Współadministratorami w ramach akcji »Enea Akademia Talentów« z dnia 21.08.2019 r.", https://www.enea.pl/akademia-talentow/tresc-zasadniczych-uzgodnien-miedzy-wspoladministratorami.pdf [dostęp: 26.06.2021].

[3] Np. uzgodnienia w „grupie kapitałowej EXTREGO": „Uzgodnienia między współadministratorami", https://www.extrego.com/uzgodnienie-pomiedzy-wspoladministratorami [dostęp: 26.06.2021].

Drugi wymiar normatywny tworzą przepisy prawa, w których przewiduje się jawność działalności podmiotów wykonujących zadania publiczne i związane z tym powszechne prawo dostępu do informacji (ewentualnie prawo do dokumentów) dotyczących takiej działalności. Obszar ten nie podlega prawnej harmonizacji w Unii Europejskiej, ponieważ w art. 15 TFUE[4] ustanawia się jedynie zasady otwartości i dostępu do dokumentów, odnoszące się do instytucji, organów i jednostek organizacyjnych Unii Europejskiej[5]. Z tego względu o zakresie powszechnego prawa do informacji i jego realizacji decydują przepisy krajowe i ich stosowanie, a nawet pewna tradycja i specyficzne lokalne uwarunkowania, co zresztą pokazują podane poniżej przykłady. Na specyfikę krajową w tym obszarze składa się także orzecznictwo sądów, które kontrolują w sprawach indywidualnych działalność podmiotów zobowiązanych do udostępniania informacji (w Polsce dotyczy to spraw z wniosków o udostępnienie informacji publicznej).

W Polsce prawo do informacji o działalności podmiotów wykonujących władzę publiczną oraz o osobach pełniących funkcję publiczną zostało zagwarantowane w art. 61 Konstytucji RP[6], a na poziomie ustaw zwykłych – przede wszystkim w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej[7]. Ustawa obejmuje swoim zakresem podmiotowym władze publiczne i szeroki katalog innych podmiotów realizujących zadania publiczne (np. organy samorządów gospodarczych i zawodowych oraz osoby prawne, w których Skarb Państwa lub jednostki samorządu terytorialnego mają pozycję dominującą w rozumieniu przepisów o ochronie konkurencji i konsumentów), jak również partie polityczne i reprezentatywne organizacje związkowe i pracodawców (art. 4 ust.1–2 u.d.i.p.). Ustawowe prawo do informacji publicznej przyznano zaś każdemu, bez możliwości uzależnienia wykonywania tego prawa od wykazania przez korzystającego z niego interesu prawnego lub faktycznego (art. 2 u.d.i.p.).

Odnosząc powyższy wstęp do stosowania RODO, to jak wynika z orzecznictwa sądów administracyjnych w praktyce, okazuje się, że sporo osób zainteresowanych korzysta z przepisów o dostępie do informacji publicznej, aby żądać od administratorów informacji o zastosowaniu RODO, a głównie dokumentów będących materialnymi przejawami wykonywania tego aktu. Wnioski są kierowane do tych administratorów, którzy jednocześnie objęci są zakresem podmiotowym ustawy o dostępie do informacji publicznej. Sądy administracyjne właściwe w sprawach dostępu do informacji publicznej musiały w konkretnych sprawach udzielić odpowiedzi, czy informacje i dokumenty będące wynikiem stosowania RODO są w ogóle objęte zakresem przedmiotowym przepisów o dostępie do informacji publicznej oraz czy informacje (dokumenty) w tym względzie korzystają z prawnej ochrony ich poufności. W niniejszym tekście

---

[4] Wersja skonsolidowana Traktatu o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 326 z 2012 r., s. 47).

[5] K. Kowalik-Bańczyk, *Komentarz do art. 255 TWE* [w:] *Traktat Ustanawiający Wspólnotę Europejską. Komentarz*, t. 3, red. D. Kornobis-Romanowska, J. Łacny, Warszawa 2009, s. 683.

[6] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483).

[7] Dz. U. z 2020 r., poz. 2176; dalej: u.d.i.p.

przedstawiam orzecznictwo sądów administracyjnych w tym zakresie oraz formułuję wnioski z niego wynikające.

Informacja publiczna jako kryterium stosowania przepisów o dostępie do informacji publicznej

Ustalenia dotyczące informacji publicznej mają kluczowe znaczenie, ponieważ pojęcie to wyznacza przedmiotowy zakres stosowana ustawy o dostępie do informacji publicznej (art. 1 ust.1 u.d.i.p.). Do udostępnienia zaś takiej informacji zobowiązane są wszystkie podmioty objęte mocą ustawy (w tym także administratorzy w rozumieniu art. 4 pkt 7 RODO), które znajdują się w posiadaniu takiej informacji (art. 4 ust. 3 u.d.i.p.), co oznacza potrzebę istnienia zmaterializowanej postaci takiej informacji, w praktyce – wcześniejszego utrwalenia informacji[8].

Problem kwalifikowania materialnych przejawów stosowania RODO przez administratora podlegającego przepisom o dostępie do informacji publicznej wpisuje się w dotychczasowe sprawy sporne (sądowe) oraz dyskusję (w doktrynie) w przedmiocie zakresu znaczeniowego pojęcia „informacja publiczna", które trwają właściwie od początku obowiązywania ustawy o dostępie do informacji publicznej, tj. od 1 stycznia 2002 r.

Zakres znaczeniowy tego pojęcia ustalany jest na podstawie art. 1 ust. 1 u.d.i.p., zgodnie z którym informacją publiczną jest każda informacja o sprawach publicznych. W orzecznictwie podkreśla się, że granice informacji publicznej należy określać poprzez trzy przesłanki, których łączne wystąpienie wskazuje, że dana informacja jest informacją publiczną. Po pierwsze, sprawa musi dotyczyć informacji rozumianej jako pewna wiadomość dotycząca faktów; wnioskiem o udostępnienie może być objęte jedynie pytanie o określone fakty, o stan określonych zjawisk na dzień udzielania odpowiedzi. Faktem jest każda czynność i każde zachowanie organu wykonującego zadania publiczne podjęte w zakresie wykonywania takiego zadania. Fakt dotyczy zatem konkretnego zdarzenia lub czynności wykonanej przez podmiot zobowiązany do udzielenia informacji publicznej. Po wtóre, informacja powinna istnieć i znajdować się w posiadaniu podmiotu zobowiązanego do jej udzielenia. Wreszcie po trzecie informacja powinna dotyczyć spraw publicznych, o których mowa w art. 1 ust. 1 u.d.i.p., które definiuje się, jako każde działanie władzy publicznej w zakresie zadań stawianych państwu dotyczących lub służących ogółowi albo mających na celu zadysponowanie majątkiem publicznym. Desygnatem jest więc tu publicznoprawny charakter działalności danego podmiotu. Na pojęcie sprawy publicznej, o której ma być udzielona informacja publiczna, składa się więc przede wszystkim charakter publiczny zadań

[8] M. Pawełczyk, R. Stankiewicz, *Zmaterializowana forma* informacji *jako jeden z podstawowych elementów definicj*i informacji publicznej, „Radca Prawny" 2012, nr 132, s. 2D i n., a także orzecznictwo tam przywołane.

wykonywanych przez określony podmiot. Zatem tam, gdzie występuje aktywność organów publicznych, mamy do czynienia z informacją publiczną[9].

W opozycji do spraw publicznych stawia się dokument wewnętrzny obejmujący sferę, która nie dotyczy tych spraw. Co istotne, pojęcie dokumentu wewnętrznego nie zostało użyte w ustawie o dostępie do informacji, a jest jedynie wynikiem interpretacji przez sądy art. 1 ust. 1 u.d.i.p., w której poszukuje się obszarów aktywności nie mieszczących się w kategorii sprawy publicznej. Jednak w orzecznictwie nie pojawiło się nawet jednolite rozumienie tego pojęcia. Oczywiście z samej nazwy wynika, że funkcjonuje on w sferze wewnętrznej; według jednego z orzeczeń będzie to dokument, który nie jest skierowany do podmiotów zewnętrznych, może służyć wymianie informacji między pracownikami danego podmiotu, może określać ich zasady działania w określonych sytuacjach lub może być fragmentem przygotowań do powstania aktu, będącego forma działalności dane podmiotu[10].

W orzecznictwie można wyodrębnić trzy rodzaje argumentów uzasadniających kreowanie dokumentów wewnętrznych w sprawach dostępu do informacji publicznej[11]. Według pierwszego rodzaju argumentów, istotny pozostaje cel pozyskania informacji ze sfery wewnętrznej, w którym nie mieszczą się indywidualne interesy osób, domagających się informacji z tej sfery; dostęp do informacji publicznej powinien bowiem służyć realizacji interesu publicznego. W drugim poglądzie przyczyną wyłączenia dokumentu wewnętrznego z kategorii informacji publicznych jest brak waloru oficjalności tych dokumentów. Może to wynikać z tego, że w tych dokumentach jedynie projektuje się określony sposób działania, a tym samym dotyczą one sfery zamierzeń, a nie faktów. Dokumenty te mogą służyć co prawda realizacji zadania publicznego, ale nie przesądzają o kierunku działania organu w konkretnej sprawie. Przedmiotowe dokumenty mogą także służyć gromadzeniu i wymianie informacji oraz uzgadnianiu stanowisk i poglądów; mają one charakter organizacyjny i porządkowy. Trzeci rodzaj argumentów odnosi się do negatywnych konsekwencji udostępnienia informacji ze sfery wewnętrznej, np. ujawnienie pism wewnętrznych w przedsiębiorstwach energetycznych dotyczących postępowania podczas wykrywania nielegalnego poboru energii mogłoby zmniejszyć efektywność przeprowadzanych kontroli w tym zakresie.

To o tyle istotny podział na informacje publiczne i inne kategorie informacji (w tym dokumenty wewnętrzne), że dopiero, gdy określona informacja zostanie zakwalifikowana jako informacja publiczna, znajdzie do jej ujawniania zastosowanie ustawa o dostępie do informacji publicznej. Nawet jednak w takim przypadku przewidziane ustawą prawo do informacji o sprawach publicznych nie jest prawem nieograniczonym i ustawodawca dopuścił możliwość odmowy udostępnienia takiej informacji

---

[9] Wyrok NSA z dnia 30 września 2015 r., I OSK 2093/14, Centralna Baza Orzeczeń Sądów Administracyjnych (CBOSA).

[10] Wyrok NSA z dnia 18 sierpnia 2010 r., I OSK 851/10, CBOSA.

[11] G. Sibiga [w:] *Główne problemy prawa do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państw Unii Europejskiej*, red. *idem*, Warszawa 2014, s. 134 i n., a także orzecznictwo tam przywołane.

w sytuacjach określonych w art. 5 u.d.i.p. (ochrona informacji niejawnych oraz ochrona innych tajemnic ustawowo chronionych, tajemnica przedsiębiorcy, prywatność osoby fizycznej).

W ten sposób w orzecznictwie stworzono podwójny mechanizm ograniczania dostępu do informacji. Pierwszym etapem jest ustalanie, czy określona informacja dotyczy sprawy publicznej, a przez to czy jest informacją publiczną, do której stosuje się ustawę. Pozostałych informacji nie będzie obejmowało prawo dostępu do informacji publicznej, nawet jeśli są efektem działalności władzy publicznej. Dopiero w drugim etapie tak wyodrębnione informacje publiczne są oceniane pod kątem nazwanych ograniczeń prawa znajdujących się w art. 5 u.d.i.p. oraz w innych ustawach, a to ze względu na odesłanie do ustaw ustanawiających tajemnice zawarte w art. 5 ust. 1 u.d.i.p.

Czy materialne przejawy stosowania RODO stanowią informację publiczną?

Odnosząc powyższy podział informacji znajdujących się w posiadaniu podmiotów zobowiązanych do materialnych przejawów stosowania RODO, zauważam w orzecznictwie sądowym rozróżnienie na informacje o stosowaniu RODO oraz dokumenty będące wynikiem tego stosowania, czemu zresztą wyraz dałem już w tytule niniejszego artykułu.

W pierwszym przypadku warte zauważenia są dwa wyroki Wojewódzkiego Sądu Administracyjnego w Gorzowie Wielkopolskim[12], w których stwierdzono, że informacja dotycząca czynności, jakie podjął administrator w związku z wejściem w życie RODO, mających na celu ochronę danych osobowych, jest informacją publiczną w rozumieniu art. 1 ust. 1 tej ustawy i w związku z tym mają tu zastosowanie przepisy ustawy o dostępie do informacji publicznej. W tej sprawie wnioskujący zwrócił się do administratora (okręgowej rady adwokackiej – ORA) o udzielenie informacji na temat wspomnianych czynności, w szczególności wniósł o udzielenie odpowiedzi na pytania: 1) w jaki sposób był realizowany we wskazanym przez wnioskującego okresie obowiązek informacyjny, o którym mowa w art. 13 i 14 RODO oraz o udostępnienie klauzuli informacyjnej, jeżeli takową się posługuje ORA; 2) jakie środki organizacyjne i techniczne – we wskazanym we wniosku przedziale czasowym – wprowadzono, ażeby chronić dane osobowe przed ich utratą lub zniszczeniem oraz nieuprawnionym dostępem; 3) czy został wyznaczony inspektor ochrony danych (IOD), a jeżeli tak, to jakie są jego personalia i w jakim miejscu upublicznione są dane IOD oraz informacje, kiedy IOD został powołany.

Według sądu, wnioskujący jest uprawniony do żądania precyzyjnej odpowiedzi na swoje pytania. Mogą one dotyczyć nie tylko aktualnych czynności administratora

[12] Wyroki WSA w Gorzowie Wielkopolskim: z dnia 22 stycznia 2020 r., II SAB/Go 192/19; oraz z dnia 12 listopada 2020 r., II SA/Go 483/20, CBOSA.

w celu wykonania obowiązków informacyjnych z art. 13–14 RODO, ale także czynności dokonywanych w przeszłości we wskazanym przez żądającego przedziale czasowym. Odpowiada temu obowiązek administratora udzielenia odpowiedzi na tak szczegółowo postawione pytania, a jeżeli nie jest on w stanie udzielić żądanej informacji, to stanowisko w tym względzie powinno być przekonująco uzasadnione, tak aby twierdzenia w tym względzie były uprawdopodobnione[13].

Inne podejście sądy prezentują, gdy chodzi o ujawnianie konkretnych dokumentów ze sfery wewnętrznej administratora służących do wykonania obowiązków określonych w RODO. W wyroku WSA w Łodzi z 12 lutego 2019 r.[14] stwierdzono, że prowadzone rejestry czynności przetwarzania oraz rejestry kategorii czynności przetwarzania nie stanowią informacji publicznej, lecz stanowią dokument o charakterze wewnętrznym (organizacyjnym i porządkowym), co oznacza, że nie podlegają one udostępnianiu na podstawie ustawy o dostępie do informacji publicznej. Przedmiotem wniosku do organu administracji publicznej (administratora) o udostępnienie informacji na podstawie przepisów o dostępie do informacji publicznej były właśnie ujawnienie tych dwóch rejestrów. Jednak – zdaniem sądu – rejestry, o których mowa w art 30 RODO, „nie zawierają informacji o sprawach publicznych, lecz informację o sposobie gromadzenia danych osobowych. Są więc nośnikiem informacji o charakterze wewnętrznym, porządkowym, ewidencyjnym, który ma służyć zapewnieniu m.in. porządku i bezpieczeństwa. Takie rejestry nie odnoszą się natomiast do publicznej sfery działania organu" i w związku z tym jako takie nie zawierają informacji publicznej. Przypomniano bowiem, że cele prowadzenia rejestrów dotyczą administratora i podmiotu przetwarzającego, tj. pozwalają im usystematyzować wykonywane czynności oraz całościowo spojrzeć na wykonywane operacje przetwarzania danych osobowych pod względem zgodności m.in. z wymaganiami prawnymi. Rejestry mają ponadto ułatwić organowi nadzorczemu kontrolę wszystkich procesów przetwarzania danych w organizacji.

Kolejnym dokumentem, którego kwalifikacji dokonały sądy administracyjne, jest zgłoszenie naruszenia ochrony danych do organu nadzorczego. W wyroku z dnia 7 sierpnia 2019 r.[15] WSA w Gliwicach odniósł się do żądania wobec administratora – z powołaniem się na przepisy o dostępie do informacji publicznej – udostępnienia dokumentu zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych konkretnego naruszenia ochrony danych. Co wydaje się istotne, wnioskujący nie żądał ujawnienia informacji o merytorycznych działaniach organu czy czynnościach pozostających w zakresie jego właściwości, lecz treści pisma zawierającego zgłoszenie naruszenia ochrony danych do organu nadzorczego. Sąd uznał, że dokument ten nie podlega przepisom o dostępie do informacji publicznej i uzasadnił to dwoma rodzajami argumentów. Po pierwsze, zgłoszenie naruszenia ochrony danych stanowi korespondencję wewnętrzną organów (tj. organu zgłaszającego oraz Prezesa UODO) w zakresie RODO

[13] Zob. ww. wyrok II SA/Go 483/20, CBOSA.
[14] II SAB/Łd 181/18, CBOSA.
[15] Wyrok WSA w Gliwicach z dnia 7 sierpnia 2019 r., III SAB/Gl 206/19, CBOSA.

prowadzoną w związku z ochroną danych osobowych i zapewnieniem ich zgodnego z prawem przetwarzania, a nie czynność organu, do której został on powołany. W pojęciu informacji publicznej mieści się bowiem wiedza o działaniach pozostających w zakresie właściwości danego organu, zarządzaniu czy dysponowaniu mieniem czyli działaniach skierowanych na zewnątrz organu. Tymczasem pismo zawierające zgłoszenie naruszenia jest czynnością faktyczną o charakterze wewnętrznym. Po wtóre, zgłaszając naruszenie ochrony danych administrator inicjuje postępowanie w sprawie indywidualnej, a zawiadomienie staje się elementem akt postępowania, którego wnioskujący o informację publiczną nie jest stroną. Postępowanie to jest prowadzone w trybie ustawy o ochronie danych osobowych, a dostęp do akt takiego postępowania nie jest objęty ustawą o dostępie do informacji publicznej.

W tej samej sprawie Naczelny Sąd Administracyjny w wyroku z dnia 11 sierpnia 2020 r.[16], przychylając się do stanowiska wojewódzkiego sądu administracyjnego, użył częściowo zmodyfikowanej argumentacji opierającej się na twierdzeniu, że informacja publiczna dotyczy tylko sfery faktów, a żądane dokumenty nie spełniają tego warunku. W jego ocenie, pismo przekazujące zgłoszenie naruszenia ochrony danych, jako niedotyczące sfery faktów, lecz stanowiące korespondencję wewnętrzną pomiędzy administratorem a Prezesem Urzędu Ochrony Danych Osobowych, wykorzystaną na potrzeby związane z zamierzonymi działaniami danego podmiotu w przyszłości, nie może być uznane za informację podlegającą udostępnieniu na podstawie i w trybie ustawy o dostępie do informacji publicznej. Dokumenty zawierające zgłoszenie w zakresie naruszenia przez organ zawierają informacje, które mogą zostać wykorzystane przez organ administracji publicznej w przyszłości dla potrzeb postępowania prowadzonego w związku ze zgłoszonym naruszeniem ochrony danych osobowych i zapewnieniem ich zgodnego z prawem przetwarzania. Nie dotyczą one więc sfery faktów, lecz sfery zamierzeń.

Czy dokumenty dotyczące stosowania RODO są chronione poufnością?

W przedstawionym orzecznictwie kryterium oceny sądów jest charakter informacji, wyrażający się w odpowiedzi na pytanie, czy mamy do czynienia z informacją publiczną, a nie treść informacji pod kątem jej potencjalnej poufności. Inaczej ujmując, sąd nie analizowały, czy treść określonych dokumentów stosowania RODO powinna korzystać z ochrony poufności i w jakim zakresie powinno to następować.

Problem jest o tyle istotny, że obecny stan publicznej niedostępności opiera się jedynie na zaliczeniu poszczególnych dokumentów do sfery wewnętrznej podmiotów publicznych (administratorów), a nie ze względu na potrzebę zachowania w sekrecie treści dokumentów, czy chociażby ich części.

Polska ustawa o dostępie do informacji publicznej wymaga w art. 5 ust. 1 dla ograniczenia dostępności informacji publicznej istnienia tajemnicy ustawowo chronionej

[16] Wyrok NSA z dnia 11 sierpnia 2020 r., I OSK 224/20, CBOSA.

(obok tajemnicy przedsiębiorcy, prywatności osoby fizycznej oraz ochrony informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych). W związku z tym, gdy dojdzie do zaklasyfikowania konkretnej informacji jako informacji publicznej tylko objęcie jej prawną tajemnicą sprawia, że pozostanie ona niedostępna. W dotychczasowym orzecznictwie sądowym nie oceniono natomiast jeszcze, czy z przepisów RODO można wywodzić taką tajemnicę, chociaż w zakresie zapewnienia bezpieczeństwa technicznego i organizacyjnego danych osobowych poprzez poufność wewnętrznych polityk ochrony danych. Zdawkowe wypowiedzi judykatury wskazują, że z samej generalnej zasady z art. 24 ust. 1 RODO nie wynika, aby statuowała ona szczególną kategorię tajemnicy prawnie chronionej[17].

Problem ustalenia prawnych granic poufności unaocznia wyrok WSA w Opolu z dnia 16 marca 2021 r.[18], który dotyczył ujawnienia dokumentów z audytu bezpieczeństwa informacji w urzędzie miejskim. W odpowiedzi na żądanie ujawnienia protokołu, a następnie sprawozdania z tego audytu, burmistrz przyjął, że wnioskowany dokument ma charakter wewnętrzny. W jego opinii przedmiotowy dokument dotyczy sposobów zabezpieczenia danych osobowych poprzez opracowanie i wdrożenie oraz realizację techniczno-organizacyjnych zabezpieczeń danych. Podniósł, że dokument, o którego udostępnienie wnosił skarżący obejmuje zagadnienia związane z opracowaniem i wdrożeniem oraz wykonywaniem zabezpieczeń fizycznych i infrastruktury informatycznej. Dlatego też nawet ogólny opis technicznych i organizacyjnych środków bezpieczeństwa nie podlega ujawnieniu i powszechnemu dostępowi. Sąd, stwierdzając bezczynność burmistrza, uznał, że zarówno protokół audytowy, jak i sprawozdanie z audytu zawierają wspólne cechy przesądzające o ich urzędowym charakterze. Sąd podniósł również, że stanowią one dokumentację przebiegu i efektów kontroli działalności podmiotu zobowiązanego do udostępnienia informacji publicznej w zakresie wykonywanej przez ten podmiot działalności publicznej (art. 6 ust. 1 pkt 4 lit. a tiret drugie u.d.i.p.), a przez to mają charakter informacji publicznej. Organ (burmistrz) zobowiązany jest zatem do odniesienia się do treści dokumentu i danych w nim zawartych w aspekcie tego, czy je udostępnia, czy uznaje ich ochronę w zakresie tajemnicy chronionej prawnie; a jeżeli tak – to w jakim zakresie i dlaczego tak uznaje. Dlatego też nakazano w wyroku rozpatrzenie merytoryczne wniosku o udostępnienie informacji publicznej, a rozpoznając wniosek, organ winien jest ustalić, czy nie zachodzą przesłanki ograniczające dostępność informacji, o których mowa w art. 5 ust. 1 i 2 u.d.i.p. i wydać decyzję odmowną w razie ich zaistnienia bądź udzielić informacji publicznej w przypadku braku ograniczenia do niej dostępu.

[17] Wyrok WSA w Poznaniu z dnia 26 września 2019 r., IV SA/Po 578/19, CBOSA.
[18] II SAB/Op 3/21, CBOSA.

Wnioski

Problemy z sądowym ustaleniem granic powszechnej dostępności dokumentów stosowania RODO wpisują się w dwa istotne dylematy polskich przepisów o dostępie do informacji publicznej: kwalifikacją, czy określona informacja jest informacją publiczną oraz ograniczeniem dostępności informacji publicznej ze względu na ustawowo chronioną tajemnicę.

Obecnie w orzecznictwie sądów administracyjnych podjęto przede wszystkim pierwszy temat. Jednak w mojej ocenie, za daleko niewystarczające należy uznać stwierdzenie niedostępności informacji tylko z tego powodu, że dokumenty dotyczące stosowania RODO mają charakter dokumentu wewnętrznego, który nie podlega zakresowi przepisów o dostępie do informacji publicznej. Pojęcie dokumentu wewnętrznego nie posiada jednoznacznych podstaw normatywnych i pozostaje jedynie oparte na różnorodnych (i częściowo nie do końcach jasnych) argumentach sprowadzających się do takiej wykładni art. 1 ust. 1 u.d.i.p., w której poszukuje się obszarów aktywności niemieszczących się w kategorii sprawy publicznej. Wyodrębnienie sfery wewnętrznej jest każdorazowo zależne całkowicie od składu orzekającego sądu.

Natomiast ciągle otwarte w orzecznictwie pozostaje pytanie, czy dokumenty dotyczące stosowania RODO korzystają z prawnej ochrony poufności ich treści. Oczywiście w wykonaniu RODO tworzy się znaczny zasobów różnorodnych dokumentów i nie chodzi o prawne szczegółowe określenie publicznej dostępności każdego z nich. Jednak na razie przedmiotem analizy sądów nie było nawet generalne ustalenie granic ich powszechnej dostępności, i chociażby kierunkowe określenia znaczenia w tym względzie zasady integralności i poufności z art. 5 ust. 1 lit. f RODO czy też tajemnicy inspektora ochrony danych z art. 38 ust. 5 RODO.

Podumowując, należy stwierdzić, że aktualny stan, w tym wynikający z orzecznictwa, powoduje wśród administratorów objętych mocą przepisów o dostępie do informacji publicznej niepewność co do warunków i zakresu poufności treści dokumentów. Problemy sprowadzają się do pytań, jaki dokument i w jakich sytuacjach staje się informacją publiczną lub dokumentem wewnętrznym; a jeżeli uznany zostanie za informację publiczną, to na jakich prawnych zasadach ma następować weryfikacja, czy jego treść jest powszechnie dostępna, czy też chroniona poufnością. Przedstawione dylematy stanowią element szerszej oceny, według której przepisy ustawy o dostępie do informacji publicznej utraciły cechę pewności (przewidywalności zastosowania), a to właśnie ze względu na niejasny jej zakres przedmiotowy stosowania, opierający się na kryterium „informacji publicznej”[19].

[19] M. Bernaczyk, *Dokument wewnętrzny jako ograniczenie konstytucyjnego prawa do informacji. Rozstrzyganie kolizji w teorii i praktyce prawa*, Warszawa 2017 r., s. XXXVI.

Literatura

Bernaczyk M., *Dokument wewnętrzny jako ograniczenie konstytucyjnego prawa do informacji. Rozstrzyganie kolizji w teorii i praktyce prawa*, Warszawa 2017.

Główne problemy prawa do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państw Unii Europejskiej, red. G. Sibiga, Warszawa 2014.

Kowalik-Bańczyk K., *Komentarz do art. 255 TWE* [w:] *Traktat Ustanawiający Wspólnotę Europejską. Komentarz*, t. 3, red. D. Kornobis-Romanowska, J. Łacny, Warszawa 2009.

Pawełczyk M., Stankiewicz R., *Zmaterializowana forma informacji jako jeden z podstawowych elementów definicji informacji publicznej*, „Radca Prawny" 2012, nr 132.

Streszczenie

Grzegorz Sibiga

Publiczna dostępność na podstawie przepisów o dostępie do informacji publicznej informacji i dokumentów dotyczących stosowania RODO przez administratora w orzecznictwie sądów administracyjnych

Przedmiotem artykułu jest przedstawienie i ocena orzecznictwa sądów administracyjnych dotyczących publicznej dostępności – na podstawie przepisów o dostępie do informacji publicznej – informacji i dokumentów o stosowaniu RODO. Chodzi o potencjalne obowiązki ujawnienia nałożone na tych administratorów, którzy są jednocześnie podmiotami objętymi mocą przepisów o dostępie do informacji publicznej. Dylematy związane z jawnością informacji i dokumentów dotyczących RODO wpisują się w szersze problemy związane z niejasnym zakresem stosowania przepisów o dostępie do informacji publicznej oraz z prawnymi warunkami ograniczeń dostępności spowodowanych poufnością. Aktualny stan, w tym wynikający z orzecznictwa sądowego, powoduje wśród administratorów niepewność co do warunków i zakresu poufności treści dokumentów dotyczących stosowania RODO.

Słowa kluczowe: informacja publiczna; publiczny dostęp; dokument wewnętrzny; poufność; RODO.

Summary

Grzegorz Sibiga

Public Availability of Information and Documents on Controller's Compliance with GDPR Under the Provisions on Access to Public Information in the Jurisprudence of Administrative Courts

This article aims to present and assess the judicature of the Polish administrative courts concerning the public availability of information and documents on GDPR compliance under the Act on Access to Public Information. It is about the potential disclosure obligations imposed on those controllers who are also the entities covered by the provisions on the access to public informa-

tion. The dilemmas surrounding the disclosure of information and documents regarding GDPR compliance are part of broader issues relating to the unclear scope of application of the Act on Access to Public Information and the confidential nature of such information. The current legal situation, including judicial decisions, leads to uncertainty among controllers regarding the disclosure conditions and scope of confidentiality of documents regarding GDPR compliance.

Keywords: public information; public access; internal document; confidentiality; GDPR.

Xawery Konarski
TKP Kancelaria Traple Konarski Podrecki i Wspólnicy
xawery.konarski@traple.pl
ORCID: 0000-0003-4428-1900

https://doi.org/10.26881/gsp.2021.4.06

Administracyjna kara finansowa w sprawie *cookies*. Komentarz na kanwie postanowienia Krajowej Komisji Informatyki i Wolności we Francji (CNIL) z dnia 7 grudnia 2020 r. w sprawie *Amazon Europe Core*, SAN-2020-013

1. Wprowadzenie

Problematyka prawna korzystania z identyfikatorów internetowych, takich jak pliki cookies[1], jest jedną z najczęściej poruszanych w kontekście ochrony prywatności i danych osobowych użytkowników usług łączności elektronicznej. Zasady korzystania z nich stały się w ostatnich latach przedmiotem szeregu orzeczeń Trybunału Sprawiedliwości Unii Europejskiej (TSUE)[2], a także decyzji organów regulacyjnych w poszczególnych państwach UE[3].

W dniu 7 grudnia 2020 r. francuski organ ds. ochrony danych osobowych[4] (CNIL) wydał decyzje nakładające kary pieniężne za naruszenie francuskich przepisów dotyczących cookies przez amerykańskie podmioty zaliczane do tzw. Big Tech (Amazon, Google)[5]. Sprawy te wywołały ogromne zainteresowanie nie tylko z uwagi na

[1] Pliki cookies (tzw. ciasteczka) stanowią dane informatyczne, w szczególności pliki tekstowe, które przechowywane są w urządzeniu końcowym użytkownika strony internetowej. „Ciasteczka" używane są w różnych celach – np. optymalizacji korzystania z treści dostępnych na stronie internetowej, identyfikacji użytkownika, celach analitycznych, reklamowych itp.

[2] Najważniejsze z orzeczeń Trybunału Sprawiedliwości dotyczących cookies to: wyrok TSUE z dnia 1 października 2019 r. w sprawie *Planet49 GmbH* (C-673/17), wyrok TSUE z dnia 29 lipca 2019 r. w sprawie *Fashion ID GmbH & Co. KG* (C-40/17) oraz wyrok TSUE z dnia 5 czerwca 2018 r. w sprawie *Wirtschaftsakademie Schleswig-Holstein GmbH* (C-210/16).

[3] Przykładem rozstrzygnięcia tego rodzaju jest decyzja hiszpańskiego organu nadzorczego (AEPD) z dnia 3 marca 2020 r. w sprawie *Twitter Inc.* (PS/00299/2019).

[4] Commission Nationale de l'Informatique et des Libertés (Krajowa Komisja Informatyki i Wolności).

[5] Decyzja CNIL z dnia 7 grudnia 2020 r. w sprawie *Amazon Europe Core* (SAN-2020-013) oraz decyzja CNIL z dnia 7 grudnia 2020 r. w sprawie *Google LLC* oraz *Google Ireland* (SAN-2020-012). W dalszej części niniejszego artykułu omówiono decyzję w sprawie *Amazon Europe Core*. Warto w związku z tym podkreślić, że stan faktyczny i prawny oraz uzasadnienie decyzji CNIL w sprawach *Google LLC* oraz

rekordową wysokość kar (łącznie 100 mln euro), ale przede wszystkim na dokonane w nich przez CNIL rozstrzygnięcie szeregu istotnych zagadnień dotyczących wzajemnej relacji przepisów o e-prywatności oraz o ochronie danych osobowych (RODO), a także związanych z tym kompetencji krajowych organów nadzorczych w sytuacjach transgranicznego przetwarzania danych. Problematyka ta zostanie omówiona w niniejszym artykule w ramach analizy decyzji CNIL, dotyczącej spółki Amazon Europe Core S.à r.l. (AEC; spółka AEC).

2. Stan faktyczny i prawny

Analizowana sprawa dotyczyła oceny przez CNIL prawidłowości procesu zapisywania plików cookies po wejściu na stronę amazon.fr, w szczególności w zakresie, w jakim pliki te były instalowane na urządzeniach odwiedzających tę witrynę użytkowników, znajdujących się na terytorium Francji. Uczestnikami postępowania były dwie spółki z grupy Amazon: Amazon Online France SAS z siedzibą we Francji oraz spółka AEC z siedzibą w Luksemburgu. Pierwszy z tych podmiotów zajmuje się promocją i sprzedażą we Francji produktów i usług reklamy internetowej, opracowanych oraz zarządzanych przez spółkę AEC i działających w oparciu o dane gromadzone za pomocą cookies. Głównym przedmiotem działalności spółki AEC jest z kolei prowadzenie europejskich stron internetowych „Amazon", poprzez które realizowana jest sprzedaż internetowa towarów. Jedną z zarządzanych przez AEC witryn jest strona internetowa amazon.fr, dostępna pod adresem URL https://www.amazon.fr. Roczny obrót AEC w roku, w którym wszczęto postępowanie (2019) wyniósł 7,7 mld euro.

Postępowanie kontrolne zostało formalnie zainicjowane przez CNIL w dniu 29 listopada 2019 r. W jego trakcie dokonano m.in. trzykrotnych oględzin witryny amazon.fr, a także kontroli w siedzibie francuskiej spółki Amazon Online France SAS. W sprawie wymienianie były również liczne pisma pomiędzy organem a spółkami z grupy Amazon.

Na podstawie zgromadzonego materiały dowodowego, CNIL ustalił, że po bezpośrednim wejściu przez użytkowników na witrynę amazon.fr lub po przekierowaniu ich na tą stronę przez baner reklamowy umieszczony na stronach podmiotów trzecich, na urządzeniach internautów znajdujących się na terytorium Francji instalowane były pliki cookies. Do czynności tych dochodziło bez wiedzy i zgody użytkowników, a podmiotem decydującym o sposobie wykonania tych czynności była spółka AEC. Zbierane w ten sposób informacje o użytkownikach były następnie wykorzystywane zarówno na cele spersonalizowanej reklamy spółek Amazon (*first party cookies*), jak i innych podmiotów, które instalowały cookies w porozumieniu z Amazonem (*third party cookies*).

Oceny prawnej przedstawionego powyżej stanu faktycznego francuski organ ds. ochrony danych osobowych dokonał na podstawie art.82 francuskiej ustawy

Google Ireland zawierają wiele elementów wspólnych.

o ochronie danych osobowych[6]. Przepis ten stanowi implementację art. 5 ust. 3 dyrektywy 2002/58/WE[7], w wersji zmienionej dyrektywą 2009/136/WE[8]. Zgodnie z jego treścią, każdy abonent lub użytkownik usługi łączności elektronicznej musi zostać poinformowany „w jasny i wyczerpujący sposób", o celu, dla którego w jego urządzaniu końcowym są przechowywane informacje lub uzyskiwany dostęp do tych informacji (np. za pomocą cookies), a także o sposobie, w jaki może się sprzeciwić dokonywaniu takich czynności. Poza wyjątkami opisanymi w ustawie (a które nie znalazły zastosowania w analizowanej sprawie), abonent lub użytkownik musi również, po otrzymaniu powyższych informacji, wyrazić zgodę na dokonanie tych czynności, a zgoda ta może także zostać uzyskana poprzez„odpowiednie ustawienia parametrów jego urządzenia".

Zgodnie z art. 16 francuskiej ustawy, CNIL – oprócz nadzoru nad przestrzeganiem przepisów RODO – ma również kompetencję do kontroli przestrzegania przepisów stanowiących implementację dyrektywy 2002/58/WE. W przypadku stwierdzonych naruszeń przepisów o e-prywatności, CNIL ma również określone uprawnienia naprawcze, a także prawo do nałożenia sankcji administracyjnych, w tym kar pieniężnych (art. 20.III). Co istotne, kary pieniężne w takich przypadkach mogą być nakładane w wysokości takiej jak określono w art. 83 ust. 4 RODO, z uwzględnieniem kryteriów ich wymierzania wskazanych w art. 83 RODO (art. 20 III ust. 7 ustawy francuskiej).

3. Decyzja CNIL

Na podstawie zgromadzonego materiału dowodowego, CNIL stwierdził naruszenie przez spółkę AEC przepisu art. 82 ustawy francuskiej i w dniu 7 grudnia 2020 r. wydał decyzję, zgodnie z którą:

1) na AEC nałożono karę pieniężną w wysokości 35 mln euro;
2) nakazano spółce dostosowanie prowadzonego przetwarzania, w terminie trzech miesięcy od doręczenia niniejszej decyzji, do wymogów art. 82 francuskiej ustawy o ochronie danych, w szczególności poprzez uprzednie poinformowanie osób, których dane dotyczą, w sposób jasny i wyczerpujący, np. za pomocą banera informacyjnego pojawiającego się przy pierwszym wejściu użytkownika na stronę amazon.fr, niezależnie od sposobu, w jaki trafił on na tę stronę:

---

[6] Loi Informatique et Libertes, N°78-17 z dnia 6 stycznia 1978 r. ze zm.; dalej: francuska ustawa o ochronie danych osobowych; ustawa francuska.

[7] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), (Dz. Urz. UE L 201, s. 37 ze zm.).

[8] Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (Dz. Urz. UE L 337, s. 11).

- o dokładnych celach wykorzystywania wszystkich plików cookies, których instalacja jest uzależniona od zgody użytkownika oraz
- o dostępnych użytkownikom środkach, za pomocą których można wyrazić sprzeciw na dokonanie tej czynności;

3) w przypadku niewykonania powyższego nakazu dostosowania przetwarzania do wymogów art. 82 ustawy francuskiej nałożono dodatkową karę w wysokości 100 tys. euro za każdy dzień zwłoki w wykonaniu tego zobowiązania;
4) zdecydowano również o podaniu treści decyzji do publicznej wiadomości na stronie internetowej CNIL i na stronie internetowej Légifrance przez okres dwóch lat od jej opublikowania.

Rozstrzygając o wysokości nałożonej kary oraz podaniu treści decyzji do publicznej wiadomości, CNIL wziął pod uwagę – zgodnie z kryteriami określonymi w art. 83 RODO – wymienione niżej okoliczności.

Po pierwsze, skalę naruszenia przez AEC obowiązków określonych w art. 82 ustawy francuskiej, w szczególności fakt niespełnienia w ogóle (lub w nieznacznym zakresie) obowiązku informacyjnego, a także wadliwość sposobu pozyskiwania zgody użytkowników na zapisywanie na ich urządzeniach cookies reklamowych. Naruszenie to uznano za szczególnie poważne, ponieważ przeprowadzona kontrola wykazała, że w trakcie wejścia pojedynczego użytkownika na witrynę amazon.fr, ponad 20 podmiotów współpracujących z AEC instalowało w jego urządzeniu cookies, co prowadziło następnie do wyświetlania mu przez te podmioty reklam internetowych.

Po drugie, istotne znaczenie miała również ilość użytkowników dotkniętych powyższym naruszeniem. W okresie prowadzonego przez CNIL postępowania doszło bowiem do zainstalowania poprzez stronę internetową amazon.fr ponad 300 milionów cookies (identyfikatorów internetowych).

Pod trzecie, wzięto także pod uwagę wysokość globalnego obrotu AEC w 2019 r. (7,7 mld euro), jak również fakt, że prowadzona działalność ma bezpośredni związek z uzyskiwaniem tych przychodów, instalowanie cookies ułatwia bowiem spersonalizowaną reklamę produktów sprzedawanych przez AEC za pomocą witryny amazon.fr.

Powyższe okoliczności, a także dominująca pozycja AEC w sektorze handlu elektronicznego przesądziły o uznaniu, że interes publiczny wymaga podania treści decyzji CNIL do publicznej wiadomości w okresie dwóch lat od jej ogłoszenia.

4. Problematyka prawna wyroku

Analizowana decyzja CNIL odnosi się do szeregu istotnych i mających uniwersalne znaczenie problemów prawnych związanych ze stosowaniem przepisów krajowych, implementujących dyrektywę o e-prywatności. Zaliczyć do nich należy w szczególności:

1) określenie właściwości rzeczowej organu ds. ochrony danych osobowych w zakresie oceny legalności instalowania i dostępu do informacji zapisywanych w plikach cookies, w tym również – w przypadku transgranicznej działalności da-

nego podmiotu – ewentualnego zastosowania mechanizmu *One Stop Shop* (OSS) – art. 56 i n. RODO;
2) wyznaczenie zakresu terytorialnego stosowania przepisów o e-prywatności;
3) określenie zasad dopuszczalnego instalowania i dostępu do informacji przechowywanych w plikach cookies.

5. Właściwość rzeczowa CNIL oraz zastosowanie mechanizmu *One Stop Shop*

5.1. Argumentacja AEC i CNIL

W trakcie postępowania, AEC kwestionował kompetencję rzeczową CNIL do rozstrzygnięcia sprawy, twierdząc, że właściwym organem jest organ ds. ochrony danych osobowych w państwie, w którym spółka ma siedzibę, tj. w Luksemburgu. Zdaniem AEC, analizowana sprawa była w bowiem istocie sprawą z zakresu RODO. Przesądza o tym, nierozerwalny związek pomiędzy instalowaniem cookies, a późniejszym wykorzystaniem danych osobowych w ten sposób zebranych. Istotny jest również sposób implementacji przepisów dyrektywy 2002/58/WE przez francuskiego ustawodawcę, który dokonał jej bezpośrednio w ustawie o ochronie danych osobowych, a nie w odrębnych (sektorowych) przepisach.

Spółka AEC dodatkowo argumentowała, że nawet gdyby przyjąć, że analizowana sprawa nie jest sprawą z zakresu ochrony danych osobowych, to z uwagi na jej transgraniczny charakter, a także brak odpowiednich przepisów w dyrektywie 2020/58/WE określających organy właściwe w takich sytuacjach, zastosowanie do niej w każdym razie powinien znaleźć określony w art.55 i n. RODO mechanizm współpracy pomiędzy organami nadzorczymi (OSS) w różnych państwach Unii Europejskiej . Zgodnie z nim, dla transgranicznego przetwarzania danych osobowych, dokonywanego przez AEC w związku z korzystaniem z cookies, za tzw. wiodący organ nadzorczy powinien zostać uznany organ w Luksemburgu, i to on powinien rozstrzygnąć tę sprawę. Dopuszczalność stosowania mechanizmu OSS określonego w RODO – w niniejszej sprawie uzasadnia okoliczność, że zgodnie z art. 1 ust. 2 dyrektywy 2002/58/WE, jej przepisy uzupełniają – jako *lex specialis* – przepisy o ochronie danych osobowych i w braku odrębnego uregulowania w nich określonego zagadnienia, te ostatnie znajdują zastosowanie jako *lex generali*.

Z powyższą argumentacją nie zgodził się CNIL. Francuski organ po pierwsze potwierdził, że przedmiotowe postępowanie nie dotyczyło ochrony danych osobowych, ale oceny wykonania wzorowanych na dyrektywie 2002/58/WE i określonych w art. 82 ustawy francuskiej, obowiązków z zakresu ochrony prywatności w sieciach łączności elektronicznej. Francuski organ ds. ochrony danych osobowych podkreślił również, że trzeba dokonać rozróżnienia pomiędzy operacją instalowania i odczytywania informacji zapisywanych na urządzeniach użytkowników a późniejszym przetwarzaniem

danych osobowych w ten sposób zebranych. Do oceny dopuszczalności pierwszej z tych czynności właściwy jest przepis art. 82 ustawy francuskiej, natomiast dla określana legalności przetwarzania danych osobowych – przepisy RODO.

Jeżeli chodzi o wyznaczenie organu nadzorującego przepisy o e-prywatności, to zgodnie z art. 15a) dyrektywy 2002/58/WE (dodanym w dyrektywie 2009/136/WE), ustawodawcy krajowi mają swobodę w określeniu, który z organów ma sprawować nadzór nad przestrzeganiem przepisów krajowych implementujących przepisy dyrektywy. W przypadku Francji zadanie to powierzono organowi do spraw ochrony danych osobowych. Sprawowany w tym zakresie przez CNIL nadzór sprawowany jest więc w celu egzekwowania przestrzegania przepisów dyrektywy 2002/58/WE, a nie przepisów RODO. O braku możliwości posłużenia się mechanizmem OSS, a co za tym idzie – przekazania spraw do „wiodącego organu nadzorczego" w innym państwie, przesądza jednoznacznie treść art. 15a ust. 2 dyrektywy 2002/58/WE, zgodnie z którym – organem odpowiedzialnym za przestrzeganie przepisów ma być „właściwy organ krajowy" w państwie, w którym doszło do naruszenia w danej sprawie, tj. we Francji.

Z powyższych przyczyn CNIL uznał, że po pierwsze, jest właściwy rzeczowo do rozstrzygnięcia sprawy AEC jako organ wskazany w art. 16 ustawy francuskiej do przestrzegania przepisów o e-prywatności, a po drugie, brak jest podstaw prawnych do przekazania sprawy organowi luksemburskiemu jako organowi wiodącemu w rozumieniu art. 55 RODO, mechanizm OSS nie znajduje bowiem zastosowania do spraw z zakresu ochrony prywatności, których dotyczy dyrektywa 2002/58/WE.

5.2. Komentarz

W analizowanej sprawie kluczowa jest okoliczność dokonania implementacji art. 5 ust. 3 dyrektywy 2002/58/WE w ramach francuskiej ustawy o ochronie danych osobowych, a nie – jak to uczyniono w wielu państwach Unii Europejskiej – w ramach sektorowych ustaw dotyczących usług łączności elektronicznej[9]. Zgodnie z przyjętym w ustawie francuskiej rozwiązaniem, CNIL został wyznaczony do nadzoru nad przestrzeganiem przepisów implementujących dyrektywę 2002/58/WE. W konsekwencji, CNIL występuje w dwóch rolach – jako organ ds. ochrony danych osobowych oraz jako organ ds. ochrony prywatności. W postępowaniu dotyczącym AEC decyzja została wydana przez CNIL jako organ nadzorujący przepisy o prywatności.

Za prawidłowe należy uznać stanowisko CNIL o braku stosowania się, określonego w RODO, mechanizmu OSS do transgranicznych spraw dotyczących ochrony przysługujących użytkownikom na podstawie przepisów implementujących dyrektywę 2002/58/WE. Organy nadzorcze powołane do przestrzegania tych ostatnich przepisów mają bowiem niezależną i odrębną od organów ds. ochrony danych osobowych, kompetencję do rozstrzygania tych spraw. Mimo braku w dyrektywie 2020/58/WE odrębnych przepisów dotyczących sytuacji transgranicznego przetwarzania, nie można

[9] Przykładem tego drugiego sposobu implementacji jest Polska. Art. 5 ust. 3 dyrektywy 2002/58/WE został bowiem implementowany w art. 173 ustawy – Prawo telekomunikacyjne z dnia 16 lipca 2004 r. (tekst jedn.: Dz. U. z 2021 r., poz. 576; dalej: u.p.t., ustawa – Prawo telekomunikacyjne).

w takiej sytuacji stosować przepisów RODO. Stanowisko to jednoznacznie potwierdza opinia Europejskiej Rady Ochrony Danych (EROD), zgodnie z którą „mechanizmy współpracy i spójności dostępne dla organów ochrony danych na podstawie rozdziału VII RODO dotyczą monitorowania stosowania przepisów RODO. Mechanizmów określonych w RODO nie stosuje się do egzekwowania wdrażania dyrektywy o prywatności i łączności elektronicznej na szczeblu krajowym."[10].

Francuski organ do spraw ochrony danych osobowych trafnie dokonał również rozróżnienia pomiędzy czynnościami zapisywania i odczytu cookies oraz późniejszego przetwarzania danych osobowych w ten sposób pozyskanych. Konstrukcyjnie są to bowiem, co prawda bezpośrednio powiązane, ale jednak odrębne czynności mające za przedmiot dwa niezależne dobra prawnie chronione: prywatność użytkowników usług łączności elektronicznej oraz dane osobowe. Przepisy o prywatności chronią w szczególności prawo użytkowników do decydowania, czy i w jakim celu w ich urządzeniach końcowych mogą być instalowane i następnie przechowywane różnego rodzaju dane zawierające informacje o nich. Ochrona ta przysługuje użytkownikom niezależnie od charakteru tych informacji, w tym – czy mają charakter danych osobowych. W sytuacji gdy będą miały taki status, zastosowanie znajdą również przepisy RODO w zakresie podstaw dopuszczalnego przetwarzania tych informacji. W konsekwencji takiego rozróżnienia, należy przyjąć, że o ile na instalowanie np. cookies reklamowych bezwzględnie wymagana jest zgoda użytkownika, o tyle nie można wykluczyć przetwarzania danych osobowych w ten sposób zebranych, w oparciu o podstawę prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f RODO. Przewidziany w art. 5 ust. 3 dyrektywy 2002/58/WE oraz wzorowanym na nim art. 82 ustawy francuskiej, wymóg pozyskania zgody nie określa bowiem podstaw przetwarzania danych osobowych o użytkownikach np. na potrzeby spersonalizowanej reklamy.

Za interesujące uznać należy przyjęte we francuskiej ustawie rozwiązanie, zgodnie z którym w sprawach o naruszenie prywatności CNIL może nakładać kary pieniężne w tej samej wysokości i na takich samych zasadach, jak to przewidziano w art. 83 ust. 4 RODO. Z uwagi na autonomię, którą mają ustawodawcy krajowi w zakresie określania sankcji za naruszenie przepisów implementujących dyrektywę 2002/58/WE, tego rodzaju rozwiązanie jest konstrukcyjnie dopuszczalne i z pewnością przyczynia się do większej spójności w zakresie nakładania kar za różnego rodzaju naruszenia danych osobowych i prywatności w sieciach łączności elektronicznej. Na marginesie trzeba też zauważyć, że odpowiada ono założeniom projektu rozporządzenia o e-prywatności, zgodnie z którym kary za naruszenie tego rozporządzenia mają zostać zrównane z karami za nieprzestrzeganie przepisów RODO (art. 23 projektu)[11]. Na

[10] Zob. pkt 91 opinii 5/2019 Europejskiej Rady Ochrony Danych z dnia 12 marca 2019 r. w sprawie wzajemnej zależności między dyrektywą o prywatności i łączności elektronicznej a RODO, w szczególności w zakresie właściwości, zadań i uprawnień organów ochrony danych.

[11] Wniosek – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE, wersja projektu Rozporządzenia UE w sprawie prywatności i łączności elektronicznej z dnia 10 lutego 2021, 6087/21.

koniec warto przypomnieć, że inny – niż francuski – model implementacji dyrektywy 2002/58/WE przyjął polski ustawodawca. Transpozycji przepisu art. 5 ust. 3 dyrektywy 2002/58 WE dokonano bowiem w regulacji sektorowej dotyczącej łączności elektronicznej, w szczególności w art. 173 ustawy – Prawo telekomunikacyjne. Najważniejszą tego konsekwencją jest brak kompetencji Prezesa Urzędu Ochrony Danych Osobowych (PUODO) do egzekwowania obowiązków określonych w tym przepisie. W tym zakresie wyłącznie właściwy jest Prezes Urzędu Komunikacji Elektronicznej (UKE), którego kompetencje do nałożenia sankcji określono w art. 209 ust.1 pkt 27 i art. 209 ust. 1^1 pkt 2 u.p.t. Warto przy tym podkreślić, że inaczej niż w przypadku przepisów RODO, w których za legalność przetwarzania danych odpowiada tylko administrator, na gruncie art. 173 u.p.t. odpowiedzialność mogą również ponosić podmioty świadczące usługi telekomunikacyjne lub usługi świadczone drogą elektroniczną i dokonujące na zlecenie innego podmiotu instalacji plików cookies (np. w celu realizacji jego celów marketingowych). Prezes Urzędu Ochrony Danych Osobowych jest natomiast wyłącznie właściwy w sprawach realizacji określonych w RODO obowiązków przetwarzania danych osobowych, w tym weryfikacji legalności przetwarzania informacji tego rodzaju zapisanych w cookies.

6. Terytorialny zakres stosowania przepisów o e-prywatności

6.1. Argumentacja AEC i CNIL

Zgodnie z art.3 (I) ustawy francuskiej, jej przepisy mają zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego we Francji, niezależnie od tego, czy przetwarzanie odbywa się w tym państwie.

Mając na względzie treść powyższego przepisu, AEC zakwestionował stosowanie francuskiej ustawy (w tym jej art. 82) do dokonywanego przez niego instalowania i odczytu plików cookies. Zdaniem spółki, nie została w szczególności spełniona przesłanka, zgodnie z którą przetwarzanie danych osobowych musi odbywać się „w ramach działalności jednostki organizacyjnej administratora" na terytorium Francji. Nie istnieje bowiem nierozerwalny związek między działalnością Amazon Online France SAS z jednej strony, a umieszczaniem plików cookie przez Amazon Europe Core – jako administratora – na stronie amazon.fr. Istotne jest przy tym, że Amazon Online France SAS nie tylko nie zajmuje się umieszczaniem plików cookies na urządzeniach użytkowników, ale jego działalność polega wyłącznie na wsparciu doradczym przedsiębiorstw, które chcą sprzedawać swoje towary poprzez witrynę amazon.fr, zarządzaną przez AEC. Spółka argumentowała również, że to AEC – a nie Amazon Online France SAS – w imieniu klientów umieszcza na stronach internetowych osób trzecich reklamy, po których kliknięciu następuje przekierowanie na podstrony z odpowiednimi towarami dostępnymi na witrynie amazon.fr.

Z powyższym stanowiskiem nie zgodził się CNIL, który w pierwszej kolejności podkreślił, że art. 3 ustawy francuskiej wzorowany był na art. 4 dyrektywy 95/46/WE[12], który to przepis określał prawo właściwe dla przetwarzania danych osobowych na terytorium Unii Europejskiej. W aktualnym stanie prawnym, tj. po rozpoczęciu obowiązywania RODO i ustanowieniu w nim odrębnych reguł, art. 4 dyrektywy 95/46/WE co prawda został uchylony, ale brak jest przeszkód, aby nadal we francuskiej ustawie utrzymać te zasady w zakresie nieobjętym RODO, w szczególności na potrzeby określenia prawa francuskiego jako właściwego w sprawach rozstrzyganych na podstawie przepisów implementujących przepisy dyrektywy 2002/58/WE. Pozwala to również na skorzystanie z dorobku orzecznictwa TSUE, wydanego na podstawie art. 4 dyrektywy 95/46/WE.

W powyższym kontekście, CNIL potwierdził, że poza sporem jest, że Amazon Online France SAS jako spółka z siedzibą we Francji ma cechy „jednostki administracyjnej", o której mowa w art. 3 (I) ustawy francuskiej, a także, że świadczy usługi promujące działalność AEC, będącego administratorem. Francuski organ ds. ochrony danych osobowych odwołał się w związku z tym do dwóch orzeczeń TSUE. Zgodnie z pierwszym z nich, wydanym w dniu 13 maja 2014 r. w sprawie *Google Spain*, trybunał uznał, że przetwarzanie danych osobowych przez wyszukiwarkę Google było wykonywane „w ramach działalności" Google Spain (jako spółki należącej do Google Inc.) w zakresie, w jakim ta spółka miała na celu zapewnienie w Hiszpanii promocji i sprzedaży powierzchni reklamowej oferowanej przez tę wyszukiwarkę, co zdaniem trybunału służy uczynieniu usługi oferowanej przez tę wyszukiwarkę opłacalną . Ponadto, CNIL podkreślił, że chociaż orzeczenie w sprawie Google Spain dotyczyło działalności administratora (Google Inc.) mającego siedzibę poza Unią Europejską, to w późniejszym orzeczeniu z 5 czerwca 2018 r., TSUE zastosował tę samą rozszerzającą interpretację przetwarzania „w kontekście działalności" na terytorium Unii Europejskiej, również w sytuacji, w której administratorem był podmiot z innego państwa UE[13].

Mając na względzie ustalony w sprawie stan faktyczny, a także wskazówki interpretacyjne zawarte w powyższych orzeczenia TSUE, francuski organ uznał, że ponieważ Amazon Online France SAS ma siedzibę we Francji, a także prowadzi działalność umożliwiającą promocję i marketing we Francji narzędzi opracowanych przez AEC, to obydwa kryteria określone w art. 3 (I) francuskiej ustawy o ochronie danych są spełnione, i w związku z tym CNIL jako organ właściwy może rozstrzygać sprawę na podstawie art. 82 tej ustawy.

---

[12] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 281, s. 31; dalej: dyrektywa 95/46/WE).

[13] Wyrok prejudycjalny TSUE w sprawie złożonego przez Bundesverwaltungsgericht (niemiecki federalny sąd administracyjny) zapytania w postępowaniu Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH, przy udziale: Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht, (TSUE, 5 czerwca 2018 r., C-210/16, pkt 53).

6.2. Komentarz

Niewątpliwie słabym punktem przepisów dyrektywy 2002/58/WE jest brak określenia w nich prawa właściwego do stosowania wobec tych czynności objętych tymi przepisami. Należy podkreślić, że w związku z taką luką, ustawodawcy krajowi mają swobodę w określaniu kryteriów stosowania prawa danego państwa w sprawach dotyczących ochrony prywatności i łączności elektronicznej. Z możliwości takiej skorzystał legislator francuski, który dla transgranicznych spraw z zakresu ochrony prywatności przyjął takie przesłanki terytorialnego stosowania ustawy, jak to określono w art. 4 dyrektywy 95/46/WE, która została następnie uchylona przepisami RODO. Ustanie obowiązywania przepisów dyrektywy 95/46/WE nie skutkuje jednak brakiem możliwości posługiwania się nadal kryteriami określonymi w jej art. 4 w zakresie, w jakim stosują się one do spraw objętych dyrektywą 2002/58/WE. Jest to konsekwencja omawianej już powyżej niezależności reżimów ochrony danych osobowych oraz prywatności w sektorze łączności elektronicznej. Z tych przyczyn treść art. 3 (I) ustawy francuskiej i związaną z tym interpretację CNIL należy uznać za dopuszczalną, choć niewątpliwie nieco konstrukcyjnie „karkołomną".

W związku z powyższym, warto również podkreślić, że jeszcze większe kontrowersje wywołuje ocena transgranicznych spraw z zakresu obowiązywania dyrektywy 2002/58/WE, w sytuacjach gdy prawo krajowe państwa, w którym dochodzi do dokonania czynności objętych tą regulacją, nie zawiera – tak jak ustawa francuska – norm wskazujących właściwość prawa. W takich sytuacjach generalnie możliwe jest przyjęcie dwóch alternatywnych rozwiązań. Po pierwsze, można przyjąć zasadę „państwa pochodzenia", zgodnie z którą właściwe jest państwo członkowskie Unii Europejskiej, w której siedzibę ma podmiot dokonujący danej instalacji cookies. Po drugie, można kierować się zasadą „państwa przeznaczenia", zgodnie z którą decydujące jest terytorium państwa, w którym znajduje się urządzenie użytkownika, na jakim dochodzi do zapisania i odczytu cookies. Wobec braku orzecznictwa w tym zakresie (również w Polsce), opowiadam się za drugim z powyższych stanowisk z następujących powodów.

Po pierwsze, sprawy ochrony danych osobowych zostały w dyrektywie 2000/31/WE[14] wyraźnie wyłączone z zakresu jej stosowania, a zatem i z określonej w niej zasady państwa pochodzenia dotyczącej usług społeczeństwa informacyjnego (art. 1 ust. 5 lit. b).

Po drugie, w przypadku usług łączności elektronicznej, za decydujące kryterium dla określenia prawa właściwego przyjmuje się miejsce świadczenia usługi telekomunikacyjnej (usługi łączności elektronicznej). Zatem w przypadku, gdy problematyka instalowania cookies na urządzeniach użytkowników regulowana jest aktem prawnym właściwym dla łączności elektronicznej, to wówczas do rozstrzygania spraw dotyczących

[14] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz. Urz. WE L 178, s. 1).

ewentualnych naruszeń w tym zakresie właściwy będzie organ ds. telekomunikacji państwa, w którym do naruszeń doszło.

Przenosząc powyższe uwagi na grunt prawa polskiego, należy stwierdzić, że ze względu na fakt, że w prawie polskim regulacja dotycząca cookies zawarta jest w przepisach o łączności elektronicznej, w szczególności art. 173 ustawy – Prawo telekomunikacyjne, trzeba przyjąć, że Prezes UKE – jako organ odpowiadający za przestrzeganie zasad określonych w tych przepisach – będzie właściwy wówczas, gdy instalacji i odczytu cookies dokona podmiot znajdujący się na terytorium Polski (kryterium miejsca świadczenia usługi lub zasada państwa przeznaczenia).

7. Zasady dopuszczalnego instalowania i dostępu do informacji przechowywanych w cookies

7.1 Argumentacja AEC i CNIL

W trakcie prowadzonego postępowania spółka AEC twierdziła, że należycie spełniła wymogi art. 82 ustawy francuskiej poprzez należyte spełnienie obowiązku informacyjnego oraz pozyskiwanie wymaganych prawem zgód użytkownika na instalację cookies. Spółka AEC twierdziła w szczególności, że po naciśnięciu linku „Find out more" znajdującego się na banerze informacyjnym dostępnym na stronie amazon.fr, użytkownik był przekierowywany do tzw. polityki cookies. W przypadku natomiast, gdy użytkownik na stronę amazon.fr trafiał poprzez przekierowanie z reklamy dostępnej na witrynie podmiotu trzeciego, to wówczas wyświetlana mu była również ikona „AdChoices", która kierowała go do strony z informacjami dotyczącymi zasad prowadzenia targetowanej reklamy. Spółka AEC wskazała również, że dodatkowo w dolnej części strony znajdują się odnośniki (linki) do stron, w których opisana jest tzw. polityka cookies oraz polityka prowadzenia reklamy targetowanej. W podsumowaniu, spółka zauważyła również trudność w spełnieniu obowiązków w zakresie cookies, ponieważ brak jest jednolitego stanowiska organów nadzorczych w poszczególnych państwach Unii Europejskiej.

Z powyższymi argumentami nie zgodził się CNIL, zarzucając spółce niewykonanie lub nienależyte wykonanie obowiązku informacyjnego oraz wadliwe pozyskiwanie zgody użytkowników. Organ w pierwszej kolejności zarzucił spółce AEC, że w umieszczanych na stronie domowej informacjach zbyt ogólnie opisywano wszystkie cele, dla których instalowane były cookies różnego rodzaju. W szczególności informacja o tym, że pliki są umieszczane na urządzeniach użytkowników w celu „oferowania i polepszenia świadczenia usług" nie pozwala użytkownikowi ocenić, jakiego rodzaju działania reklamowe będą w stosunku do niego prowadzone na podstawie tak zebranych danych. Tego rodzaju ogólna informacja nie zawierała również wymaganego prawem opisu środków (sposobów), za pomocą których użytkownik może się sprzeciwić zapisowi i odczytowi cookies. Podobnie – strona, do której przekierowywała ikona „AdChoices",

również nie zawierała informacji o celach zapisywania plików cookies oraz możliwości wyrażenia odmowy na tę czynność, a jedynie informację, że użytkownik poprzez zaznaczenie odpowiedniego pola może zażądać, aby nie były wyświetlane reklamy na podstawie jego zainteresowań. Według CNIL, za niewystarczające, z punktu widzenia spełnienia obowiązku informacyjnego, należało również uznać umieszczenie na stronie domowej linku do tzw. polityki cookies.

Francuski organ ds. ochrony danych osobowych stwierdził również, że w rozstrzyganej sprawie nie zachodziły wyjątki od konieczności uzyskania zgody użytkowników, a sposób jej pozyskania przez AEC nie spełniał wymogów określonych w art. 82 ustawy francuskiej. Pliki cookies były bowiem instalowane zaraz po wejściu użytkowników na stronę amazon.fr, bez możliwości zapoznania się przez nich z – nawet niekompletną – informacją na temat tego, jak zbierane w ten sposób dane będą wykorzystywane. Co istotne, CNIL nie zakwestionował argumentu spółki AEC, że zgoda taka może być – co do zasady – pozyskana za pomocą odpowiednich ustawień przeglądarki, ale podkreślił, że w każdym przypadku musi ją poprzedzać przekazanie informacji wymaganych prawem, czego AEC nie czynił.

W świetle powyższego, CNIL stwierdził, że naruszenie przepisów art. 82 francuskiej ustawy o ochronie danych polega na tym, że spółka umieszcza pliki cookies na terminalu użytkowników znajdujących się na terytorium Francji, przed uzyskaniem ich zgody i bez dostarczenia im informacji przewidzianych w tym artykule oraz na określonych w nim warunkach.

7.2. Komentarz

Zarówno samo rozstrzygnięcie, jak i uzasadnienie decyzji CNIL w części dotyczącej spełnienia wymogów określonych w art. 82 ustawy francuskiej nie budzi większych kontrowersji, ponieważ uchybienia AEC w zakresie spełnienia obowiązku informacyjnego oraz pozyskania zgody były oczywiste.

Francuski organ ds. ochrony danych osobowych prawidłowo ocenił, że w analizowanym stanie faktycznym nie zachodził żaden z wyjątków od obowiązku informacyjnego, określonych w ustawie. Trafna jest również konstatacja, że z prawnego punktu widzenia, nie ma znaczenia, w jaki sposób użytkownik trafia na witrynę internetową, czy bezpośrednio, czy poprzez reklamę umieszczoną na stronie podmiotu trzeciego. W obydwu przypadkach taki sam jest zakres obowiązków, które należy wypełnić, zgodnie z przepisami krajowymi implementującymi przepis art. 5 ust. 3 dyrektywy 2002/58/WE.

Nie budzi także wątpliwości, że instalacja plików cookies powinna nastąpić po otrzymaniu przez użytkownika ww. informacji, a nie – jak to było w stanie faktycznym sprawy – równocześnie z dokonaniem tej czynności. Wynika to bezpośrednio z treści art. 82 ustawy francuskiej i stanowiącej pierwowzór tego przepisu art. 5 ust. 3 dyrektywy 2002/58/WE.

Jeżeli chodzi o zakres informacji, które użytkownik powinien otrzymać, to w art. 5 ust. 3 dyrektywy 2002/58/WE wskazano cele przetwarzania, a więc cele, dla których

informacje są przechowywane na urządzeniach końcowych użytkowników po to, aby następnie podmiot instalujący cookies, miał do nich dostęp. Administratorzy powinni więc określić, czy instalowane są np. cookies wydajnościowe, funkcjonalne, analityczne, reklamowe itp. Francuski ustawodawca poszerzył w art. 82 zakres udzielanych informacji o obowiązek podania informacji o środkach wyrażenia sprzeciwu na instalację cookies. Taki zabieg jest dopuszczalny, w przypadku dyrektywy 2002/58/WE mamy bowiem do czynienia z wymogiem minimalnej harmonizacji. Pozostawia to możliwość ustalenia przez państwa Unii Europejskiej wymagań bardziej rygorystycznych niż określone w dyrektywie.

Prawidłowe jest również ustalenie CNIL, zgodnie z którym ww. informacje, określone w art. 82 ustawy francuskiej, powinny być widoczne zaraz po wejściu na witrynę internetową i nie mogą być ukryte np. w tzw. polityce cookies, dostępnej dopiero po naciśnięciu odpowiedniego linku na (internetowej) stronie domowej. Należy w związku z tym rekomendować spełnianie obowiązku informacyjnego w taki sposób, aby pierwsza warstwa, która wyświetla się w momencie wejścia użytkownika na stronę, zawierała istotne informacje (tj. informację o stosowaniu plików cookies i ich celach oraz sposobie, w jaki użytkownicy mogą akceptować, konfigurować i odrzucać używanie takich plików), natomiast druga warstwa powinna zawierać szczegółowe informacje o plikach cookies. Informacje te powinny być łatwo dostępne dla użytkownika, np. z wykorzystaniem linku do „polityki cookies" czy też „polityki prywatności".

Podsumowanie

Najbardziej interesujące elementy uzasadnienia decyzji CNIL dotyczą określenia właściwości rzeczowej organu w sprawach dotyczących cookies, a także zastosowania prawa francuskiego do działalności podmiotów mających siedzibę w innym państwie Unii Europejskiej i korzystających z informacji zapisanych w cookies umieszczanych na urządzeniach położonych na terytorium Francji. Należy w związku z tym podkreślić specyfikę rozwiązań przyjętych przez ustawodawcę francuskiego. Po pierwsze, CNIL w ustawie o ochronie danych osobowych umocowany został nie tylko do egzekwowania przepisów RODO, ale również przepisów implementujących dyrektywę 2002/58/WE. Po drugie, przy określaniu terytorialnej właściwości przepisów francuskich w sprawach z zakresu dyrektywy o e-prywatności posłużono się takimi przesłankami, jak określone w art. 4 dyrektywy 95/46/WE, uchylonej następnie przepisami RODO.

Z powyższych względów, argumentacji przedstawionej przez francuski organ ds. ochrony danych osobowych nie można stosować w sprawach rozstrzyganych na gruncie przepisów prawnych tych państw Unii Europejskiej, które transponowały przepisy dyrektywy 2002/58/WE do sektorowych regulacji łączności elektronicznej, a także – inaczej niż ustawodawca francuski – w swoich przepisach nie wprowadziły norm określających właściwość terytorialną w tych sprawach. Przykładem jest polski system prawny, w ramach którego przepis art. 5 ust. 3 dyrektywy 2002/58/WE

implementowano w art. 173 u.p.t., a w ustawie tej nie określono również odrębnie zakresu terytorialnego jego stosowania. W konsekwencji, inaczej niż w analizowanej sprawie Amazon Europe Core, w sprawach dotyczących cookies, właściwy jest wyłącznie Prezes Urzędu Komunikacji Elektronicznej, którego zakres kompetencji obejmuje ocenę zgodności z prawem instalacji i odczytu cookies dokonywanych przez podmiot znajdujący się na terytorium Polski.

Streszczenie

Xawery Konarski

Administracyjna kara finansowa w sprawie *cookies*.
Komentarz na kanwie postanowienia Krajowej Komisji Informatyki i Wolności we Francji (CNIL) z dnia 7 grudnia 2020 r. w sprawie *Amazon Europe Core*, SAN-2020-013

Problematyka prawna korzystania z identyfikatorów internetowych takich jak pliki cookies jest jedną z najczęściej poruszanych w kontekście ochrony prywatności i danych osobowych użytkowników usług łączności elektronicznej. Zasady korzystania z nich stały się w ostatnich latach przedmiotem szeregu orzeczeń Trybunału Sprawiedliwości Unii Europejskiej (TSUE), a także decyzji organów regulacyjnych w poszczególnych państwach UE. Istotną decyzję w tym zakresie wydał w dniu 7 grudnia 2020 r. francuski organ ds. ochrony danych osobowych (CNIL), nakładając karę pieniężną za naruszenie francuskich przepisów dotyczących cookies przez spółkę Amazon (SAN-2020-013).

W kontekście powyższej decyzji, należy podkreślić specyfikę rozwiązań przyjętych przez ustawodawcę francuskiego. Po pierwsze, CNIL w ustawie o ochronie danych osobowych umocowany został nie tylko do egzekwowania przepisów RODO, ale również przepisów implementujących dyrektywę 2002/58/WE. Po drugie, przy określaniu terytorialnej właściwości przepisów francuskich w sprawach z zakresu dyrektywy o e-prywatności, posłużono się takimi przesłankami, jak określone w art. 4 dyrektywy 95/46/WE, uchylonej następnie przepisami RODO.

Z powyższych względów, przedstawionej przez francuski organ ds. ochrony danych osobowych argumentacji, nie można stosować w sprawach rozstrzyganych na gruncie przepisów prawnych tych państw Unii Europejskiej, które transponowały przepisy dyrektywy 2002/58/WE do sektorowych regulacji łączności elektronicznej, a także – inaczej niż ustawodawca francuski – w swoich przepisach nie wprowadziły norm określających właściwość terytorialną w tych sprawach. Przykładem jest polski system prawny, w ramach którego przepis art. 5 ust. 3 dyrektywy 2002/58/WE implementowano w art. 173 ustawy – Prawo telekomunikacyjne.

Słowa kluczowe: RODO; przepisy o e-Prywatności; pliki cookies; zgoda użytkownika; właściwość organów administracji.

Summary

Xawery Konarski

**Administrative Fine Concerning Installation of Cookies.
Comment on the Order of the National Commission for Information Technology and Freedoms in France (CNIL) of 7 December 2020 in the *Amazon Europe Core Case*, SAN-2020-013**

The legal problem of the use of online identifiers such as cookies is one of the most frequently addressed in the context of protecting the privacy and personal data of users of electronic communications services. In recent years, the principles of their use have been the subject of a number of decisions of the Court of Justice of the European Union (CJEU), as well as decisions issued by regulatory bodies in several EU countries. An important decision in this regard was issued on December 7, 2020 by the French data protection authority – National Commission for Information Technology and Freedoms (CNIL), imposing on Amazon company an administrative fine for violating French cookie laws (reference SAN-2020-013).

In the context of the above decision, the specificity of the solutions adopted by the French legislator should be underlined. First, the CNIL has been empowered by the French Data Protection Act to enforce not only the provisions of the GDPR, but also the provisions implementing Directive 2002/58/EC. Secondly, the territorial jurisdiction of the French legislation in matters falling under the scope of the ePrivacy Directive follows the same rationale as Article 4 of Directive 95/46/EC, subsequently repealed by the GDPR provisions.

For the foregoing reasons, the reasoning put forward by the French data protection authority cannot be applied to cases decided under the legislation of those European Union members states which have transposed the provisions of Directive 2002/58/EC into the sectoral regulation of electronic communications and, unlike the French legislator, have not introduced rules in their legislation designating territorial jurisdiction in such cases. An example is the Polish legal system, where the provision of Article 5(3) of Directive 2002/58/EC has been implemented in Article 173 of the Act on Telecommunications Law.

Keywords: GDPR; e-Privacy provisions; cookies; user's consent; competence of administrative authorities.

Michał Czerniawski
michael.czerniawski@gmail.com
Vrije Universiteit Brussel
ORCID: 0000-0002-8051-1294

https://doi.org/10.26881/gsp.2021.4.07

Rola Komitetu Art. 93 RODO w procedurze oceny adekwatności państw trzecich

1. Wstęp

W dobie globalizacji i społeczeństwa informacyjnego, transfery danych osobowych są niezbędnym elementem rozwoju gospodarki cyfrowej[1]. Nie powinno budzić wątpliwości, że istnieje potrzeba funkcjonowania efektywnych instrumentów, które umożliwiają ponadnarodową wymianę danych osobowych. Rozwiązania te muszą gwarantować należytą ochronę przekazywanych informacji, a ponadto, o czym nieraz się zapomina, powinna istnieć procedura nadzoru nad ich przyjmowaniem i oceny ich zgodności z unijnymi przepisami nie tylko *ex post*, w szczególności przez Trybunał Sprawiedliwości Unii Europejskiej (TSUE), ale także *ex ante* – w tym zakresie odpowiednie zadania spoczywają na Europejskiej Radzie Ochrony Danych (EROD), która udziela Komisji Europejskiej (Komisja) swojej opinii, oraz – będącej przedmiotem niniejszego opracowania – procedurze komitetowej. Z perspektywy Unii Europejskiej i ochrony praw podstawowych, wypracowywanie odpowiednich rozwiązań w obszarze transferów danych nie jest zadaniem łatwym, choćby dlatego, że poziom ochrony danych osobowych w poszczególnych państwach świata jest bardzo zróżnicowany, a tylko kilkanaście z nich wprowadziło standardy porównywalne z wymogami unijnymi.

Adekwatność ochrony danych osobowych, czyli model oceny zgodności przepisów państw trzecich z zasadami ochrony danych osobowych, wprowadzony został do unijnego porządku prawnego wraz z dyrektywą 95/46/WE[2]. Ewoluował on na

[1] Za wciąż aktualne, pomimo upływu dwunastu lat, można uznać następujące obserwacje: „Obecnie jesteśmy świadkami szybkiego rozwoju społeczeństwa informacyjnego, społeczeństwa, w którym niezwykle cennym towarem stało się szczególne dobro niematerialne jakim jest informacja. Taki stan rzeczy jest w dużej mierze skutkiem rosnącej łatwości przekazywania informacji oraz powszechność dostępu do otwartej sieci teleinformatycznej – Internetu. W ciągu ostatnich kilku lat skala przetwarzania danych osobowych osiągnęła niespotykane nigdy przedtem rozmiary i aktualnie transfer danych osobowych jest elementem niezbędnym do prawidłowego funkcjonowania globalnego rynku" – zob. M. Czerniawski, *Transfer danych osobowych z terytorium Polski do państwa trzeciego niezapewniającego odpowiedniego poziomu ochrony danych osobowych*, Przegl. Prawn. UW 2009, nr 3–4, s. 11.

[2] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 281, s. 31; dalej: dyrektywa 95/46/WE).

przestrzeni lat i obecnie obejmuje dwa rodzaje adekwatności: zgodnie z ogólnym rozporządzeniem o ochronie danych[3] oraz zgodnie z tzw. dyrektywą policyjną[4]. Jak wskazuje się w art. 45 ust. 1 RODO, przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Analogicznym przepisem dyrektywy policyjnej jest jej art. 36 ust. 1. Standardy ochrony danych osobowych, które Unia Europejska uznała za podobne do swoich, wprowadziły dotychczas jedynie państwa należące do Europejskiego Obszaru Gospodarczego (które *de facto* implementowały do swoich porządków prawnych część przepisów wspólnotowych) oraz następujące państwa świata: Andora, Argentyna, Guernsey, Izrael, Japonia, Jersey, Kanada (tylko w odniesieniu do podmiotów objętych PIPEDA[5]), Nowa Zelandia, Szwajcaria, Wyspa Man, Urugwaj, Wielka Brytania (wobec której po raz pierwszy wydano dwie decyzje - dotyczącą RODO i dotyczącą LED) oraz Wyspy Owcze[6]. Warto odnotować, że tylko decyzje dotyczące poziomu ochrony zapewnianego przez Japonię oraz Wielką Brytanię, zostały wydane w oparciu o kryterium merytorycznej równoważności (*essentially equivalent*), wprowadzonego w wyroku Trybunału Sprawiedliwości w sprawie *Schrems II*[7]. Obecnie Komisja Europejska kończy prace nad analizą decyzji o adekwatności wydanych pod rządami dyrektywy 95/46/WE, weryfikując czy spełniają one wymogi ustanowione w orzecznictwie TSUE, a publikacji odpowiedniego raportu należy spodziewać się w najbliższych miesiącach. W momencie zakończenia prac nad niniejszym artykułem, toczą się prace nad decyzją w sprawie adekwatności Korei Południowej.

Stałym elementem modelu adekwatności, obecnym od samego początku jego funkcjonowania, jest procedura komitetowa – tzw. komitologia. W ramach komitologii

---

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1; dalej: RODO).

[4] Dyrektywa 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 (Dz. Urz. UE L 119, s. 89; dalej: LED, dyrektywa policyjna).

[5] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

[6] Lista państw zapewniających odpowiedni do unijnego poziom ochrony danych osobowych jest dostępna na stronie Komisji Europejskiej: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [dostęp: 11.11.2021]. Przytłaczająca większość państw na świecie nie spełnia wymogów unijnych, które warunkują możliwość swobodnego eksportu danych osobowych z terytorium UE do państw trzecich. W praktyce oznacza to olbrzymią liczbę transferów danych osobowych wykonywanych z krajów Europejskiego Obszaru Gospodarczego do państw niezapewniających adekwatnego poziomu ochrony, a więc w oparciu o mechanizmy przewidziane w art. 46-49 RODO.

[7] Wyrok TS z dnia 16 lipca 2020 r. w sprawie C-311/18, *Data Protection Commissioner przeciwko Facebook Ireland Ltd. Maximillian Schrems*, ECLI:EU:C:2020:559.

wydawana jest, w drodze głosowania, formalna opinia w sprawie projektów aktów wykonawczych opracowanych przez Komisję – w tym przypadku projektów decyzji wykonawczych Komisji Europejskiej stwierdzających odpowiedni stopień ochrony danych osobowych przez państwo trzecie.

Pod rządami dyrektywy 95/46/WE, komitetem właściwym do kontrolowania działań Komisji w tym zakresie był komitet ustanowiony na podstawie jej art. 31 (Komitet Art. 31); (obecnie jest to Komitet Art. 93)[8]. Działalność komitetu pozostaje w cieniu opinii dotyczących projektów decyzji o adekwatności wydawanych przez EROD czy rezolucji Parlamentu Europejskiego, pełni on natomiast kluczową rolę w całej procedurze, kontrolując działania Komisji Europejskiej w odniesieniu do oceny poziomu ochrony danych osobowych w państwach trzecich. Skupiający przedstawicieli państw członkowskich, komitet może zablokować wydanie decyzji o adekwatności.

Komitologia, pomimo jej istotnej funkcji w procesie wydawania decyzji o adekwatności i realnego wpływu na kształt tych decyzji, pozostaje praktycznie niezauważona. Jedną z przyczyn takiego stanu rzeczy jest z pewnością ograniczona transparentność podejmowanych w jej ramach działań oraz brak szerszych informacji dotyczących funkcjonowania samego komitetu – informacje o jego aktywności, przekazywane przez Komisję Europejską w ramach rejestru komitologii, mają charakter bardzo lakoniczny i są dostępne jedynie poprzez ogólny rejestr wszystkich procedur komitetowych, często z pewnym opóźnieniem. Z jednej strony, taki stan rzeczy pozwala chronić kulisy unijnego procesu decyzyjnego, z drugiej – utrudnia dostęp do nawet najbardziej podstawowych informacji dotyczących jego przebiegu.

Jak wskazano w niniejszym opracowaniu, komitet pracuje zazwyczaj pod presją Komisji Europejskiej, mając ograniczony czas na podjęcie decyzji. Choć w procedurze komitetowej uczestniczą przedstawiciele państw członkowskich posiadający wiedzę w obszarze ochrony danych osobowych, wydaje się, że partycypacja ekspertów zewnętrznych, przede wszystkim EROD i Europejskiego Inspektora Ochrony Danych (EIOD), wpłynęłaby pozytywnie na prace komitetu i pozwoliłaby na większy pluralizm

[8] Zgodnie z motywem 167 RODO, Komisji powierza się uprawnienia wykonawcze, które muszą być wykonywane zgodnie z rozporządzeniem (UE) nr 182/2011. Motyw ten wskazuje na konieczność brania pod uwagę potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Motyw 168 RODO z kolei wskazuje, że procedura komitetowa znajduje zastosowanie w stosunku do aktów wykonawczych dotyczących: standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi oraz między podmiotami przetwarzającymi; kodeksów postępowania; technicznych standardów i mechanizmów certyfikacji; odpowiedniego stopnia ochrony zapewnianego przez państwo trzecie, terytorium lub określony sektor w tym państwie trzecim lub organizację międzynarodową; standardowych klauzul ochrony danych; formatów i procedur wymiany informacji drogą elektroniczną między administratorami, pomiotami przetwarzającymi i organami nadzorczymi na potrzeby wiążących reguł korporacyjnych; wzajemnej pomocy; oraz uzgodnień w sprawie wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych. Motyw 169 RODO reguluje zaś kwestię aktów wykonawczych mających natychmiastowe zastosowanie. Wskazuje on, że Komisja powinna przyjmować tego typu akty, jeżeli z dostępnych dowodów wynika, że państwo trzecie, terytorium lub określony sektor w tym państwie trzecim lub organizacja międzynarodowa nie zapewniają odpowiedniego stopnia ochrony, i jeżeli zachodzi szczególnie pilna potrzeba działania.

prezentowanych na jego forum poglądów. Dopuszczenie, pod określonymi warunkami, ekspertów dałoby przedstawicielom państw członkowskich jeszcze pełniejszy ogląd sytuacji i przepisów prawa, których dotyczy projekt decyzji Komisji Europejskiej, a przez to – szerszą wiedzę, w oparciu o którą wydawaliby swoją opinię.

2. Czynniki wpływające na decyzje o adekwatności państw trzecich

Decyzje o adekwatności są podejmowane przez Komisję Europejską nie tylko wyłącznie w oparciu o przesłanki prawne, ale od dawna mają także swój wymiar polityczny oraz ekonomiczny. Dotychczas beneficjentem swoistego specjalnego traktowania w tym zakresie były Stany Zjednoczone Ameryki[9]; to USA umożliwiono stworzenie po kolei dwóch specjalnych mechanizmów samocertyfikacji: tzw. Bezpiecznej Przystani (*Safe Harbour*) oraz tzw. Tarczy Prywatności (*Privacy Shield*), oba z nich uzyskały decyzje o zapewnianiu odpowiedniego poziomu ochrony danych osobowych. Obecnie, po unieważnieniu adekwatności obu tych instrumentów przez TSUE[10], rozpoczęły się prace nad kolejnym tego typu mechanizmem, mającym umożliwić swobodny przepływ danych osobowych pomiędzy Unią Europejską a Stanami Zjednoczonymi Ameryki[11].

Ministerstwo Administracji i Cyfryzacji[12] w swoim raporcie z 2014 r. poświęconym programowi „Bezpieczna Przystań" wprost wskazywało na czynniki inne niż ochrona danych osobowych, które mogą mieć wpływ na ocenę adekwatności państw trzecich. Przede wszystkim resort wskazywał na czynnik polityczny: „Mając na względzie komplikacje, jakie potencjalnie mogą wyniknąć z braku adekwatności ochrony danych, tak Unia Europejska, jak i USA uznały, że powinien istnieć instrument, który pozwoli na przekazywanie danych osobowych z terytorium UE do USA"[13]. Ministerstwo Administracji i Cyfryzacji stwierdzało też wprost: „Zarówno strona europejska, jak i amerykańska podczas prac nad zasadami »bezpiecznej przystani« mogła pójść na pewne

[9] Szerzej na ten temat zob. M. Czerniawski, *Transfer*…, s. 12.

[10] Zob. odpowiednio Wyrok Trybunału z dnia 6 października 2015 r. ws. C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner*, ECLI:EU:C:2020:559 oraz wyrok ws. C-362/14, *Data Protection Commissioner przeciwko Facebook Ireland Ltd. Maximillian Schrems*, ECLI:EU:C:2015:650.

[11] Zgodnie z informacjami prezentowanymi przez Komisję Europejską, zintensyfikowano prace nad nowym instrumentem – zob. wspólne oświadczenie prasowe komisarza ds. sprawiedliwości Didiera Reyndersa i sekretarz handlu USA Giny Raimondo, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443 [dostęp: 11.11.2021].

[12] W przeszłości rząd polski w procedurze komitologii przewidzianej w art. 31 dyrektywy 95/46/WE reprezentowali przedstawiciele Ministerstwa Administracji i Cyfryzacji, a następnie Ministerstwa Cyfryzacji. Zob. M. Czerniawski, komentarz do art. 93 [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2017, s. 1123.

[13] Ministerstwo Administracji i Cyfryzacji, Departament Społeczeństwa Informacyjnego, Analiza Programu „Bezpieczna Przystań" („Safe Harbour") w zakresie przekazywania danych osobowych z terytorium Polski do odbiorców w Stanach Zjednoczonych Ameryki, Warszawa, stan prawny na dzień 10 kwietnia 2014 r., s. 4

ustępstwa, istniała bowiem silna polityczna wola wypracowania kompromisu, nawet kosztem pewnych ustępstw"[14].

Poza kwestiami politycznymi, MAiC wskazywało także na czynnik ekonomiczny i rolę Stanów Zjednoczonych jako jednego z największych partnerów handlowych Unii Europejskiej: „Decyzja Komisji Europejskiej w sprawie uznania adekwatności »bezpiecznej przystani« ma nie tylko kontekst prawny, ale także swój aspekt ekonomiczny – brak rozwiązań umożliwiających efektywne przekazywanie danych osobowych z terytorium Unii Europejskiej do USA mógłby mieć negatywny wpływ na pozycję europejskich, w tym polskich, przedsiębiorstw na globalnym rynku. Mógłby on też mieć niekorzystny wpływ na rozwój usług społeczeństwa informacyjnego – Internet nie zna granic, a duża część największych, najbardziej innowacyjnych firm działających *online*, z usług których na co dzień korzystają m.in. Polacy oraz polskie przedsiębiorstwa ma swoje siedziby w USA"[15]. W tym kontekście warto odnotować, że obecnie w 2021 r. koszty ewentualnego całkowitego wstrzymania transferów danych osobowych pomiędzy Unią Europejską a Stanami Zjednoczonymi Ameryki niektórzy badacze szacują na setki miliardów euro[16].

3. Od Komitetu Art. 31 dyrektywy 95/46/WE do Komitetu Art. 93 RODO

Procedura komitetowa lub też komitologia jest procesem przyjmowania przez Komisję Europejską aktów wykonawczych do unijnych aktów prawnych. Kompetencje wykonawcze są przekazywane Komisji w akcie prawnym, którego dotyczą – w obszarze ochrony danych osobowych była to w przeszłości dyrektywa 95/46/WE, a obecnie odniesienia do procedury komitetowej znajdują się w RODO, rozporządzeniu 2018/1725[17] oraz w dyrektywie policyjnej. Podczas wykonywania tych kompetencji, gdy tak zdecydował unijny prawodawca, Komisja jest wspierana przez komitet – stąd

[14] *Ibidem.*

[15] *Ibidem.*

[16] Tytułem przykładu zob. raport Analyst Group (R. Kepes, J. White i A. Yeater), *The importance of cross-border data flows. An economic assessment of restrictions on extra-EU data transfers*. Autorzy przeanalizowali skutek wstrzymania transferów danych dla wybranych branż, natomiast wnioski z ich raportu pokazują skalę możliwych kosztów także dla innych sektorów gospodarki: *Across telecommunications, digital payments, global services outsourcing, and pharmaceutical R&D, the quantifiable harm that could be caused by restricting personal data flows is significant. Moreover, due to the extensive use of data and personal data in many other industries, the case studies described in this report serve only as examples of the types and magnitudes of impact of a policy that restricts the transfer of personal data to third countries*. Należy odnotować, że badanie zostało sfinansowane przez Facebook.

[17] Rozporządzenie Parlamentu Europejskiego i Rady 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz. Urz. UE L 295, s. 39; dalej: rozporządzenie 2018/1725).

też nazwa całej procedury. Komitet składa się z ekspertów państw członkowskich, których pracom przewodniczy przedstawiciel Komisji.

Należy zgodzić się ze stanowiskiem, że procedura komitologii to próba wprowadzenia mechanizmów kontrolnych nad zwiększającymi się sukcesywnie kompetencjami Komisji w zakresie tworzenia i wykonywania (wdrażania) prawa UE[18], a jej celem jest *de facto* ochrona interesów państw członkowskich – w sytuacji coraz bardziej rosnących kompetencji Komisji Europejskiej w sferze tworzenia prawa unijnego. Ma ona za zadanie chronić rolę państw członkowskich jako „władców traktatu" (*masters of the treaty*)[19]. W tym kontekście pojawiają się pytania o to, czy silna pozycja komitetów, niemających przecież traktatowego umocowania w systemie decyzyjnym Unii Europejskiej, nie stanowi jednak zbyt mocnej ingerencji państw członkowskich w kompetencje przyznane instytucjom UE, zwłaszcza Komisji Europejskiej[20].

W przypadku komitetu zajmującego się kwestiami dotyczącymi ochrony danych osobowych, pomimo posiadania oficjalnej nazwy[21], przyjęto dla jego identyfikacji posługiwać się numerem artykułu, który w danym okresie stanowi podstawę prawną dla działania tego gremium. Zgodnie z art. 31 dyrektywy 95/46/WE, Komisja była wspierana przez komitet składający się z przedstawicieli państw członkowskich, na którego czele stał przedstawiciel Komisji. Artykuł 31 ust. 2 dyrektywy 95/46/WE stanowił, że przedstawiciel Komisji prezentuje komitetowi projekt środków, które należy podjąć. Komitet wydawał opinię o projekcie w terminie wyznaczonym przez przewodniczącego, zależnie od pilności sprawy, a opinie komitetu były przyjmowane większością głosów, przy czym przewodniczący nie brał udziału w głosowaniu[22]. Jeżeliby spojrzeć na statystyki prac Komitetu Art. 31, to działał on dość aktywnie – przez okres obowiązywania dyrektywy 95/46/WE odbył w sumie 73 posiedzenia; ostatnie spotkanie miało miejsce w dniu 15 listopada 2016 r.[23] Komitet Art. 31 zaprzestał funkcjonowania z dniem 25 maja 2018 r., to jest z dniem rozpoczęcia stosowania RODO, i został zastąpiony komitetem, o którym mowa w art. 93 tego aktu prawnego.

---

[18] Pogląd ten podzielają m.in. R. Grzeszczak – zob. *idem*, *Władza wykonawcza w systemie Unii Europejskiej*, Warszawa 2011, s. 236 oraz P. Tosiek – zob. *idem*, *Komitologia: szczególny rodzaj decydowania politycznego w Unii Europejskiej*, Lublin 2007, s. 332.

[19] P. Tosiek, *Komitologia: szczególny rodzaj*…, s. 107.

[20] R. Grzeszczak, *Władza wykonawcza*…, s. 241.

[21] Oficjalna nazwa zarówno Komitetu art. 31, jak i Komitetu art. 93 to *Committee on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.

[22] Ponadto, zgodnie z tym przepisem, Komisja mogła przyjąć środki, które stosowało się niezwłocznie. Jeżeli jednak środki te nie były zgodne z opinią komitetu, Komisja niezwłocznie powiadamiała o tym Radę. W takim przypadku: a) Komisja odraczała stosowanie podjętych środków o trzy miesiące od daty takiego powiadomienia; b) Rada, stanowiąc większością kwalifikowaną, mogła podjąć w tym terminie inną decyzję. W praktyce, nigdy z tej procedury nie skorzystano.

[23] Por. stronę Komisji Europejskiej poświęconą tej procedurze komitologii: https://ec.europa.eu/transparency/comitology-register/screen/committees/C27000/consult?lang=en [dostęp: 11.11.2021].

4. Charakterystyka procedury komitetowej

4.1. Głosowanie w Komitecie Art. 93

Procedurę komitologii reguluje szczegółowo unijne rozporządzenie 182/2011[24], w którym zróżnicowano także rodzaje procedur komitetowych. W przypadku Komitetu Art. 93, zastosowanie znajdzie co do zasady tzw. procedura sprawdzająca, o której mowa w art. 5 tego rozporządzenia, a w szczególnym przypadku – dotyczącym jedynie kompetencji wskazanych w art. 45 ust. 5 RODO, tj. uchylenia, zmiany lub zawieszenia decyzji o adekwatności – można mieć do czynienia również z procedurą nadzwyczajną. Zgodnie z zasadami procedury sprawdzającej, (art. 5 ust. 1 rozporządzenia 182/2011) i art. 4 ust. 2 Regulaminu Komitetu (*Rules of Procedure*), opinie komitetu przyjmowane są kwalifikowaną większością głosów. Artykuł 16 ust. 4 Traktatu o Unii Europejskiej[25] stanowi, że większość kwalifikowana to co najmniej 55% członków Rady, jednak nie mniej niż piętnastu z nich, reprezentujących państwa członkowskie, których łączna liczba ludności stanowi co najmniej 65% ludności Unii. Z kolei mniejszość blokująca musi obejmować co najmniej czterech członków Rady, w przeciwnym razie uznaje się, że większość kwalifikowana została osiągnięta.

Możliwe są trzy rodzaje rozstrzygnięć komitetu:

- pozytywna opinia komitetu wobec projektu aktu wykonawczego przedłożonego przez Komisję;
- negatywna opinia komitetu wobec projektu aktu wykonawczego przedłożonego przez Komisję;
- niewydanie przez komitet jakiejkolwiek opinii.

W przypadku gdy opinia komitetu jest pozytywna (tj. kwalifikowana większość państw członkowskich opowiedziała się za przyjęciem aktu wykonawczego), Komisja przyjmuje projekt aktu wykonawczego. Zgodnie z art. 4 ust. 3 Regulaminu Komitetu, istnieje możliwość wydania pozytywnej opinii przez aklamację, tj. bez formalnego głosowania. W praktyce Komisja zawsze dąży do rozstrzygnięcia głosowania przez konsensus, poddając projekt decyzji pod głosowanie tylko w przypadku sprzeciwu któregokolwiek z państw członkowskich wobec wydania decyzji przez aklamację bądź też w przypadku zastosowania procedury pisemnej. Konsensus osiągnięto choćby przy opiniowaniu pierwszej decyzji o adekwatności wydanej w oparciu o przepisy RODO – a więc przy udziale Komitetu Art. 93 – dotyczącej poziomu ochrony danych osobowych w Japonii. Była ona dyskutowana podczas pięciu spotkań komitetu, z czego podczas ostatniego odbyło się głosowanie. W sprawozdaniu z tego głosowania Komisja wskazała, że „komitet w drodze konsensusu pozytywnie zaopiniował środek

[24] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz. Urz. UE L 55, s. 13; dalej: rozporządzenie 182/2011).

[25] Traktat o Unii Europejskiej (wersja skonsolidowana) (Dz. Urz. UE C 326 z 2012 r., s. 13; dalej: TUE).

wykonawczy"[26]. Jeżeli opinia komitetu jest negatywna (tj. kwalifikowana większość państw członkowskich opowiedziała się przeciw przyjęciu aktu wykonawczego), Komisja nie przyjmuje projektu aktu. Komitet Art. 93, tak jak jego poprzednik, jest więc władny uniemożliwić Komisji wydanie aktu wykonawczego w proponowanym przez Komisję brzmieniu. Jeżeli Komisja uzna akt wykonawczy za konieczny, przewodniczący komitetu może przedstawić zmienioną wersję projektu aktu wykonawczego w ciągu dwóch miesięcy od wydania negatywnej opinii albo przedstawić do dalszej dyskusji projekt aktu wykonawczego komitetowi odwoławczemu w ciągu miesiąca od wydania takiej opinii[27].

W przypadku gdy komitet nie wyda żadnej opinii, tj. w sytuacji, w której nie uzyskano kwalifikowanej większości głosów ani za przyjęciem projektu aktu wykonawczego, ani za jego odrzuceniem, Komisja może przyjąć akt lub przedstawić jego nową, zmienioną wersję. Jednakże w takiej sytuacji, zgodnie z art. 5 ust. 4 lit. c rozporządzenia 182/2011, Komisja nie może przyjąć projektu aktu wykonawczego, gdy zwykłą większością głosów swoich członków komitet wyraził sprzeciw wobec jego przyjęcia. Także w sytuacji nieprzyjęcia projektu w wyniku braku opinii, jeżeli uważa się akt wykonawczy za konieczny (oceny tej dokonuje Komisja), przewodniczący może przedstawić zmienioną wersję tego aktu temu samemu komitetowi w ciągu dwóch miesięcy od głosowania albo przedstawić do dalszej dyskusji projekt aktu wykonawczego komitetowi odwoławczemu w ciągu miesiąca od głosowania.

Warto odnotować, że w mechanizmie komitologii głosy wstrzymujące się są *de facto* głosami przeciwko wydaniu pozytywnej opinii. Dzieje się tak, gdyż po pierwsze, głosowanie zmierza do zebrania większości kwalifikowanej za wydaniem pozytywnej opinii co do aktu wykonawczego. W związku z tym, każdy głos, który nie jest głosem „za", w praktyce takiej większości nie buduje – wstrzymanie się od głosu jest więc wygodnym rozwiązaniem dla państw członkowskich mających wątpliwości co do projektu aktu wykonawczego. Po drugie, w mojej ocenie, wydanie aktu wykonawczego bez pozytywnej opinii komitetu stanowiłoby dla Komisji ryzyko polityczne i świadczyłoby o tym, że mandat, w oparciu o który wydała ona w takich warunkach konkretny akt wykonawczy jest niezwykle słaby. Nie wydaje mi się, żeby Komisja zdecydowała się kiedykolwiek na takie ryzyko w obszarze kompetencji Komitetu Art. 93, zwłaszcza w kontekście decyzji o adekwatności, co do których należy się spodziewać, że mogą być one zaskarżone do Trybunału Sprawiedliwości Unii Europejskiej. Choćby ze względu na to, że w postępowaniach przed TSUE Komisja może potrzebować wsparcia państw członkowskich, wydanie decyzji przy sprzeciwie członków komitetu, będących

[26] Zgodnie z treścią sprawozdania z posiedzenia Komitetu w dniu 15 stycznia 2019 r., *The Committee delivered a positive opinion on the Implementing Measure by consensus*. Treść sprawozdania: https://ec.europa.eu/transparency/comitology-register/screen/documents/060401/1/consult?lang=en [dostęp: 11.11.2021].

[27] W praktyce działań zarówno Komitetu Art. 31, jak i Komitetu Art. 93 procedura odwoławcza nigdy nie miała miejsca. Szerzej o tej procedurze zob. – L. Tosoni, komentarz do art. 93 [w:] Ch. Kuner, L.A. Bygrave, Ch. Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary*, Oksford 2019, s. 1285–1286.

reprezentantami państw członkowskich, choć z prawnego punktu widzenia możliwe, w mojej ocenie, nie wydaje się prawdopodobne.

Przewodniczący do uzyskania opinii komitetu, w szczególności w sytuacji, gdy projekt aktu wykonawczego był już przedmiotem jego obrad, może skorzystać z procedury pisemnej. Zgodnie z art. 3 ust. 5 rozporządzenia 182/2011, w procedurze pisemnej przyjmuje się, że każdy członek komitetu, który przed upływem wyznaczonego terminu nie sprzeciwia się projektowi aktu wykonawczego lub nie wstrzymuje się wyraźnie od głosowania nad nim, wyraża swoją milczącą zgodę w odniesieniu do projektu aktu wykonawczego. W toku prac Komitetu Art. 93, procedura pisemna była stosowana w trakcie pandemii wirusa COVID-19, znalazła zastosowanie choćby przy ocenie adekwatności przepisów prawa Wielkiej Brytanii – zarówno dla RODO, jak i LED[28] oraz podczas opiniowania nowego zestawu standardowych klauzul umownych[29]. Należy odnotować, że Komitet Art. 93 może też zastosować procedurę nadzwyczajną, o której mowa w art. 8 rozporządzenia 182/2011, a która dotyczy aktów wykonawczych mających natychmiastowe zastosowanie. Jak wskazuje się w art. 8 ust. 1 ww. rozporządzenia, można ją zastosować „w przypadku należycie uzasadnionej szczególnie pilnej potrzeby" – w takiej sytuacji Komisja przyjmuje akt wykonawczy mający natychmiastowe zastosowanie, bez wcześniejszego przedstawienia go komitetowi, i pozostający w mocy przez okres nieprzekraczający sześciu miesięcy, chyba że akt podstawowy stanowi inaczej. Nie później niż czternaście dni po przyjęciu takiego aktu przewodniczący przedstawia go Komitetowi Art. 93 – w celu uzyskania jego opinii. Jeżeli opinia wydana przez komitet jest negatywna, Komisja natychmiast uchyla akt wykonawczy. Jak już wspomniano, procedura ta znajdzie zastosowanie jedynie w sytuacji wskazanej w art. 45 ust. 5 RODO.

4.2. Regulamin Komitetu Art. 93

W procedurze komitetowej, każdy komitet sam ustala zasady swojego działania, oczywiście w przewidzianych przez prawo UE ramach. Nie inaczej jest w przypadku Komitetu Art. 93, który działa w oparciu o przyjęty przez siebie regulamin, doprecyzowujący postanowienia rozporządzenia 182/2011. Regulamin komitetu został przyjęty podczas jego posiedzenia w dniu 21 września 2018 r. W porównaniu do regulaminu Komitetu Art. 31, wprowadzono w nim kilka istotnych zmian:

---

[28] Zob. *Written vote on the draft Commission Implementing Decisions on the adequate protection of personal data by the United Kingdom pursuant to Regulation (EU) 2016/679 and pursuant to Directive (EU) 2016/680*, https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD%282021%291032/consult?lang=en [dostęp: 11.11.2021].

[29] Zob. *Written vote on Draft Implementing Decision on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 and Article 29(7) of Regulation (EU) 2018/1725 and on Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679*, https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD%282021%29817/consult?lang=en [dostęp: 11.11.2021].

1) w art. 2 ust. 2 lit. b Regulaminu Komitetu usunięto wymóg formy pisemnej dla zgłaszania przez przedstawicieli państw członkowskich nowych punktów do porządku obrad. W praktyce powinno to pozwalać na zmianę agendy nawet tuż przed rozpoczęciem posiedzenia komitetu, co nie było możliwe zgodnie z regulaminem Komitetu Art. 31. Państwa członkowskie mają swobodę w proponowaniu kwestii mających być przedmiotem dyskusji, natomiast o ostatecznym kształcie agendy decyduje Komisja, jako przewodniczący komitetu;
2) jasno wskazano, że w każdym przypadku istotne zmiany w projektach aktów wykonawczych, które wymagają dogłębnej analizy, takie jak projekty decyzji stwierdzających odpowiedni stopień ochrony, przedkłada się nie później niż trzy dni kalendarzowe przed datą posiedzenia (art. 3 ust. 1 Regulaminu Komitetu). Takie postanowienie ma zapobiec pojawianiu się nowych wersji dokumentów tuż przed posiedzeniami i jest istotne w kontekście zapewniania państwom członkowskim odpowiedniego czasu na ocenę dokumentów przedłożonych przez Komisję;
3) dodano punkt dotyczący uczestnictwa w posiedzeniach Komitetu Art. 93 przedstawicieli Islandii, Norwegii, Lichtensteinu i Szwajcarii (art. 7 ust. 1 Regulaminu Komitetu).

Sekretariat komitetu zapewnia Komisja Europejska – Dyrekcja Generalna ds. Sprawiedliwości i Konsumentów (DG JUST), a jego pracom przewodniczy urzędnik Komisji[30]. Komisja zapewnia obsługę sekretariatu komitetu, a w razie potrzeby – również grupom roboczym utworzonym w jego ramach (art. 9 Regulaminu Komitetu). Ponadto, Komisja sporządza sprawozdania z posiedzeń komitetu (art. 10 Regulaminu Komitetu). Przewodniczący niezwłocznie, nie później niż w terminie jednego miesiąca od daty posiedzenia, przesyła projekt sprawozdania członkom komitetu. Mogą oni zgłaszać do niego uwagi na piśmie. Członkowie komitetu mają prawo zażądać zaprotokołowania swojego stanowiska. Przewodniczący odpowiada także za sporządzenie sprawozdania na potrzeby prowadzonego przez Komisję rejestru prac wszystkich komitetów, krótko opisującego każdy punkt porządku obrad i wyniki głosowania nad projektem aktu wykonawczego przedłożonego komitetowi. Tylko to sprawozdanie jest publicznie dostępne. Co istotne, w sprawozdaniu na potrzeby rejestru nie podaje się indywidualnego stanowiska poszczególnych państw członkowskich.

W skład komitetu wchodzi po jednym przedstawicielu z każdego kraju UE. Odpowiadają oni przed swoim państwem członkowskim i są związani instrukcjami uzgodnionymi na poziomie krajowym. Do udziału w posiedzeniach komitetu, prócz przedstawicieli państw członkowskich UE, zapraszani są także przedstawiciele Islandii, Liechtensteinu i Norwegii. Posiedzenia komitetu odbywają się w Brukseli (w trakcie pandemii COVID-19 odbywały się też posiedzenia zdalne), a Komisja przed każdym spotkaniem wysyła do organów krajowych zaproszenie, porządek obrad i projekt aktu wykonawczego – ma to miejsce nie później niż czternaście dni kalendarzowych przed datą posiedzenia. Należy podkreślić konieczność uczynienia przez Komisję zadość tym

[30] W momencie ukończenia prac nad niniejszym artykułem funkcję przewodniczącego Komitetu Art. 93 pełni Emmanuel Crabit, dyrektor w DG JUST.

wymogom formalnym – w przypadku innych procedur komitologii, niedochowanie terminów przewidzianych dla dystrybucji dokumentów, uznanych przez Trybunał Sprawiedliwości za „istotne zasady proceduralne", prowadziło nawet do nieważności całego aktu wykonawczego opiniowanego przez dany komitet[31]. Agenda spotkań opracowywana jest przez Komisję. Posiedzenie komitetu zwołuje przewodniczący bądź z własnej inicjatywy, bądź na wniosek zwykłej większości członków komitetu. Według mojej wiedzy, wszystkie dotychczasowe posiedzenia zarówno Komitetu Art. 93, jak wcześniej – Komitetu Art. 31, były zwoływane z inicjatywy Komisji Europejskiej.

Przekazanie agendy i projektów dokumentów z odpowiednim wyprzedzeniem jest szczególnie istotne po unijnej reformie ochrony danych osobowych, gdy komitet może dyskutować kwestie objęte zarówno RODO, rozporządzeniem 2018/1725, jak i dyrektywą policyjną. O ile w pracach Komitetu Art. 31 poszczególne państwa członkowskie reprezentowały co do zasady te same osoby, o tyle w pracach Komitetu Art. 93 skład reprezentacji państw członkowskich może być bardziej zróżnicowany, ponieważ często państwa członkowskie mają różnych ekspertów zajmujących się ogólną ochroną danych osobowych oraz przetwarzaniem danych osobowych objętym LED, odpowiedzialność za te prace spoczywa też często na poziomie krajowym na różnych resortach. Ponadto, w przypadku dyskusji poświęconych LED oraz w kwestiach dotyczących rozwoju dorobku Schengen, w pracach komitetu mogą brać przedstawiciele Szwajcarii, którzy nie są zapraszani na posiedzenia lub punkty obrad poświęcone kwestiom wynikającym z RODO oraz rozporządzenia 2018/1725.

Zgodnie z art. 3 ust. 3 rozporządzenia 182/2011, komitet wydaje opinię o projekcie aktu wykonawczego w terminie wyznaczonym przez przewodniczącego na podstawie pilności sprawy. Terminy powinny być proporcjonalne i umożliwiać członkom komitetu wczesne i skuteczne przeanalizowanie projektu aktu wykonawczego oraz wyrażenie swoich opinii. W praktyce jednak nie zawsze czas wyznaczony przez Komisję jest dostatecznie długi, aby umożliwić państwom członkowskim odpowiednią analizę przedkładanych dokumentów[32]. Jak już wspomniano, istotne zmiany w projektach aktów wykonawczych, które wymagają dogłębnej analizy, takie jak projekty decyzji stwierdzających odpowiedni stopień ochrony, Komisja przedkłada nie później niż trzy dni kalendarzowe przed datą posiedzenia.

Zgodnie z art. 5 ust. 1 Regulaminu Komitetu, każde państwo członkowskie traktowane jest jako jeden członek komitetu. Każdy członek komitetu decyduje o składzie swojej delegacji i informuje o nim przewodniczącego. Za zgodą przewodniczącego, delegacjom mogą towarzyszyć eksperci, którzy nie wchodzą w ich skład. Nie później niż pięć dni kalendarzowych przed datą posiedzenia komitetu, państwa członkowskie przekazują przewodniczącemu następujące informacje:

– skład każdej delegacji, chyba że przewodniczący już go zna;

---

[31] Tak L. Tosoni, komentarz do art. 93…, s. 1280. Zob. także wyrok TS z dnia 20 września 2017 r. ws. C-183/16 P, *Tilly-Sabco SAS*, pkt 114, ECLI:EU:C:2017:704.

[32] Zob. P. Tosiek, *Komitologia: szczególny rodzaj*…, s. 301.

– imiona i nazwiska oraz funkcje ekspertów towarzyszących delegacjom, a także powody, dla których ich obecność jest wymagana.

Jeżeli przed posiedzeniem komitetu przewodniczący nie wyrazi sprzeciwu wobec uczestnictwa eksperta, uważa się, że zgoda na jego udział została udzielona. Warto też dla porządku wspomnieć, że w toku spotkań komitetu, każdy przedstawiciel państwa członkowskiego może zabrać głos i zgłosić uwagi do projektu aktu wykonawczego. Ponadto, delegacja państwa członkowskiego może reprezentować jeszcze jedno inne państwo członkowskie. Państwo członkowskie reprezentowane w komitecie informuje o tym przewodniczącego przed posiedzeniem lub najpóźniej przed głosowaniem.

Zgodnie z art. 11 ust. 2 Regulaminu Komitetu, przedstawiciele państw członkowskich oraz zaproszeni eksperci informują przewodniczącego o jakimkolwiek konflikcie interesów odnośnie konkretnego punktu porządku obrad komitetu. W przypadku takiego konfliktu interesów na wniosek przewodniczącego dana osoba wycofuje się z udziału w posiedzeniu na czas omawiania odpowiednich punktów porządku obrad.

5. Kompetencje Komitetu Art. 93

Jak wskazuje się w art. 291 ust. 2 TFUE[33], akty wykonawcze są wydawane, gdy konieczne są jednolite warunki wykonywania prawnie wiążących aktów Unii. Większość uprawnień Komitetu Art. 93 dotyczy przekazywania danych osobowych do państw trzecich, tj. państw znajdujących się poza terytorium Europejskiego Obszaru Gospodarczego. Jeśli chodzi o transfery danych, można tu wyróżnić następujące kompetencje: a) opiniowanie projektów decyzji o adekwatności; b) opiniowanie projektów decyzji dotyczących standardowych klauzul umownych przygotowanych przez Komisję; c) opiniowanie projektów decyzji dotyczących standardowych klauzul umownych przygotowanych przez krajowe organy ochrony danych; d) kompetencje w zakresie wiążących reguł korporacyjnych (BCR)[34].

Można zauważyć, że działalność Komitetu Art. 93 koncentruje się przede wszystkim na kwestiach dotyczących transferów danych osobowych do państw trzecich, tj. poza Europejski Obszar Gospodarczy bądź do organizacji międzynarodowych.

[33] Wersja skonsolidowana Traktatu o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 326 z 2012 r., s. 47).

[34] W celu uzyskania szerszej informacji o funkcjonowaniu standardowych klauzul umownych i wiążących reguł korporacyjnych, zob. D. Karwala, *Komercyjne transfery danych osobowych do państw trzecich*, Warszawa 2018. Krótkie streszczenie zasad transferów danych osobowych opublikowała też w języku polskim Komisja Europejska: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pl [dostęp: 11.11.2021].

5.1. Kompetencje Komitetu Art. 93 na podstawie RODO

Dla porządku należy odnotować, że w porównaniu do pierwotnego projektu Komisji[35], w ostatecznej wersji RODO katalog kompetencji Komisji do wydawania aktów delegowanych i wykonawczych został znacząco ograniczony. Może to świadczyć o dążeniu Rady UE i Parlamentu Europejskiego do ograniczenia wpływu Komisji na procesy prawodawcze w obszarze ochrony danych osobowych.

Kompetencje Komitetu Art. 93 obejmują proces decyzyjny związany ze stwierdzeniem odpowiedniego stopnia ochrony państwa trzeciego, terytorium lub określonego sektora lub określonych sektorów w tym państwie trzecim lub organizacji międzynarodowej (art. 45 ust. 3 RODO). Obejmują także proces odwrotny, o którym mowa w art. 45 ust. 5 RODO, tj. stwierdzenia, że państwo trzecie – lub terytorium lub jeden lub więcej określonych sektorów w tym państwie trzecim – lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony i związane z tym uchylenie, zmianę lub zawieszenie decyzji o adekwatności, bez mocy wstecznej.

Jeśli chodzi o pozostałe uprawnienia dotyczące transferów danych osobowych, komitet uczestniczy w procedurze: a) przyjmowania standardowych klauzul ochrony danych, zgodnie z art. 46 ust. 2 lit. c RODO; b) zatwierdzania standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję – zgodnie z art. 46 ust. 2 lit. d RODO; c) określania formatu i procedury wymiany informacji między administratorami, podmiotami przetwarzającymi i organami nadzorczymi dotyczących wiążących reguł korporacyjnych – art. 47 ust. 3 RODO.

Jeśli chodzi o inne obszary niż transfery danych osobowych, procedura komitetowa znajduje zastosowanie do: a) standardowych klauzul dla umów pomiędzy administratorem a podmiotem przetwarzającym oraz umów podpowierzenia przetwarzania danych osobowych (art. 28 ust. 7 RODO); b) stwierdzania powszechnego obowiązywania w UE kodeksu postępowania, jego zmiany lub rozszerzenia (art. 40 ust. 9 RODO); c) określania technicznych standardów mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych, a także sposobów upowszechniania i uznawania tych mechanizmów certyfikacji oraz znaków jakości i oznaczeń (art. 43 ust. 9 RODO)[36]; d) określania formuły i procedury wzajemnej pomocy organów nadzorczych oraz zasad wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a EROD, w szczególności standardowego formatu przekazywania informacji drogą elektroniczną (art. 61 ust. 9 RODO); e) określenia zasad wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a EROD, w szczególności standardowego formatu takiej wymiany (art. 67 RODO).

---

[35] Por. Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), Bruksela, dnia 25.01.2012 r., COM(2012) 11 final.

[36] Warto odnotować, że zarówno kodeksy postępowania, jak i certyfikacja oraz znaki jakości i oznaczenia mogą odgrywać rolę także przy przekazywaniu danych osobowych do państw trzecich – zob. art. 46 ust. 2 lit. e oraz art. 46 ust. 2 lit. f RODO.

Należy podkreślić, że wydawanie aktów wykonawczych jest uprawnieniem, a nie obowiązkiem Komisji Europejskiej.

5.2. Kompetencje Komitetu Art. 93 na podstawie rozporządzenia 2018/1725

Odesłania do procedury komitetowej i Komitetu Art. 93, można odnaleźć także w rozporządzeniu regulującym przetwarzanie danych osobowych przez instytucje, organy i jednostki organizacyjne UE. Znajdzie ona zastosowanie w przypadku przyjmowania standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi oraz między podmiotami przetwarzającymi, w przypadku przyjmowania wykazu operacji przetwarzania, jeżeli wymagane są uprzednie konsultacje administratorów dokonujących przetwarzania danych osobowych z EIOD na potrzeby wykonania zadania realizowanego w interesie publicznym oraz w przypadku przyjmowania standardowych klauzul umownych zapewniających stosowne gwarancje dla międzynarodowego przekazywania danych. Jeśli chodzi o uprzednie konsultacje z EIOD, zgodnie z art. 40 ust. 4 rozporządzenia 2018/1725, Komisja może, w drodze aktu wykonawczego, ustanowić wykaz przypadków, w których administratorzy muszą konsultować się z EIOD i uzyskać jego uprzednią zgodę na przetwarzanie danych osobowych do celów wykonania zadania realizowanego przez administratora w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym.

W art. 96 rozporządzenia 2018/1725 wprost się wskazuje, że właściwy dla opiniowania wydawanych zgodnie z nim aktów wykonawczych jest właśnie Komitet Art. 93 RODO[37], do konsultacji z EIOD nie znajdzie jednak zastosowania procedura nadzwyczajna, stąd brak odniesienia do tej procedury w tym przepisie.

5.3. Kompetencje Komitetu Art. 93 na podstawie dyrektywy policyjnej

Jak już wspomniano, procedura komitetowa obejmuje także decyzje o adekwatności uregulowane w dyrektywie policyjnej[38]. Tematyce tej poświęcony jest art. 36 LED. Dyrektywa policyjna stanowi *lex specialis* wobec RODO, ustanawiając przepisy o ochronie 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 tym ochrony

[37] Jak wskazuje się w motywie 84 rozporządzenia 2018/1725, aby zapewnić jednolite warunki wdrażania tego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem 182/2011. W przypadku przyjmowania standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi oraz między podmiotami przetwarzającymi, w przypadku przyjmowania wykazu operacji przetwarzania, jeżeli wymagane są uprzednie konsultacje administratorów dokonujących przetwarzania danych osobowych z EIOD na potrzeby wykonania zadania realizowanego w interesie publicznym oraz w przypadku przyjmowania standardowych klauzul umownych zapewniających stosowne gwarancje dla międzynarodowego przekazywania danych należy stosować procedurę sprawdzającą.

[38] Szerzej o decyzjach o adekwatności wydawanych na podstawie LED – zob. L. Drechsler, *Comparing LED and GDPR Adequacy: One Standard Two Systems*, „Global Privacy Law Review" 2020, nr 1, s. 93–103.

przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Operacje przetwarzania w tych celach będą objęte decyzjami o adekwatności wydanymi w oparciu o LED. Zgodnie z art. 58 ust. 1 LED, Komisję wspomaga komitet ustanowiony na mocy art. 93 RODO[39]. W odniesieniu do zagadnień uregulowanych w dyrektywie, w szczególności stwierdzania, w oparciu o jej postanowienia, odpowiedniego poziomu ochrony danych osobowych, komitet stosuje procedurę sprawdzającą bądź procedurę aktu wykonawczego mającego natychmiastowe zastosowanie – tj. procedury analogiczne do tych przewidzianych w art. 93 RODO. Procedura nadzwyczajna może być zastosowana jedynie w przypadku konieczności uchylenia, zmiany lub zawieszenia decyzji o adekwatności, o czym stanowi art. 36 ust. 5 LED.

6. Relacje z Europejską Radą Ochrony Danych i z Europejskim Inspektorem Ochrony Danych

Warto odnotować, że Komitet Art. 93 jest na bieżąco informowany o pracach toczących się w ramach EROD. Europejska Rada Ochrony Danych ma bowiem prawny obowiązek informowania komitetu o przyjętych przez siebie opiniach, wytycznych oraz zaleceniach – wynika on bezpośrednio z art. 70 ust. 3 RODO. W praktyce jednak dokumenty EROD, czy w przeszłości – Grupy Roboczej Art. 29[40], nigdy nie były przedmiotem dyskusji komitetu jako samodzielny punkt agendy. Przy okazji prac nad decyzjami o adekwatności dyskutowano natomiast odpowiednie opinie EROD, a wcześniej Grupy Roboczej Art. 29.

W przypadku dyskusji dotyczących adekwatności, choć Komisja Europejska nie ma takiego obowiązku, gdyż są one niewiążące[41], zasadniczo podczas prac nad projektami decyzji uwzględnia ona co najmniej w części sugestie zawarte w opiniach EROD. Komitet przed głosowaniem dyskutuje więc projekty decyzji już zmodyfikowane

[39] W motywie 90 LED wymienia się uprawnienia wykonawcze Komisji, przysługujące jej w oparciu o tę dyrektywę: stwierdzanie odpowiedniego stopnia ochrony zapewnianego przez państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizację międzynarodową; określanie formuły i trybu wzajemnej pomocy oraz ustalanie zasad wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a EROD. Jak widać, jest to katalog węższy niż ten wprowadzony w RODO. Zgodnie z motywem 91 LED, należy stosować procedurę sprawdzającą wobec przyjmowania aktów wykonawczych w sprawie stwierdzenia odpowiedniego stopnia ochrony zapewnianego przez państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizację międzynarodową oraz w sprawie formuły i trybu wzajemnej pomocy i ustalania zasad wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a EROD, zważywszy że akty te mają zasięg ogólny. Z kolei motyw 92 LED co do zasady odpowiada, przytoczonemu powyżej, motywowi 169 RODO.

[40] Grupa robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Była ona niezależnym europejskim ciałem doradczym w zakresie ochrony danych i prywatności. Zadania grapy określały art. 30 dyrektywy 95/46/WE oraz art. 15 dyrektywy 2002/58/WE. Z dniem 25 maja 2018 r. grupa została zastąpiona przez Europejską Radę Ochrony Danych.

[41] Szerzej na temat konsultowania EROD i EIOD – zob. L. Tosoni, Komentarz do art. 93…, s. 1283–1284.

na podstawie uwagi EROD oraz oczywiście ze zmianami wprowadzonymi w wyniku dyskusji w komitecie. Nigdy nie zdarzyło się także, aby głosowanie na forum Komitetu Art. 93, jak i jego poprzednika, odbyło się przed wydaniem opinii przez EROD (wcześniej – Grupę Roboczą Art. 29).

Istotnym zagadnieniem w kontekście spotkań Komitetu Art. 93 wydaje się możliwość uczestnictwa w jego posiedzeniach przedstawicieli EROD i EIOD. W mojej ocenie, zgodnie z regulaminem Komitetu Art. 93, zarówno EROD, jak i EIOD, mogą brać w nich udział – pozwalają na to postanowienia Regulaminu Komitetu dotyczące uczestnictwa ekspertów, i taką też rolę w procedurze komitetowej mogą pełnić reprezentanci EROD i EIOD. Zgodnie z art. 7 ust. 3 Regulaminu Komitetu, eksperci mogą być zapraszani przez przewodniczącego, z jego inicjatywy bądź na wniosek członka komitetu[42]. Jako eksperci mogą być zapraszani m.in. przedstawiciele „podmiotów trzecich". Nie powinno budzić wątpliwości, że do tej kategorii można zaliczyć reprezentantów EROD oraz EIOD.

Wydaje się, że szersze zaangażowanie EROD w prace Komitetu Art. 93, byłoby zgodne z wolą co najmniej jednego z unijnych współprawodawców – Parlamentu Europejskiego. W szczególności warto odnotować, że w toku negocjacji RODO, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego proponowała rozbudowanie przepisu dotyczącego zadań EROD[43]. Działanie to należy uznać za chęć przekazania części dotychczasowych uprawnień Komisji do ciała bardziej wyspecjalizowanego w obszarze ochrony danych osobowych[44]. Okoliczność ta wydaje się także wskazywać na istnienie po stronie Parlamentu Europejskiego woli szerszego zaangażowania EROD w proces prawotwórczy na poziomie Unii Europejskiej, w tym w obszarze aktów wykonawczych.

Wreszcie, Komisja Europejska jako jedyna uczestniczy w pracach dotyczących ochrony danych osobowych toczących się zarówno w Komitecie Art. 93, jak i na forum Rady UE (włączając w to odpowiednie grupy robocze) oraz EROD. Jest także obecna podczas obrad mających miejsce w Parlamencie Europejskim, choćby w komisji LIBE. Często więc to ona decyduje, jakie informacje dotyczące dyskusji toczących się równolegle w EROD przekazać Komitetowi Art. 93, a także przedstawia ich podsumowanie, ma więc wpływ na informacje, jakie otrzymują przedstawiciele państw członkowskich uczestniczący w pracach komitetu.

---

[42] Warto odnotować, że członkowie Komitetu mogą zwykłą większością głosów sprzeciwić się ich udziałowi w posiedzeniu. Ponadto, eksperci nie są obecni podczas głosowania komitetu i nie biorą w nim udziału.

[43] Zob. art. 66 – Zadania Europejskiej Rady Ochrony Danych, w rezolucji ustawodawczej Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

[44] Szerzej zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do Art. 93* [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2017, s. 896.

W tym miejscu warto podkreślić, że Komisja jest nie tylko przewodniczącym i sekretariatem komitetu. Jest także stroną dyskusji, ponieważ zależy jej na przekonaniu członków komitetu do pozytywnego zaopiniowania przedłożonego przez nią projektu aktu prawnego, zanim formalnie zostanie on poddany pod głosowanie. Nie jest więc ona w omawianym procesie podmiotem bezstronnym i nie powinna być postrzegana w tej procedurze jako tzw. *honest broker* – neutralny pośrednik. Na jej aktywność mają wpływ, omówione powyżej, czynniki polityczne i ekonomiczne. Wreszcie, czego najlepszym dowodem jest unieważnienie przez TSUE zarówno decyzji Komisji w sprawie „Bezpiecznej Przystani", jak i „Tarczy Prywatności" – nie jest ona w swych działaniach w obszarze ochrony danych osobowych nieomylna.

To Komisja wyznacza państwom członkowskim czas na dokonanie analiz przedkładanych dokumentów, który często jest dość krótki. To ona decyduje także, kiedy konkretny projekt aktu wykonawczego należy uznać za pilny. W przeszłości, np. w przypadku oceny, bardzo różnego od europejskiego, systemu prawa Japonii, czy też analizy „Tarczy Prywatności", która składała się nie z jednego, ale z szeregu różnych oświadczeń i zobowiązań strony amerykańskiej, sprawiało to pewne trudności. Komitet pracuje więc zazwyczaj pod presją ze strony Komisji Europejskiej, mając ograniczony czas na podjęcie decyzji. Dopuszczenie, pod określonymi warunkami, ekspertów dałoby więc przedstawicielom państw członkowskich, w krótkim czasie, dostęp do dodatkowej wiedzy, mogącej pomóc w należytej ocenie projekt aktu wykonawczego. Tym bardziej uzasadnione wydaje się więc stanowisko, że większa partycypacja ekspertów wpłynęłaby pozytywnie na prace komitetu i pozwoliłaby na większy pluralizm obecnych na jego forum poglądów.

Dopuszczenie ekspertów nie może mieć jednak miejsca bezwarunkowo – po pierwsze, eksperci nie powinni w żadnej mierze uczestniczyć w części posiedzeń komitetu, w trakcie której podejmowane są decyzje, ich udział mógłby polegać na przedstawieniu stanowiska i odpowiedzi na ewentualne pytania przedstawicieli państw członkowskich; po drugie – w przypadku zaproszenia ekspertów, informacja o ich udziale w posiedzeniu powinna być podana do publicznej informacji; po trzecie – powinny być to osoby bądź podmioty niezależne, które zgłoszą istniejące konflikty interesów zgodnie z zasadami procedury komitetowej. Tytułem przykładu, ekspertami mogliby być niezależni naukowcy czy też sygnaliści (*whistleblowers*), ale już nie przedstawiciele podmiotów z państw trzecich, które mają bezpośredni interes w wydaniu pozytywnej decyzji o adekwatności. Zgodnie z art. 11 ust. 2 Regulaminu Komitetu, zaproszeni eksperci powinni poinformować przewodniczącego o jakimkolwiek konflikcie interesów odnośnie konkretnego punktu porządku obrad Komitetu. Zgodnie z art. 7 ust. 3 regulaminu, zwykła większość członków komitetu może sprzeciwić się udziałowi eksperta w posiedzeniu.

W szczególności użyteczny byłby bezpośredni udział przedstawicieli EROD (lub w zależności od tematu dyskusji – EIOD) w pracach komitetu. Pozwoliłby on na pełniejszy przepływ informacji czy stanowisk choćby w zakresie opinii dotyczących projektów decyzji o adekwatności, które przyjmuje EROD, a które są następnie przedmiotem dyskusji w ramach procedury komitetowej i rozwianie możliwych wątpliwości przed

głosowaniem przez przedstawicieli państw członkowskich nad projektem decyzji o odpowiednim stopniu ochrony danych osobowych w państwie trzecim. Przedstawiciel EROD lub EIOD, zapraszany w formie eksperta, mógłby odpowiadać na pytania członków komitetu czy bezpośrednio wyjaśniać motywy stojące za poszczególnymi fragmentami wydanych opinii (bądź też – w zależności od przebiegu dyskusji – innych dokumentów wydawanych przez EROD lub EIOD), a także prostować ewentualne nieścisłości, gdyby takie pojawiały się w toku dyskusji. Wiedza ekspercka przedstawicieli EROD lub EIOD mogłaby być wykorzystywana także podczas prac grup roboczych, których możliwość powoływania przewiduje Regulamin Komitetu.

7. Poufność prac Komitetu Art. 93

Zgodnie z art. 13 ust. 2 Regulaminu Komitetu, obrady komitetu mają charakter poufny. Dokumenty przekazywane członkom komitetu, ekspertom i przedstawicielom osób trzecich mają charakter poufny, chyba że udzielono dostępu do tych dokumentów lub Komisja udostępniła je publicznie w innym trybie. Na członkach komitetu, a także ekspertach i przedstawicielach osób trzecich spoczywa obowiązek zachowania poufności. Udzielenie zarówno członkom komitetu, jak i ekspertom informacji o poufności obrad jest obowiązkiem przewodniczącego. Jednocześnie, co istotne z perspektywy ograniczonej transparentności działań komitetu, jeżeli dane państwo poprosi Komisję o upublicznienie swojego stanowiska prezentowanego w toku obrad tego gremium, to Komisja powinna je podać do publicznej wiadomości.

Zgodnie z art. 13 Regulaminu Komitetu, wnioski o dostęp do dokumentów komitetu są rozpatrywane zgodnie z unijnymi przepisami regulującymi dostęp do informacji publicznej. O udostępnieniu informacji decyduje Komisja. Jeśli państwo członkowskie otrzyma żądanie dotyczące dokumentu dotyczącego komitologii, będącego w jego posiadaniu – chyba że wskazano już, czy dokument zostanie ujawniony lub nie – państwo członkowskie ma obowiązek skonsultowania się z Komisją w celu podjęcia decyzji co do jego upublicznienia. Alternatywnie, państwa członkowskie mogą również przekazać odpowiednie żądanie do Komisji Europejskiej.

8. Podsumowanie

Jak wskazano powyżej, Komitet Art. 93 ma za zadanie pełnić funkcję kontrolną wobec działań prawodawczych w obszarze ochrony danych podejmowanych przez Komisję, w tym w zakresie procesu wydawania decyzji o adekwatności. Przez ponad dwadzieścia lat stosowania unijnych przepisów o ochronie danych osobowych, działalność komitetu, pomimo jego realnego wpływu na kształt unijnej ochrony danych osobowych, zawsze pozostawała w cieniu aktywności podejmowanych przez EROD (wcześniej Grupę Roboczą Art. 29) czy rezolucji Parlamentu Europejskiego. W świetle

ograniczonej transparentności prac komitetu i jego, potencjalnie, znaczącego wpływu na europejskie przepisy o ochronie danych osobowych, włączając w to kwestie o znaczeniu kluczowym – takie jak transfery danych osobowych do państw trzecich, uzasadnione jest pytanie o to, jak wyważyć konieczność ochrony istotnych elementów unijnego procesu decyzyjnego z możliwością kontroli społecznej nad tym procesem, oraz jak zapewnić większy pluralizm prezentowanych na forum komitetu poglądów.

Warto przy tym odnotować istotną rolę, jaką w pracach Komitetu Art. 93 pełni Komisja – poprzez przewodniczenie jego pracom, sporządzanie agendy czy sporządzanie sprawozdań ze spotkań komitetu. Z jednej strony – w praktyce Komisja zwołuje posiedzenia komitetu tylko wtedy, gdy jest to konieczne i jest do tego zmuszona wymogami unijnej procedury komitetowej. Z drugiej zaś – liczba spotkań komitetu pokazuje, że nie pełni on roli wyłącznie „maszynki do głosowania" zatwierdzającej projekty decyzji przedkładanych przez Komisję. Na jego forum toczą się dyskusje, które, jak choćby w przypadku „Tarczy Prywatności", wymagały organizacji szeregu spotkań, i których rezultaty są doskonale widoczne na zewnątrz: wydanie przez komitet pozytywnej opinii co do decyzji o adekwatności zawsze wiązało się z koniecznością wprowadzenia zmian do pierwotnych projektów dokumentów. Pomimo zaangażowania komitetu, nie udało się uniknąć niepowodzeń – Trybunał Sprawiedliwości uchylił dotychczas dwie decyzje pozytywnie zaopiniowane przez komitet (jeszcze jako Komitet Art. 31) – obie dotyczące mechanizmów przekazywania danych osobowych do Stanów Zjednoczonych Ameryki.

Z tej perspektywy, a także w szerszym kontekście odpowiedzialności państw członkowskich za efekt końcowy wdrażania prawa UE[45], może dziwić, że komitet, przynajmniej w latach 2013–2019, nigdy nie korzystał w swoich pracach ze wsparcia eksperckiego, polegając na informacjach przedkładanych przez Komisję Europejską. Komisja, która uczestniczy w pracach zarówno komitetu, jak i Rady UE oraz EROD, ma jako jedyna szczegółową wiedzę o działaniach podejmowanych we wszystkich tych gremiach, może też pełnić rolę swoistego pośrednika, przedstawiając w czasie spotkań komitetu informacje m.in. o dyskusjach toczących się w ramach EROD, czy wyjaśniając jego opinie oraz inne publikowane dokumenty. Nie jest ona jednak w omawianym procesie podmiotem całkowicie bezstronnym – zależy jej przecież na przekonaniu członków komitetu do pozytywnego zaopiniowania przedłożonego przez nią projektu aktu prawnego zanim formalnie zostanie on poddany pod głosowanie. W tym kontekście, w szczególności w przypadku dyskusji dotyczących adekwatności państw trzecich, udział przedstawicieli EROD jako ekspertów w spotkaniach komitetu pozwoliłby na bezpośrednią wymianę informacji między EROD a reprezentantami państw członkowskich bez pośrednictwa Komisji. Wiedza ekspercka w obszarze ochrony danych osobowych przedstawicieli EROD (lub – w zależności od tematu dyskusji – także EIOD)

[45] Wydaje się, że poprzez obecność – za pośrednictwem komitetów – przedstawicieli państw członkowskich w systemie stanowienia aktów wykonawczych Unii Europejskiej, odpowiedzialność za efekt końcowy wdrażania przepisów prawa unijnego zostaje, przynajmniej częściowo, rozciągnięta także na rządy państw członkowskich, zob. R. Grzeszczak, *Władza wykonawcza*…, s. 239.

mogłaby być wykorzystywana również podczas prac grup roboczych, których możliwość powoływania ma komitet.

Z kolei szersze informowanie o pracach komitetu stanowiłyby cenną informację nie tylko dla opinii publicznej, a także dla Parlamentu Europejskiego, który chociaż nie jest bezpośrednio zaangażowany w proces wydawania decyzji o adekwatności, to odnosi się do nich w swoich rezolucjach[46]. Powinno ono mieć jednak miejsce w sposób wyważony – wgląd w aktywność komitetu byłby np. cennym źródłem informacji dla państw trzecich starających się o uznanie adekwatności, a także dla lobbystów – i mógłby być tym samym przez nich wykorzystywany do wpływania na prace Komitetu Art. 93.

Literatura

Czerniawski M., *Transfer danych osobowych z terytorium Polski do państwa trzeciego niezapewniającego odpowiedniego poziomu ochrony danych osobowych*, Przegl. Prawn. UW 2009, nr 3–4.

Drechsler L., *Comparing LED and GDPR Adequacy: One Standard Two Systems*, „Global Privacy Law Review" 2020, nr 1.

Grzeszczak R., *Władza wykonawcza w systemie Unii Europejskiej*, Warszawa 2011.

Karwala D., *Komercyjne transfery danych osobowych do państw trzecich*, Warszawa 2018.

RODO. Ogólne rozporządzenie o ochronie danych. *Komentarz*, red. E.Bielak-Jomaa, D. Lubasz, Warszawa 2017.

Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, red. P. Litwiński, Warszawa 2017.

The EU General Data Protection Regulation (GDPR). A Commentary, red. Ch. Kuner, L.A. Bygrave, Ch. Docksey, Oksford 2019.

Tosiek P., *Komitologia: szczególny rodzaj decydowania politycznego w Unii Europejskiej*, Lublin 2007.

Streszczenie

Michał Czerniawski

Rola Komitetu Art. 93 RODO w procedurze oceny adekwatności państw trzecich

W artykule poruszono tematykę procedury komitetowej (komitologii) w unijnym prawie ochrony danych osobowych. Tak zwany Komitet Art. 93 ma za zadanie pełnić funkcję kontrolną wobec działań prawodawczych w tym obszarze podejmowanych przez Komisję Europejską, włączając w to projekty decyzji wykonawczych stwierdzających odpowiedni stopień ochrony danych osobowych przez państwo trzecie. Przez ponad dwadzieścia lat stosowania unijnych przepisów o ochronie danych osobowych, działalność tego komitetu, oraz jego poprzednika – Komitetu Art. 31, pomimo ich realnego wpływu na kształt ochrony danych osobowych w Unii Europejskiej, pozostawała w cieniu i wciąż cechuje ją brak transparentności. Dyskusje dotyczące praw

[46] Zob. choćby rezolucja Parlamentu Europejskiego z dnia 21 maja 2021 r. w sprawie odpowiedniej ochrony danych osobowych przez Zjednoczone Królestwo (2021/2594(RSP)).

podstawowych, których konkluzje mają bezpośrednie przełożenie na kształt unijnego systemu ochrony danych powinny odbywać się w sposób możliwie przejrzysty, przy szerszym udziale ekspertów w obszarze ochrony danych osobowych.

Słowa kluczowe: transfer danych osobowych do państw trzecich; adekwatność ochrony; komitologia; RODO; EROD.

Summary

Michał Czerniawski

Role of the Article 93 GDPR Committee in the Adequacy Findings

The paper discusses the committee procedure (comitology) in the EU personal data protection law. The so-called Article 93 Committee has the task of controlling European Commission's legislative activities in this area, including draft implementing decisions on an adequate protection of personal data by a third country. For over twenty years of application of the EU data protection laws, the actions of the Committee and its predecessor – Article 31 Committee, despite their significance for personal data protection in the EU, did not draw much attention and still lack transparency. Discussions regarding fundamental rights, the conclusions of which directly affect the EU data protection framework, should be carried out as transparently as possible, with wider participation of experts in the field of personal data protection.

Keywords: transfer of personal data to third countries; adequacy of the protection; comitology; GDPR; EDPB.

Glosy

Wykorzystanie danych biometrycznych w szkole

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie
z dnia 7 sierpnia 2020 r., II SA/Wa 809/20

1. **Wystarczy, aby możliwa była choćby pośrednia identyfikacja osoby, by dane jej dotyczące stanowiły jej dane osobowe, co jednoznacznie wynika z definicji zawartej w art. 4 pkt 1 RODO. Ponadto, z uwagi na charakter przetwarzania (specjalne przetwarzanie techniczne), a także charakter samych danych, które dotyczą cech fizjologicznych i fizycznych, stwierdzić należy, że przetwarzane do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców dzieci stanowią dane biometryczne, służą bowiem do zautomatyzowanej weryfikacji uprawnienia konkretnej osoby fizycznej.**
2. **Starając się literalnie odczytać wymogi adekwatności i minimalizacji, można dojść do wniosku, że w praktyce nie jest łatwo ich ze sobą pogodzić, albowiem adekwatność zakłada dokonanie oceny przydatności określonego rodzaju danych do realizacji celu, natomiast minimalizacja prowadzi do uznania, że jeśli cel można osiągnąć bez przetwarzania określonego rodzaju danych, to nie należy takich danych przetwarzać. (…) Można pogodzić ze sobą te dwa nie do końca spójne wymogi, uznając, że ich spełnienie należy oceniać łącznie, co w konsekwencji oznacza, że nie powinno się przyznawać prymatu minimalizacji kosztem adekwatności. W tej sytuacji, (…) za dopuszczalne uznać należy przetwarzanie danych w nieco szerszym zakresie niż tylko (…) konieczne minimum, pod warunkiem że przetwarzane dane mają ścisły związek z realizacją celu (np. ułatwiają jego osiągnięcie).**

Arwid Mednis
Uniwersytet Warszawski
arwid.mednis@uw.edu.pl
ORCID: 0000-0001-8130-7108

https://doi.org/10.26881/gsp.2021.4.08

Glosowany wyrok zasługuje na uwagę z kilku powodów. Po pierwsze, jest to jedno z nielicznych orzeczeń wydanych dotychczas pod rządami rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie

o ochronie danych)[1], w których Wojewódzki Sąd Administracyjny w Warszawie nie podzielił stanowiska organu ochrony danych[2]. Po drugie, wyrokowi nie można odmówić wyjątkowej wnikliwości uzasadnienia. Po trzecie wreszcie, komentowany wyrok jest pierwszym orzeczeniem sądowym w Polsce zapadłym pod rządami RODO, które dotyczyło wykorzystania danych biometrycznych[3].

Jednak głównym powodem, dla którego warto bliżej omówić ów wyrok, jest kwestia rozumienia jednej z kluczowych zasad RODO, jaką jest zasada minimalizacji, przede wszystkim w kontekście wykorzystywania danych szczególnej kategorii za zgodą osób, których dane te dotyczą.

Należałoby zatem przypomnieć krótko stan faktyczny sprawy. Szkoła podstawowa w Gdańsku od września 2015 r. wykorzystywała czytnik biometryczny w celu weryfikacji uiszczenia opłaty za posiłki uczniów. Czytnik umieszczono przy wejściu do stołówki szkolnej, tak aby na bieżąco identyfikować dzieci pobierające posiłki w stołówce oraz weryfikować uiszczenie opłaty za posiłek w danym dniu. Identyfikacja i weryfikacja odbywały się na podstawie odcisku palca ucznia. Szkoła nie posiadała żadnego zbioru, który zawierałby obrazy linii papilarnych dzieci. Dane były gromadzone tylko w czytniku w postaci zapisu ciągu bajtów. W trakcie odczytu czytnik porównywał, czy istnieje odpowiedni zapis cyfrowy, a w przypadku, gdy porównanie wypadło pomyślnie, wysyłał do programu tylko numer pozycji przypisany do konkretnego dziecka, kończąc w ten sposób weryfikację dokonanej uprzednio płatności.

Szkoła pozyskiwała dane uczniów na podstawie pisemnej zgody rodzica (opiekuna prawnego). Rodzic w umowie o korzystanie z posiłków w stołówce szkolnej miał możliwość wyboru: wyrażenia lub niewyrażenia zgody na korzystanie z czytnika na odcisk palca. Rodzice byli informowani o takiej możliwości na stronie internetowej stołówki szkolnej. Na stronie umieszczono również zasady wydawania obiadów, zgodnie z którymi uczniowie, którzy nie posiadają identyfikacji biometrycznej, przepuszczają wszystkich i oczekują na końcu kolejki, aż wszyscy uczniowie z identyfikacją biometryczną wejdą do stołówki. Po ich wejściu rozpoczyna się wpuszczanie pojedynczo uczniów bez identyfikacji biometrycznej.

Po podpisaniu umowy i wyrażeniu zgody przez rodzica na korzystanie z czytnika biometrycznego uczeń był rejestrowany w systemie ewidencji wpłat i posiłków (SEWiP) poprzez wprowadzenie jego imienia, nazwiska, klasy oraz imienia, nazwiska, adresu e-mail, numeru telefonu kontaktowego rodzica. Następnie (jeśli rodzic wyraził zgodę) dochodziło do rejestracji wzorca odcisku palca dziecka w czytniku.

Po rozwiązaniu umowy o korzystanie z obiadów w stołówce szkolnej, dane potrzebne do identyfikacji (tj. ciąg bajtów zapisany w czytniku) były usuwane, z zastrzeżeniem

---

[1] Dz. Urz. UE L 119, s. 1 ze zm.; dalej: RODO.

[2] Należy podkreślić, że glosowany wyrok jest przedmiotem skargi kasacyjnej Prezesa Urzędu Ochrony Danych Osobowych. Jednak do chwili złożenia niniejszej glosy do publikacji, rozstrzygnięcie Naczelnego Sądu Administracyjnego nie było znane.

[3] Nie jest to jednak pierwszy w Polsce wyrok dotyczący przetwarzania danych biometrycznych. Warto wspomnieć choćby wyrok Naczelnego Sądu Administracyjnego z dnia 1 grudnia 2009 r., I OSK 249/09, wydany pod rządami ustawy o ochronie danych osobowych z 1997 r.

że pozostawiano kopię archiwizacyjną na karcie micro SD, która przechowywana była w zabezpieczonym pomieszczeniu. W sytuacji gdy uczeń przestawał korzystać ze stołówki, a umowa nie została rozwiązana i rodzic nie wycofał zgody, wzorzec biometryczny zapisany w czytniku przechowywany był do czasu rozwiązania umowy lub do zakończenia roku szkolnego. Na czas wakacji wzorzec biometryczny pozostawał zapisany w czytniku i na karcie SD. W przypadku nieprzedłużenia umowy o korzystanie z obiadów w stołówce szkolnej na nowy rok szkolny dane były usuwane najpóźniej do września każdego roku.

Istotnym elementem stanu faktycznego była liczba uczniów. W roku szkolnym 2018/2019 do Szkoły uczęszczało 1247 uczniów, z czego 603 korzystało z czytnika biometrycznego, a 2 uczniów z alternatywnego systemu identyfikacji. W roku szkolnym 2019/2020 do szkoły uczęszczało 1121 uczniów, z czego 680 uczniów korzystało z czytnika biometrycznego, a 4 uczniów z alternatywnego systemu identyfikacji.

Warto odnotować, że władze szkoły stały na stanowisku, że dane przetwarzane w systemie nie są danymi biometrycznymi.

Decyzją z dnia 18 lutego 2020 r. Prezes Urzędu Ochrony Danych Osobowych (PUODO) stwierdził naruszenie przez szkołę art. 5 ust. 1 lit. c RODO (zasada minimalizacji danych) oraz art. 9 ust. 1 RODO (zakaz przetwarzania szczególnych kategorii danych). Jednocześnie PUODO nakazał szkole usunięcie danych osobowych w zakresie przetworzonych do postaci cyfrowej informacji o charakterystycznych punktach linii papilarnych palców dzieci korzystających z usług stołówki szkolnej, zaprzestanie zbierania powyższych danych osobowych oraz nałożył na szkołę karę pieniężną w wysokości 20.000 zł. Szkoła wniosła skargę na powyższą decyzję organu. Omawianym w niniejszej glosie wyrokiem z dnia 7 sierpnia 2020 r. Wojewódzki Sąd Administracyjny w Warszawie uchylił decyzję PUODO.

W dalszej części tekstu skupię się tylko na najważniejszych, moim zdaniem, elementach sprawy. Po pierwsze – na kwestii przesłanek legalności przetwarzania danych biometrycznych, a po drugie – na zasadzie minimalizacji danych i jej relacji do przesłanki zgody. Pominę natomiast inne kwestie, m.in. te związane z wysokością kary pieniężnej i przesłankami jej szacowania.

W pierwszej kolejności należy stwierdzić, że wbrew twierdzeniom szkoły, dane służące do identyfikacji i weryfikacji uprawnień do posiłków przetwarzane w czytniku i na innych nośnikach archiwizacyjnych to bez wątpienia dane biometryczne. Artykuł 4 pkt 14 RODO określa dane biometryczne jako dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Istotą definicji są zatem trzy następujące elementy:

- specjalne przetwarzanie techniczne;
- odniesienie do cech fizycznych, fizjologicznych lub behawioralnych, które są w zasadzie niezmienne i niepowtarzalne oraz
- możliwość jednoznacznej identyfikacji osoby.

Pomimo tego, że szkoła nie przechowywała obrazów odcisków palców, to jednak przedstawienie ich w czytniku w formie zapisu cyfrowego, który pozwalał na jednoznaczną identyfikację, oznacza, że były one danymi biometrycznymi. Słusznie zatem zarówno organ, jak i sąd w tym zakresie odmówiły uznania argumentacji skarżącej szkoły.

W art. 9 ust. 1 RODO zabrania się przetwarzania określonych (szczególnych) kategorii danych osobowych, wśród których są m.in. dane biometryczne, przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej. Prezes Urzędu Ochrony Danych Osobowych, powołując się na motyw 38 RODO, podkreśla w decyzji, że niezależnie od tego, czy mamy do czynienia z danymi zwykłymi czy szczególnymi, dane osobowe dzieci wymagają specjalnej ochrony, ponieważ dzieci mogą być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych. Wydaje się jednak, że uwaga ta jest nietrafna w kontekście omawianej sprawy, ponieważ motyw 38, w mojej ocenie, dotyczy przede wszystkim sytuacji, gdy dzieci, korzystając z usług w internecie, udostępniają swoje dane w rozmaitych serwisach.

Wyjątki od zakazu przetwarzania szczególnych kategorii danych zostały określone w art. 9 ust. 2 RODO. Jak słusznie wskazuje organ, katalog wymieniony w tym przepisie jest zamknięty. „Każda z przesłanek legalizujących proces przetwarzania danych osobowych ma charakter autonomiczny i niezależny. Oznacza to, że przesłanki te co do zasady są równoprawne, a wobec tego spełnienie co najmniej jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych" – podkreśla PUODO w dalszej części uzasadnienia. Jednym z wyjątków jest wyraźna zgoda podmiotu danych. W omawianej sprawie szkoła powoływała się na zgody wyrażone przez rodziców (opiekunów prawnych) uczniów. Organ zwraca jednak uwagę, że zgoda powinna być m.in. dobrowolna, a o dobrowolności zgody nie można mówić w przypadku wyraźnego braku równowagi w relacji pomiędzy administratorem a podmiotem danych. Jednakże dalsza część uzasadnienia decyzji odnosząca się do zgody i innych przesłanek jest co najmniej niespójna. Wbrew wcześniejszemu stwierdzeniu o równoważnym charakterze wszystkich przesłanek z art. 9 ust. 2 RODO, organ stwierdza dalej, że „zgoda stanowi podstawę legalizującą przetwarzanie danych osobowych jedynie wtedy, gdy nie istnieją inne przesłanki na to przetwarzanie". Jednocześnie PUODO przeprowadza analizę przepisów ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2019 r., poz. 1148; dalej: u.p.o.).

Organ zauważa, że zgodnie z art. 106 tej ustawy w celu zapewnienia prawidłowej realizacji zadań opiekuńczych, w szczególności wspierania prawidłowego rozwoju uczniów, szkoła może zorganizować stołówkę. W związku z tym stwierdza, że „podstawą przetwarzania jakichkolwiek danych osobowych dzieci w związku z realizacją tego zadania szkoły nie mogła być zgoda, ponieważ podstawą do przetwarzania danych osobowych dzieci w tym celu przez Szkołę jest art. 6 ust. 1 lit. e RODO, zgodnie z którym przetwarzanie jest zgodne z prawem między innymi gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi". Prezes Urzędu

Ochrony Danych Osobowych wywodzi z tego, że szkoła przetwarza dane osobowe ucznia na podstawie przepisów prawa, wykonując swoje ustawowe zadania. Nie potrzebuje zatem odrębnej zgody rodziców bądź pełnoletniego ucznia na przetwarzanie danych osobowych w związku z realizacją tych zadań, tj. świadczeniem usług przez stołówkę szkolną. Jednocześnie organ stwierdza, że przepisy prawa określające, jakie dane o uczniach może gromadzić szkoła, nie przewidują możliwości zbierania danych biometrycznych.

W mojej ocenie, pogląd, że zgoda jest przesłanką legalizującą przetwarzanie danych osobowych tylko wtedy, gdy nie można zastosować innych przesłanek, jest niczym nieuzasadniony. Ponadto, jest sprzeczny z wyrażonym przez organ w innym miejscu uzasadnienia poglądem, zgodnie z którym wszystkie przesłanki są równoważne i autonomiczne. Dotyczy to również przesłanek zawartych w art. 9 ust. 2 RODO[4]. Nie jest również zrozumiałe, dlaczego organ, stwierdziwszy że ma do czynienia z danymi szczególnej kategorii, analizuje podstawy opisane w art. 6 ust. 1 RODO zamiast tych zawartych w art. 9 ust. 2 RODO. Ponadto, jeśli organ uznał, że nie można zastosować przesłanki, o której mowa w art. 6 ust. 1 lit. e RODO i nie widzi innych podstaw prawnych przetwarzania, powinien był, zgodnie z powyższym poglądem, rozważyć przesłankę zgody. Niezależnie od powyższego, dokonana przez organ wykładnia ustawowych uprawnień szkoły budzi co najmniej poważne wątpliwości. Przepisy prawa oświatowego nie zawierają listy danych osobowych uczniów, które mogą być przetwarzane przez szkołę; jedynie art. 30a u.p.o. zobowiązuje jednostki oświatowe, w tym szkoły, do przetwarzania danych w zakresie niezbędnym do realizacji zadań ustawowych. W mojej ocenie, nie można na tej podstawie wykluczyć zastosowania przez szkołę przesłanki zgody. Restrykcyjne podejście eliminujące taką możliwość, wyłączyłoby bowiem całą sferę działań organizatorskich jednostek oświatowych, a więc sferę, która jest związana z zadaniami oświatowymi, ale nie jest szczegółowo uregulowana przepisami prawa.

Wojewódzki Sąd Administracyjny (WSA) w Warszawie zasadnie zatem pominął powyższy wywód PUODO i dopuścił zgodę jako podstawę przetwarzania danych uczniów korzystających ze stołówki. Uznał, że pisemne oświadczenia rodziców, w których wyraźnie wskazano cel przetwarzania danych biometrycznych, stanowią jednoznaczną i niebudzącą wątpliwości zgodę na ich przetwarzanie w określonym celu, i tym samym świadczą o spełnieniu przesłanki, o której mowa w art. 9 ust. 2 lit. a RODO. W tym miejscu pozostaje jedynie wyrazić wątpliwość co do dobrowolności zgody wyrażanej przez rodziców. Cecha ta wyraża się bowiem m.in. w braku negatywnych konsekwencji odmowy udzielenia zgody[5]. Skutkiem odmowy udzielenia zgody w omawianym przypadku jest, na co zwrócił uwagę organ, dłuższe oczekiwanie na posiłek przez uczniów, których rodzice nie wyrazili zgody na biometryczną weryfikację faktu opłacenia posiłku. Kwestia ta wymaga jednak szerszej analizy, która wykracza poza ramy niniejszej

[4] Tak m.in. P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. *idem*, Warszawa 2021, s. 205.

[5] Wytyczne 5/2020 dotyczące zgody na mocy rozporządzenia 2016/679, wersja 1.1 przyjęta dnia 4 maja 2020 r., s. 7, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pl.pdf [dostęp: 25.11.2021].

glosy. Warto jedynie wskazać, że odmowa udzielenia zgody praktycznie zawsze wiąże się z jakimś negatywnym skutkiem, pozostaje jedynie pytanie o to, czy skutek w postaci opóźnienia w świadczeniu usługi pozwalałby na zakwestionowanie dobrowolności zgody rodziców.

Szerzej natomiast chciałbym skupić się na zasadzie minimalizacji danych. Zarówno organ, jak i sąd słusznie wskazują, że obowiązek przestrzegania tej zasady jest niezależny od legitymowania się przesłanką legalności przetwarzania danych. Dotyczy to również przetwarzania danych osobowych na podstawie zgody. Innymi słowy, administrator przetwarzający dane na podstawie pozyskanej zgody jest nadal zobowiązany do przestrzegania zasady minimalizacji danych. Nie ulega również wątpliwości, że zasada ta, podobnie jak pozostałe wymienione w art. 5 RODO, ma charakter normatywny i jest samoistnym obowiązkiem nałożonym na administratora.

Zasada minimalizacji wyrażona w art. 5 ust. 1 lit. c RODO stanowi, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Z językowego punktu widzenia istnieją na tym tle różne możliwości interpretacyjne. Wydaje się bowiem, że „minimalizacja" i „niezbędność" danych nie mają tego samego znaczenia co „adekwatność" i „stosowność". Dane adekwatne do celu to dane „odpowiednie", a nie tylko „niezbędne". W praktyce ma to ogromne znaczenie, ponieważ zakres danych odpowiednich do danego celu może być znacznie szerszy od danych minimalnych, niezbędnych do realizacji tego celu.

W obowiązującym przed datą zastosowania RODO (tj. 25 maja 2018 r.) stanie prawnym, przepisy stawiały wymóg, aby dane były „prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone" (art. 6 ust. 1 lit. c dyrektywy 95/46[6]). W wersji angielskiej tej dyrektywy użyto sformułowania o identycznym znaczeniu (*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*).

Zgodnie z motywem 28 powyższej dyrektywy, „dane muszą być adekwatne, właściwe i nie wykraczać poza cele, dla których są przetwarzane" (*the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed*). W polskiej ustawie implementującej dyrektywę 95/46[7] w art. 26 ust. 1 pkt 3 znalazł się wymóg, aby dane były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Tak więc w poprzednim stanie prawnym w przepisach nie wymagano, aby przetwarzanie było ograniczone do danych niezbędnych. Wspomniany przepis RODO definiujący zasadę minimalizacji jest natomiast niejednoznaczny. Warto zatem przeanalizować stanowiska PUODO i WSA w omawianej sprawie.

Organ stwierdził, że przetwarzanie danych biometrycznych nie jest niezbędne do osiągnięcia celu, jakim jest identyfikacja uprawnienia dziecka do odebrania obiadu. Identyfikację można przeprowadzić za pomocą innych środków, mniej ingerujących

[6] Dyrektywa 95/46 Parlamentu Europejskiego i Rady z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. WE L 281, s. 31; dalej: dyrektywa 95/46).

[7] Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jedn.: Dz. U. z 2016 r., poz. 922).

w prywatność dziecka korzystającego z usług stołówki szkolnej. W szkole istniały alternatywne metody, takie jak karty elektroniczne lub podanie nazwiska i numeru umowy.

Wojewódzki Sąd Administracyjny w Warszawie podszedł do tej kwestii inaczej, przede wszystkim analizując bardzo szczegółowo stan faktyczny oraz cel przetwarzania danych.

Sąd zwraca w pierwszej kolejności uwagę na treść motywu 39 preambuły RODO, który stanowi m.in., że „(…) dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami (…)". Sąd w swoim wywodzie na tle zasady minimalizacji i powyższego motywu, kładzie nacisk na odpowiednie zdefiniowanie celu przetwarzania i stwierdza, że dane „muszą być odpowiednie i stosowne do osiągnięcia celu ich zebrania, lecz zarazem nie mogą być nadmierne". To prawidłowo określony cel determinuje zakres niezbędnych danych[8]. Tym samym – wskazuje WSA – przetwarzanie danych w zakresie zbędnym dla osiągnięcia tego celu będzie oznaczało naruszenie przepisów RODO.

Sąd przyznaje w uzasadnieniu, że wymogi minimalizacji i adekwatności nie są ze sobą spójne, a ich spełnienie należy oceniać łącznie, co w konsekwencji oznacza, że „nie powinno się przyznawać prymatu minimalizacji kosztem adekwatności"[9]. Jednocześnie podkreśla, jak ważne są okoliczności konkretnej sprawy, a więc w tym przypadku fakt, że biometria nie była jedyną metodą weryfikacji płatności oraz to, że szkoła wprowadzała wcześniej inne sposoby weryfikacji odpłatności za posiłek (np. karta obiadowa) i dopiero stwierdzając, że nie przynosi to efektów, na wniosek rady rodziców i za pisemną zgodą rodziców, zdecydowała się na wprowadzenie czytnika biometrycznego. Słusznie sąd odrzuca sugestię PUODO, że dane biometryczne mogą być wykorzystywane tylko wyjątkowo, i to w takich celach, jak np. bezpieczeństwo osobowe, przemysłowe czy ochrona informacji itp. Takie ograniczenie znikąd bowiem nie wynika. Oczywiste jest, że sięganie po dane biometryczne jest daleko idącą ingerencją w sferę prywatności, niemniej nie oznacza to, że w przypadkach takich jak w gdańskiej szkole ich użycie będzie niedopuszczalne niezależnie od okoliczności. Słusznie zatem sąd, biorąc pod uwagę okoliczności sprawy, dopuścił możliwość weryfikacji biometrycznej uczniów.

Użyte w przepisie art. 5 ust. 1 lit. c RODO określenie „adekwatne" oznacza „odpowiednie, zgodne, proporcjonalne, nienadmierne" i może być traktowane jako synonim słowa „stosowne". Pojęcia adekwatności i stosowności rozumieć można jako konieczność zachowania – jak stwierdza WSA – „odpowiednich proporcji zakresu danych do celów przetwarzania i przetwarzanie tylko takich danych, które są potrzebne dla

[8] Tak: D. Lubasz [w:] *Ochrona danych osobowych*. *Meritum*, red. *idem*, Warszawa 2020, s. 114.

[9] W literaturze zwraca się uwagę na problem interpretacji zasady minimalizmu; m.in. P. Fajgielski twierdzi, że ograniczanie danych do niezbędnego minimum byłoby interpretacją zbyt daleko idącą (*idem*, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 149).

realizacji określonych celów". Sąd wprost przyznaje, że ograniczenie danych do niezbędnego minimum – tak jak chce tego organ – byłoby interpretacją zbyt daleko idącą.

Najważniejszym elementem konkluzji sądu jest stwierdzenie, że wymóg niezbędności należy odczytywać łącznie z wymogiem adekwatności i stosowności, co powinno pozwolić na uwzględnienie okoliczności i dopuszczenie przetwarzania danych, które w istotny sposób mogą pomóc osiągnąć cele przetwarzania.

Co do zasady podzielam wyrażony przez WSA w glosowanym wyroku pogląd na temat rozumienia zasady minimalizacji, jednakże z pewnymi zastrzeżeniami. Przede wszystkim, przeformułowałbym nieco to rozumienie w następującym kierunku: w zasadzie minimalizacji nie powinno dostrzegać się konfliktu pomiędzy tym, co z jednej strony – „odpowiednie" i „stosowne", a z drugiej – „niezbędne". Wydaje się, że w pierwszej kolejności należy brać pod uwagę adekwatność (odpowiedniość) danych do określonego celu, z zastrzeżeniem że cel powinien być prawidłowo sformułowany. Zauważyć należy bowiem, że w omawianej sprawie nie wyartykułowano wyraźnie, iż chodzi nie tylko o samą weryfikację płatności, ale również o sprawność tego procesu, biorąc pod uwagę takie okoliczności jak liczbę uczniów korzystających z obiadów, czas w jakim są wydawane obiady, nieskuteczność dotychczasowych metod itp. Tak określony cel pozwala dopiero na określenie danych niezbędnych do jego realizacji. Innymi słowy, po określeniu danych osobowych odpowiednich (adekwatnych i stosownych w rozumieniu art. 5 ust. 1 lit. c RODO) do celu, administrator powinien potraktować ten zakres jako niezbędny do jego realizacji. Taka interpretacja pozwoliłaby na uniknięcie traktowania sformułowań użytych w ww. przepisie jako przeciwstawnych.

Literatura

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Ochrona danych osobowych. Meritum, red. D. Lubasz, Warszawa 2020.

Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, red. P. Litwiński, Warszawa 2021.

Streszczenie

Arwid Mednis

Wykorzystanie danych biometrycznych w szkole

Wojewódzki Sąd Administracyjny uchylił decyzję organu ochrony danych nakazującą szkole usunięcie biometrycznych danych osobowych w postaci linii papilarnych palców dzieci korzystających z usług stołówki szkolnej, zaprzestanie zbierania powyższych danych osobowych oraz nakładającą na szkołę karę pieniężną w wysokości 20 tys. zł. Kluczowa w sprawie okazała się kwestia zastosowania zasady minimalizacji (art. 5 ust. 1 lit. c RODO). Sąd stwierdził, że wymogi minimalizacji i adekwatności, o których mowa w tym przepisie nie są ze sobą spójne, a ich speł-

nienie należy oceniać łącznie, co w konsekwencji oznacza, że nie powinno się przyznawać prymatu minimalizacji kosztem adekwatności. Sąd przyznał, że użycie przez szkołę danych biometrycznych nie było jedynym dostępnym sposobem weryfikacji, czy uczeń ma opłacone obiady, niemniej zwrócił uwagę, że okoliczności sprawy wskazywały na to, że użycie innych sposobów okazało się nieskuteczne. Co do zasady należy zgodzić się ze stanowiskiem sądu z zastrzeżeniem, że w sprawie nie chodziło jedynie o skuteczną weryfikację dokonanych płatności, ale również o sprawność procesu weryfikacji (duża liczba uczniów, krótki czas na sprawdzenie). Dopiero tak rozumiany cel pomógłby określić jakie dane osobowe są odpowiednie do jego realizacji.

Słowa kluczowe: zgoda; biometria; przesłanki legalizacyjne; dobrowolność; wycofanie zgody; zgoda dziecka; forma zgody; RODO.

Summary

Arwid Mednis

Use of Biometric Data at School

The Voivodship Administrative Court revoked the decision of the data protection authority ordering the school to remove biometric personal data in the form of fingerprints of the fingers of children using the school canteen services and to stop collecting the above personal data, as well as imposing on the school an administrative fine of PLN 20,000. The key issue in the case was the application of the minimization principle (Article 5 (1) (c) of the GDPR). The court stated that the requirements of minimization and adequacy referred to in this provision are not consistent with each other and their fulfillment should be assessed jointly, which consequently means that the primacy of minimization should not be given at the expense of adequacy. The court acknowledged that the school's use of biometric data was not the only available means of verifying that the student had paid for lunches, but noted that the circumstances of the case indicated that the use of other methods had proved ineffective. As a rule, one should agree with the court's position, however with the reservation that the case was not only about effective verification of payments made, but also about the efficiency of the verification process (large number of students, short time to check). Only the purpose understood in this way would help to determine what personal data are appropriate.

Keywords: consent; biometrics; lawfulness of processing; voluntariness; withdrawal of consent; consent of the child; form of consent; GDPR.

Warunki wyrażenia zgody na użycie plików typu cookies

Wyrok Trybunału Sprawiedliwości Unii Europejskiej
z dnia 1 października 2019 r. w sprawie C-673/17
Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV przeciwko Planet49 GmbH

1. **Artykuł 2 lit. f i art. 5 ust. 3 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r., dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywy o prywatności i łączności elektronicznej), zmienionej dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r., w związku z art. 2 lit. h dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, a także z art. 4 pkt 11 i art. 6 ust. 1 lit. a rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych), należy interpretować w ten sposób, że zgoda, o której mowa w tych przepisach, nie jest ważna, jeżeli przechowywanie informacji lub dostęp do informacji już przechowywanych w urządzeniu końcowym użytkownika strony internetowej, za pośrednictwem plików cookies, zostały zaakceptowane za pomocą domyślnie zaznaczonego okienka (pola) wyboru, którego zaznaczenie użytkownik ten musi usunąć, aby odmówić udzielenia zgody.**
2. **Sposób interpretowania art. 2 lit. f i art. 5 ust. 3 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, w związku z art. 2 lit. h dyrektywy 95/46, a także z art. 4 pkt 11 i art. 6 ust. 1 lit. a rozporządzenia 2016/679, nie powinien być różny w zależności od tego, czy informacje przechowywane lub udostępniane w urządzeniu końcowym użytkownika strony internetowej stanowią dane osobowe w rozumieniu dyrektywy 95/46 i rozporządzenia 2016/679.**
3. **Artykuł 5 ust. 3 dyrektywy 2002/58, zmienionej dyrektywą 2009/136 należy interpretować w ten sposób, że informacje, jakich usługodawca powinien udzielić użytkownikowi strony internetowej, obejmują również wskazanie okresu funkcjonowania plików cookies oraz określenie, czy osoby trzecie mogą uzyskać dostęp do takich plików.**

Michał Miłosz
Uniwersytet Gdański
michal.milosz@ug.edu.pl
ORCID: 0000-0001-5633-9941

https://doi.org/10.26881/gsp.2021.4.09

Komentowane orzeczenie stanowi pierwszą wypowiedź Trybunału Sprawiedliwości UE (TSUE) w kwestii warunków wyrażenia zgody na użycie plików typu „cookies" w urządzeniach końcowych użytkowników, której wymóg uzyskania wynika w prawie unijnym z art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej[1], uwzględniające przepisy ogólnego rozporządzenia o ochronie danych[2].

Tezy wyrażone w glosowanym wyroku TSUE wyznaczają kierunek wykładni przepisów znajdujących zastosowanie przy instalowaniu plików cookies, i tym samym powinny oddziaływać na praktykę pozyskiwania zgód użytkowników na wykorzystywanie tego typu technologii. W przyszłości na tę praktykę istotny wpływ będzie miało również uchwalenie, a następnie wejście w życie procedowanego obecnie projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego i ochrony danych osobowych w łączności elektronicznej oraz uchylającego dyrektywę 2002/58/WE (rozporządzenie o prywatności i łączności elektronicznej)[3], które zawierać będzie rozbudowaną regulację dotyczącą korzystania z możliwości urządzeń końcowych użytkowników do przetwarzania i przechowywania oraz gromadzenie informacji z tych urządzeń obejmującą również stosowanie plików cookies.

Komentowany wyrok TSUE został wydany w następującym stanie faktycznym. Niemiecka spółka Planet49 zorganizowała w 2013 r. loterię promocyjną. Na stronie internetowej, poprzez którą organizowana była loteria, osoby w niej uczestniczące podawały informacje osobowe, takie jak kod pocztowy oraz imię i adres. Na stronie loterii zamieszczone były teksty dwóch oświadczeń dotyczących wyrażenia określonych zgód przez użytkowników loterii. Obok oświadczeń umieszczone były pola wyboru (tzw. „okienka"). Udział w loterii był możliwy jedynie w razie zaznaczenia przynajmniej pierwszego z tych pól. Drugie pole wyboru było domyślnie zaznaczone, zatem

[1] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. UE L 201 z 2002 r., s. 37 ze zm.; dalej: dyrektywa 2002/58; dyrektywa o e-prywatności).

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1; dalej: rozporządzenie 2016/679; ogólne rozporządzenie o ochronie danych).

[3] Zob. projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej) w wersji przyjętej przez Komitet Stałych Przedstawicieli w dniu 10 lutego 2021 r.; dalej: projekt rozporządzenia o e-prywatności, https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf [dostęp: 10.11.2021].

użytkownik musiał usunąć to zaznaczenie w celu niewyrażenia zgody, która w przeciwnym razie zostałaby automatycznie odnotowana.

Pierwsze pole wyboru służyło do wyrażenia zgody na kontakt marketingowy z uczestnikiem loterii ze strony partnerów reklamowych jej organizatora. Zgoda ta nie dotyczyła wykorzystywania plików cookies, lecz była zgodą na realizację celów marketingowych. Kwestia skuteczności udzielenia tej zgody marketingowej nie była przedmiotem rozważań TSUE, stąd też nie będzie analizowana – jako wykraczająca poza zakres zagadnień, których dotyczy niniejsza glosa.

Drugie oświadczenie zawarte na stronie loterii odnosiło się do monitorowania zachowania uczestników na witrynach internetowych partnerów reklamowych Planet49, co wiązało się z instalowaniem plików cookies. Oświadczenie przy drugim polu wyboru brzmiało: „Wyrażam zgodę na stosowanie wobec mnie usługi analizy internetowej Remintrex. Skutkuje to tym, że organizator loterii promocyjnej [Planet49] po zarejestrowaniu uczestnika w loterii instaluje pliki cookies. Umożliwi to Planet49 ocenę mojego zachowania w zakresie odwiedzania i korzystania ze stron internetowych partnerów reklamowych i dopasowanie reklam do moich preferencji przez Remintrex. Pliki cookies mogę usunąć w dowolnym czasie. Więcej na ten temat przeczytacie Państwo tutaj". Zasadniczo informacje dostarczone przez pliki cookies miały umożliwiać Planet49 wysyłanie e-maili reklamowych uwzględniających zainteresowania ujawnione na stronach internetowych partnerów reklamowych tej spółki. W plikach tych zapisywany był numer identyfikacyjny, który w powiązaniu z danymi wpisywanymi przez zapisującego się na loterię użytkownika, powodował, że zawarte w plikach cookies informacje stanowiły dane osobowe, które z plików cookies nie były przekazywane poszczególnym partnerom reklamowym Planet49. Użytkownicy informowani byli także o możliwości usunięcia w dowolnym momencie plików ze swojej przeglądarki internetowej, a także o możliwości cofnięcia w dowolnym momencie udzielonej zgody.

Związek organizacji konsumenckich zakwestionował – na drodze sądowej – praktykę pozyskiwania zgód zastosowaną przez Planet49. Na dalszym etapie postępowania w przedmiotowej sprawie niemiecki Federalny Trybunał Sprawiedliwości (FTS) uznał, że wynik postępowania głównego zależy od wykładni art. 5 ust. 3 i art. 2 lit. f dyrektywy 2002/58, art. 2 lit. h dyrektywy 95/46[4], jak też art. 6 ust. 1 lit. a rozporządzenia 2016/679. Mając wątpliwości dotyczące stosowania wskazanych przepisów prawa unijnego, FTS zwrócił się do TSUE z pytaniami prejudycjalnymi dotyczącymi skuteczności wyrażenia zgody na wykorzystanie plików cookies poprzez domyślnie zaznaczone pole wyboru, wpływu na stosowanie art. 5 ust. 3 i art. 2 lit. f dyrektywy 2002/58 faktu, że przechowywane lub udostępniane informacje są danymi osobowymi, a także zakresu obowiązków informacyjnych, wynikających z art. 5 ust. 3 dyrektywy 2002/58.

Wykorzystywanie plików cookies w urządzeniach końcowych użytkowników reguluje w prawie unijnym art. 5 ust. 3 dyrektywy 2002/58, w myśl którego: „Państwa

[4] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. UE L 281, s. 31 ze zm.; dalej: dyrektywa 95/46).

członkowskie zapewniają, aby przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym abonenta lub użytkownika było dozwolone wyłącznie pod warunkiem, że dany abonent lub użytkownik wyraził zgodę zgodnie z dyrektywą 95/46 po otrzymaniu jasnych i wyczerpujących informacji, między innymi o celach przetwarzania. Nie stanowi to przeszkody dla każdego technicznego przechowywania danych ani dostępu do nich jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej, lub gdy jest to ściśle niezbędne w celu świadczenia usługi przez dostawcę usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika". Obowiązujące obecnie rozwiązanie oznacza przyjęcie tzw. mechanizmu *opt-in*, w którym użytkownik musi co do zasady wyrazić zgodę na wykorzystywane plików cookies przed rozpoczęciem ich stosowania. Wymóg uzyskania zgody nie ma jednak charakteru bezwzględnego. Uzyskanie zgody nie jest konieczne, w przypadku gdy wykorzystywanie plików typu cookies jest niezbędne dla wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej lub w celu realizacji usługi przez dostawcę usługi społeczeństwa informacyjnego, świadczonej na żądanie abonenta lub użytkownika. Oznacza to, że zgody nie wymaga m.in. instalowanie plików cookies, które są niezbędne do zapewnienia prawidłowego funkcjonowania witryny internetowej. Wskazane w art. 5 ust. 3 dyrektywy 2002/58 wyjątki nie miały jednak zastosowania w sprawie rozpoznawanej przez TSUE[5].

Zgodnie z art. 2 lit f dyrektywy 2002/58, zgoda użytkownika lub abonenta na potrzeby tej dyrektywy odpowiada zgodzie podmiotu danych osobowych określonej w dyrektywie 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Druga z wymienionych dyrektyw została uchylona i zastąpiona ogólnym rozporządzeniem o ochronie danych, które zaczęło bezpośrednio obowiązywać we wszystkich państwach członkowskich Unii Europejskiej z dniem 25 maja 2018 r. Stosownie do art. 94 ust. 2 tego rozporządzenia, wszelkie odesłania do uchylonej przez to rozporządzenie dyrektywy 95/46 należy traktować jako odesłania do ogólnego rozporządzenia o ochronie danych.

Wniosek o wydanie orzeczenia w trybie prejudycjalnym wpłynął do TSUE jeszcze przed tą datą, jednakże trybunał uznał, że w okolicznościach sprawy, konieczne jest udzielenie odpowiedzi na przedstawione pytania prejudycjalne zarówno na podstawie dyrektywy 95/46, jak i na podstawie rozporządzenia 2016/679.

Przechodząc do problemów przedstawionych w pierwszym z pytań prejudycjalnych, wpierw należy zauważyć, że art. 5 ust. 3 dyrektywy 2002/58 dotyczy instalowania plików cookies niezależnie od tego, czy dane w nich zapisywane są danymi osobowymi.

[5] Na marginesie rozważań można wspomnieć, że projekt rozporządzenia o e-prywatności zakłada rozszerzenie katalogu wyjątków od wymogu uzyskania zgody użytkownika na wykorzystywanie plików cookies, przy czym żaden z nich nie ma dotyczyć wykorzystywania danych z tych plików do celów marketingowych.

Zważywszy, że wykładnia pojęcia zgody w rozumieniu dyrektywy 2002/58 powinna być dokonywana na mocy odesłania zawartego w art. 2 lit f tej dyrektywy, na podstawie przepisów o ochronie danych osobowych – wcześniej art. 2 lit h dyrektywy 95/46, a obecnie art. 4 pkt 11 rozporządzenia 2016/679 – istotnym pytaniem jest, czy na interpretację przepisów o udzielaniu zgody na wykorzystywanie plików cookies ma wpływ to, czy informacje w nich przechowywane stanowią dane osobowe. Trybunał na to pytanie udzielił odpowiedzi przeczącej, podkreślając, że sposób interpretowania tych przepisów nie zmienia się ze względu na okoliczność, czy dane w plikach cookies mają charakter danych osobowych. Konkluzję taką potwierdza treść motywu 24 dyrektywy 2002/58, z której wynika, że wszelkie informacje przechowywane w urządzeniach końcowych użytkownika sieci łączności elektronicznej należą do sfery prywatnej tego użytkownika, podlegającej ochronie prawnej. Zdaniem trybunału, ochrona ta obejmuje wszystkich użytkowników niezależnie od tego, czy dane przechowywane w jego urządzeniu mogą być zakwalifikowane jako dane osobowe. Również sama konstrukcja odesłania do przepisów o ochronie danych osobowych zawarta w art. 2 lit. f dyrektywy 2002/58 nie daje podstaw do różnicowania wymogów co do wyrażenia zgody na wykorzystywanie plików cookie w zależności od tego, jaki charakter mają dane w nich zapisywane. Oznacza to, że kryteria skutecznego wyrażenia zgody na przetwarzanie danych osobowych wynikających obecnie z rozporządzenia 2016/679 stanowią jednocześnie wymogi wyrażenia zgody na użycie plików typu cookies na podstawie art. 5 ust. 3 dyrektywy 2002/58.

Na gruncie przepisów ogólnego rozporządzania o ochronie danych zgoda powinna zostać udzielona w sposób dobrowolny, konkretny, świadomy i jednoznaczny. Elementy te wynikają z definicji zgody zawartej w art. 4 pkt 11 rozporządzenia 2016/679. Zgodnie z tą definicją, zgoda na przetwarzanie danych osobowych jest okazaniem woli, którego treścią jest przyzwolenie na przetwarzanie danych, i które może być wyrażone w postaci oświadczenia lub wyraźnego działania potwierdzającego. Z motywu 32 rozporządzenia 2016/679 wynika, że zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych. Pewne dalsze wymogi co do konstrukcji zgody na przetwarzanie danych można wyprowadzić jeszcze z art. 6 ust. 1 lit a oraz art. 7 rozporządzenia 2016/679[6]. Jak się wskazuje w literaturze przedmiotu, w istotnej części definicja pojęcia danych osobowych z rozporządzenia 2016/679 powiela konstrukcję zgody – ukształtowaną przepisami dyrektywy 95/46[7]. Wskazane

[6] Art. 7 rozporządzenia 2016/679 doprecyzowuje warunki wyrażenia zgody, m.in. poprzez wprowadzenie obowiązku poinformowania o możliwości cofnięcia zgody jeszcze przed jej udzieleniem oraz wymogu, zgodnie z którym cofnięcie zgody musi być równie łatwe jak jej udzielenie. Wymogi te zarówno rzutują na zakres informacji przekazywanych użytkownikowi korzystającemu z serwisu internetowego stosującego pliki cookies, jak i mogą wpływać na dobór rozwiązań technicznych umożliwiających cofnięcie zgody na instalowanie plików cookies z danego serwisu.

[7] Tak D. Lubasz [w:] *idem*, *Komentarz do art. 4 pkt 11* [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* red. *Edyta* Bielak-Jomaa, Dominik Lubasz, Warszawa 2018, s. 243.

powyżej kryteria ważnej zgody na przetwarzanie danych osobowych korespondują w pewnym stopniu z tymi, które są wskazane w motywie 17 dyrektywy 2002/58, zgodnie z którym zgoda użytkownika lub abonenta może być udzielona w jakikolwiek sposób umożliwiający swobodne i świadome wyrażenie woli użytkownika, włączając zaznaczenie okna wyboru podczas przeglądania witryny internetowej.

Trybunał Sprawiedliwości Unii Europejskiej uznał, że zarówno na gruncie przepisów dyrektywy 95/46, jak i rozporządzenia 2016/679 nie ma się do czynienia z ważnie udzieloną zgodą w rozumieniu art. 5 ust. 3 dyrektywy 2002/58, jeżeli przechowywanie informacji lub dostęp do informacji już przechowywanych w urządzeniu końcowym użytkownika strony internetowej został zaakceptowany za pomocą domyślnie zaznaczonego pola wyboru, którego zaznaczenie użytkownik musi usunąć, aby odmówić udzielenia zgody.

W świetle konstrukcji zgody wynikającej z przepisów o ochronie danych osobowych takie rozstrzygnięcie nie może budzić żadnych wątpliwości. Zarówno z wcześniejszych, jak i obecnie obowiązujących przepisów regulujących sposób wyrażenia zgody na przetwarzanie danych osobowych należy wywieść, że zgoda ta musi być wyrażona w sposób czynny[8]. W motywie 32 ogólnego rozporządzenia o ochronie danych wyjaśniono, że wyrażenie zgody może polegać m.in. na zaznaczeniu pola wyboru podczas przeglądania strony internetowej, jednocześnie motyw ten wyklucza możliwość wyrażenia zgody poprzez „milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania". Zatem brak aktywności użytkownika strony internetowej polegający na nieodznaczeniu domyślnie zaznaczonego pola wyboru nie może być uznawany za skuteczne wyrażenie zgody[9]. Nie można bowiem przyjmować, że skoro dany podmiot nie odznaczył określonego pola wyboru na stronie internetowej, to w sposób wyraźny, jednoznaczny i świadomy wyraził zgodę na wykorzystywanie plików cookies przez dany serwis internetowy. Takiej oceny nie zmienia fakt, że aby kontynuować, użytkownik musiał jeszcze kliknąć link zapisujący go na loterię. Wymóg jednoznaczności zgody oznacza, że jej wyrażenie nie powinno budzić wątpliwości co do zamiaru osoby, która jej udziela. Dlatego zgoda na pliki cookies nie może być wywodzona z kliknięcia linku umożliwiającego zapisanie się na loterię. Nie jest to bowiem działanie jednoznaczne, zważywszy, że użytkownik może w ogóle nie mieć świadomości, co do tego, iż w ten sposób wyraża „przy okazji" zgodę na instalowanie i dostęp do plików cookies[10]. Jak słusznie podkreślił trybunał, „nie można […] wykluczyć, że wspomniany użytkownik

---

[8] Zob. też K. Wiedemann, *The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado About Nothing?*, „International Review of Intellectual Property and Competition" 2020, nr 51, s. 543–553, https://link.springer.com/article/10.1007/s40319-020-00927-w [dostęp: 10.11.2021].

[9] Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4* [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018, s. 230.

[10] Zob. też uwagi dotyczące tej kwestii, w tym odniesienia do treści art. 7 ust. 2 rozporządzenia 2016/679 poczynione przez K. Wiedemanna [w:] *idem*, *The ECJ's Decision*…; zob. ponadto R. Barcelo, A. Ibraimova, E. Yaltaghian, *The Planet49 Decision: Key Takeaways*, „The National Law Review" z dnia 2 października 2019 r., https://www.natlawreview.com/article/planet49-decision-key-takeaways [dostęp: 10.11.2021].

nie przeczytał informacji towarzyszącej domyślnie zaznaczonemu okienku czy wręcz nie zwróci uwagi na to okienko przed podjęciem dalszej aktywności na odwiedzanej przezeń stronie internetowej".

Odnotowania wymaga, że trybunał nie rozpatrywał kwestii, czy w przypadku, w którym zgoda użytkownika na przetwarzanie jego danych osobowych do celów reklamowych decyduje o tym, czy może on uczestniczyć w loterii promocyjnej, spełnia wymóg wyrażenia zgody w sposób dobrowolny, uznając, że leży to poza zakresem sprawy[11]. Niewątpliwe jednak problematyka uzależniania możliwości korzystania z określonych usług od wyrażenia zgody na wykorzystanie danych osobowych w celach marketingowych jest niezwykle ważka, a ocena dopuszczalności zastosowania takiego uwarunkowania będzie stanowić kluczową kwestię w wypadkach pozyskiwania takich zgód, gdy pozostałe wymogi wyrażenia skutecznej zgody będą spełnione.

Podkreślenia wymaga, że przed podjęciem przez użytkownika działania wyrażającego zgodę na pliki cookies, żadne z tych plików, które wymagają takiej zgody, nie mogą być instalowane na urządzeniu użytkownika. Niewłaściwym działaniem serwisu internetowego jest zatem instalowanie plików cookies, zanim użytkownik będzie miał możliwość wyrażenia na nie zgody, nawet wówczas, gdy następnie są one usuwane, w razie gdy zgoda ta nie zostanie udzielona. Automatyczne instalowanie plików cookies (w tym reklamowych) zaraz po wejściu na strony internetowe google.fr oraz amazon.fr było elementem ustaleń w sprawach, w których francuski organ właściwy do spraw ochrony danych osobowych (*Commission Nationale de l'Informatique et des Libertés* – CNIL) w 2020 r. nałożył kary pieniężne na Google LLC i Google Ireland Limited (odpowiednio w wysokości 60 mln i 40 mln euro)[12] oraz na Amazon Europe Core (w wysokości 35 mln euro)[13]. Kary te zostały nałożone za nieprzekazywanie użytkownikowi wymaganych prawem informacji w związku z posługiwaniem się cookies, a także za zapisywanie plików cookies bez uprzedniej zgody użytkowników. Dodatkowo, Google został ukarany za nierespektowanie prawa do sprzeciwu.

Wynikający z wyroku TSUE wymóg udzielania zgody w sposób aktywny wyklucza posługiwanie się na stronach internetowych banerami zgód na pliki cookies z domyślnie zaznaczonymi polami wyboru – nie dotyczy to jednak plików cookies, których używanie nie wymaga zgody. Pasywnym zachowaniem, niestanowiącym zgody, będzie także pozostanie na stronie i dalsze jej przeglądanie, nawet jeśli użytkownik został poinformowany o stosowaniu plików cookies, ale nie wyraził w żaden aktywny sposób akceptacji na ich instalowanie[14]. Stąd też wykluczone jest przyjęcie, że zgoda na

[11] Zob. pkt 64 glosowanego wyroku.

[12] Źródła: https://www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland [dostęp: 10.11.2021].

[13] Źródła: https://www.cnil.fr/en/cookies-financial-penalty-35-million-euros-imposed-company-amazon-europe-core [dostęp: 10.11.2021].

[14] Europejska Rada Ochrony Danych w swych wytycznych wskazywała, że „w myśl motywu 32 przewijanie w dół, przeglądanie strony internetowej lub podobne działania użytkownika w żadnych okolicznościach nie spełniają wymogu wyraźnego i potwierdzającego działania: działania takie może być trudno odróżnić od innych działań lub reakcji użytkownika, a zatem niemożliwe również będzie stwierdzenie, że uzyskano jednoznaczną zgodę. Ponadto, w takim przypadku trudne będzie

pliki cookies może być wyrażona poprzez same ustawienia przeglądarki internetowej, bez podjęcia przez użytkownika jakiejkolwiek aktywności na odwiedzanej witrynie. Użytkownik bowiem może nie tylko nie być świadomy, jakie są domyślne ustawienia preferencji dotyczące instalowania plików cookies w jego przeglądarce internetowej, ale może też nie wiedzieć, że przeglądarka umożliwia określenie takich preferencji. Nie można też wykluczyć, że użytkownik posługuje się oprogramowaniem, które w ogóle nie zawiera takiej funkcjonalności.

W kontekście korzystania z domyślnych ustawień przeglądarki internetowej w celu ustanowenia własnych preferencji co do instalowania plików cookies należy zwrócić uwagę na złożony problem możliwości wykorzystywania tego typu ustawień w razie przetwarzania danych z plików cookies w różnych celach. Złożoność tego problemu wynika także z konieczności uwzględnienia treści przepisów krajowych implementujących w danym państwie członkowskim postanowienia dyrektywy 2002/58. Opierając się na kryterium dobrowolności zgody na przetwarzanie danych osobowych, należy uznać, że w każdym przypadku, w którym dane z plików cookie są wykorzystywane w różnych celach (wymagających zgody) i jednocześnie przetwarzane dane stanowią dane osobowe operator serwisu internetowego powinien zbierać odrębne zgody na poszczególne cele[15]. Przykładowo, sytuacja taka ma miejsce, gdy użytkownik zalogowany jest do określonego serwisu, a dane zapisywane w plikach cookies umożliwiają jego identyfikację. Sytuacja taka miała miejsce też w sprawie, w której wydano glosowany wyrok – pliki cookies wykorzystywane przez Planet49 zawierały bowiem identyfikatory powiązane z innymi danymi konkretnego użytkownika. W przypadkach takich jak wskazane powyżej serwis nie może opierać się na jednej ogólnej zgodzie, w tym wyrażonej poprzez ustawienia przeglądarki, lecz pozyskać odrębne zgody na poszczególne cele przetwarzania, które takowej zgody wymagają[16]. W razie przetwarzania danych osobowych łączne wyrażenie zgody na niepowiązane cele – np. cele analityczne i cele marketingowe podmiotów trzecich – nie będzie spełniać wymogu

---

zapewnienie użytkownikowi możliwości wycofania zgody w sposób równie łatwy, co jej udzielenie". Zob. wytyczne 05/2020 Europejskiej Rada Ochrony Danych dotyczące zgody na mocy rozporządzenia 2016/679, wersja 1.1 przyjęta dnia 4 maja 2020 r., s. 21, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pl.pdf [dostęp: 10.11.2021]; dalej: wytyczne EROD 05/2020. Por. też uwagi dotyczące czynności przeglądania strony w kontekście wymogu uzyskania zgody na wykorzystywanie plików cookies, sformułowane przez: R. Barcelo, A. Ibraimova, E. Yaltaghian, *The Planet49 Decision*… oraz G. Zanfir-Fortuna, Planet49 CJEU Judgment brings some 'Cookie Consent' Certainty to Planet Online Tracking, opubl. w dniu 3 października 2019 r., http://www.pdpecho.com [dostęp: 10.11.2021].

[15] Uzupełniająco należy wskazać, że w przypadku przetwarzania danych z plików cookies, które mają charakter danych osobowych, w rachubę może również wchodzić wymóg uzyskania swojego rodzaju kwalifikowanej zgody na gruncie rozporządzenia o ochronie danych a mianowicie „zgody wyraźniej". Przykładowo, wymóg uzyskania takiej zgody, w określonych w art. 22 rozporządzenia 2016/679 przypadkach, zachodzić będzie w razie podejmowania decyzji w oparciu o zautomatyzowane przetwarzanie danych, w tym w o profilowanie. Sytuacja taka może przykładowo wiązać się z wyświetlaniem w stosunku do użytkowników internetu, czyli podmiotów danych osobowych – reklam profilowanych w oparciu m.in. o dane zapisywane w plikach cookies.

[16] Por. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 6* [w:] *Rozporządzenie*…, s. 280.

dobrowolności na gruncie rozporządzenia 2016/679. W decyzji wydanej w styczniu 2019 r. francuski organ nadzorczy CNIL nałożył na Google LLC karę w wysokości 50 mln euro po ustaleniu w prowadzonym postępowaniu, m.in. że na prowadzonym przez Google serwisie internetowym brak jest możliwości wyrażenia oddzielnych zgód na różne cele przetwarzania[17].

Zważywszy, że narzędzia dostarczane przez przeglądarki internetowe zasadniczo nie ustalają celów, w jakich instalowane są pliki cookies i w sposób precyzyjny nie pozwalają różnicować preferencji co do różnych typów takich plików, nie da się efektu uzyskania odrębnych zgód osiągnąć poprzez zaakceptowanie w danym serwisie ustawień przeglądarki internetowej użytkownika. W praktyce oznacza to, że serwis internetowy, przetwarzając dane osobowe w plikach cookies, musi stosować własne rozwiązania umożliwiające zarządzanie takimi plikami i zgodami wyrażanymi przez użytkowników serwisu.

Na gruncie prawa polskiego – art. 173 ustawy – Prawo telekomunikacyjne[18], stanowiącego implementację art. 5 ust. 3 dyrektywy 2002/58 oraz art. 174 tejże ustawy[19] inaczej ocenia się sytuację, w których dane z plików cookies są przetwarzane w różnych celach, lecz nie zawierają danych osobowych. Zasadniczo przyjmuje się, że wystarczające jest wówczas wyrażenie jednej ogólnej zgody na instalowanie plików cookies, w tym także poprzez odesłanie do ustawień przeglądarki. Stanowisko takie opiera się na treści art. 173 ust. 2 p.t., który przewiduje, że abonent lub użytkownik końcowy może wyrazić zgodę za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub za pomocą konfiguracji usługi. Jednakże stanowisko TSUE zajęte w sprawie *Planet49*, w myśl którego wykładnia przepisów mająca zastosowanie przy zbieraniu zgód na pliki cookies nie powinna być różnicowana ze względu na to, czy zawierają one dane osobowe, czy nie – może potencjalnie prowadzić do bardziej rygorystycznej wykładni. W zarysowanym kontekście należy zauważyć, że motyw 32 rozporządzenia 2016/679 dopuszcza możliwość wyrażenia zgody poprzez wybór ustawień technicznych do korzystania z usług społeczeństwa informacyjnego. Jednocześnie Europejska Rada Ochrony Danych wyjaśniała, że w przypadku wyrażenia zgody za pośrednictwem ustawień przeglądarki internetowej ustawienia takie powinny być opracowane zgodnie z przesłankami ważnej zgody określonymi w ogólnym rozporządzeniu o ochronie danych, takimi jak na przykład fakt, że zgoda powinna być szczegółowa dla każdego z zamierzonych celów[20]. Szersza analiza tego problemu oraz relacji między przepisami unijnymi a przepisami krajowymi stanowiącymi implementację art. 5 ust. 3 dyrektywy 2002/58 wykracza poza zakres niniejszej glosy. Należy oczekiwać, że ostateczne

[17] Źródło: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc [dostęp: 10.11.2021].

[18] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (tekst. jedn.: Dz. U. z 2021 r., poz. 576; dalej: p.t.).

[19] Zgodnie z przywołanym art. 174 p.t., do uzyskania zgody abonenta lub użytkownika końcowego stosuje się przepisy o ochronie danych osobowych.

[20] Zob. wytyczne EROD 05/2020, s. 21.

rozwiązanie tego dylematu przyniesie przyjęcie rozporządzenia o e-prywatności[21]. Projekt tego rozporządzenia zakłada, tak jak ma to miejsce obecnie, że do zgody na wykorzystanie technologii typu cookies zastosowanie znajdą warunki zgody wynikające z rozporządzenia 2016/679[22]. Projekt rozporządzenia o e-prywatności przewiduje także, że zgodę tę będzie można wyrazić poprzez wykorzystanie właściwych ustawień technicznych oprogramowana umożliwiającego komunikację elektroniczną, w tym wyszukiwanie i prezentację informacji w internecie. Przy czym zawsze nadrzędna w stosunku do ustawień oprogramowania ma być zgoda wyrażona przez użytkownika w sposób bezpośredni[23].

Przedmiotem rozważań TSUE w wyroku w sprawie *Planet49* był również zakres informacji, jaki należy przekazać na podstawie art. 5 ust. 3 dyrektywy 2002/58 osobie wyrażającej zgodę na wykorzystywanie plików cookies, a konkretnie – kwestia, czy muszą one zawierać także informację o okresie funkcjonowania plików cookies oraz o tym, czy podmioty trzecie mogą uzyskać dostęp do tych plików.

W myśl art. 5 ust. 3 dyrektywy 2002/58, wykorzystywanie plików cookies możliwe jest pod warunkiem, że zgoda użytkownika na nie została wyrażona „po otrzymaniu jasnych i wyczerpujących informacji, między innymi o celach przetwarzania". Zdaniem TSUE, w sytuacji, w której pliki cookies mają na celu zbieranie informacji do celów reklamowych w odniesieniu do produktów partnerów organizatora loterii promocyjnej, zarówno wskazanie okresu funkcjonowania plików cookies, jak też określenie, czy osoby trzecie mogą mieć dostęp do tych plików stanowi element jasnych i wyczerpujących informacji, które należy przekazać zgodnie z przywołanym przepisem dyrektywy 2002/58. Trybunał zauważył również, że podanie informacji dotyczących okresu funkcjonowania plików cookies spełnia wymóg rzetelnego przetwarzania danych[24].

Odnosząc się do stanowiska wyrażonego przez trybunał, w pierwszej kolejności należy zauważyć, że jednym z podstawowych kryteriów wyrażenia skutecznej zgody na gruncie przepisów ogólnego rozporządzenia o ochronie danych jest wyrażenie jej w sposób świadomy. Kryterium świadomości zgody wiąże się z wymogiem przekazania osobie, która ma jej udzielić, informacji niezbędnych do zrozumienia istoty tego, na co wyraża zgodę i typowych konsekwencji jej wyrażenia[25]. Należy uznać, że kwestia udostępniania danych pozyskiwanych na podstawie zgody podmiotom trzecim jest istotnym aspektem realizowanego celu lub celów przetwarzania danych. Konsekwentnie należy uznać, że udostępnianie danych z plików cookies podmiotom trzecim stanowi element charakterystyki celu, w jakim dane te są przetwarzane. W przypadku udostępniania danych z plików cookies podmiotom trzecim, udostępnianie to wpły-

[21] Aktualnie proponowane rozwiązania zawiera art. 8 projektu rozporządzenia o e-prywatności.

[22] Zob. art. 4a projektu rozporządzenia o e-prywatności.

[23] Zob. art. 4 ust. 2 i 2aa projektu rozporządzenia o e-prywatności.

[24] W piśmiennictwie zauważono, że spostrzeżenie takie jest to o tyle wyjątkowe, iż trybunał w swoim orzecznictwie w zakresie ochrony danych osobowych zazwyczaj nie dokonuje ustaleń w odniesieniu do rzetelności przetwarzania – zob. G. Zanfir-Fortuna, Planet49…

[25] Por. P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 128.

wa niewątpliwe na skalę przetwarzania, która z kolei powinna być istotnym kryterium branym pod uwagę przy wyrażaniu świadomiej zgody na wykorzystywanie plików cookies. Zatem słuszna jest konkluzja, że informacja o udostępnianiu danych z plików cookies podmiotom trzecim wchodzi w zakres informacji przekazywanych na podstawie art. 5 ust. 3 dyrektywy 2002/58.

Natomiast dyskusyjna jest teza, która zdaje się wynikać z trzeciego punktu sentencji glosowanego wyroku, i która została sformułowana także w opinii rzecznika generalnego[26], zgodnie z którą informacja udzielana użytkownikowi strony internetowej o wykorzystywaniu plików cookies, gdy dane z nich nie są udostępnianie żadnym podmiotom trzecim, musi również wyraźnie stwierdzać ten fakt[27]. W wyroku, w kontekście tego zagadnienia, TSUE przywołał treść art. 10 dyrektywy 95/46 oraz art. 13 rozporządzenia 2016/679, określających zakres informacji koniecznych do przekazania osobie, od której dane są pozyskiwane. Należy jednak zauważyć, że z treści art. 13 rozporządzania 2016/679 wyraźnie wynika, że informacje o odbiorcach danych osobowych lub o kategoriach odbiorców muszą być podane jedynie wtedy, jeżeli takowi istnieją. Jak wskazuje się w literaturze przedmiotu, nie zawsze wszystkie wymienione w art. 13 ust. 1 kategorie informacji są wymagane, o czym m.in. świadczy warunkowe stwierdzenie zawarte w lit. e wskazanego przepisu[28]. Co za tym idzie, nie wynika z niego wymóg wyraźnego wskazywania, że takowych odbiorców nie ma. Podobnie powinna być też intepretowana treść art. 10 lit. c nieobowiązującej już dyrektywy 95/46. Stąd też zastrzeżenie, że podmioty trzecie nie uzyskują dostępu do danych z plików cookies, można co najwyżej uznać za element uzupełniający opis celu, w jakim dane z cookies są wykorzystywane, a jakim jest podejmowanie określonej formy działań marketingowych na rzecz tych podmiotów.

Przechodząc do tezy o konieczności zawarcia w informacji przekazywanej użytkownikom stron internetowych o okresie funkcjonowania plików cookies, należy ją uznać za w pełni zasadną. Okres wykorzystywania takich plików wprost przekłada się na skalę przetwarzania danych, gdyż wpływa na ilość zbieranych informacji o zachowaniach i preferencjach związanych z przeglądaniem stron internetowych przez konkretnego użytkownika. Zatem informacje te są kluczowe, aby zrozumieć zasadnicze konsekwencje udzielenia zgody. Stąd też, przekazanie informacji co do czasu przechowywania plików cookies, względnie kryteriów wskazywania tego czasu, stanowi jeden z elementów wymogu wyrażenia świadomiej zgody na ich instalowanie. W tym przypadku trafne jest odwołanie się, jak uczynił to TSUE, do treści art. 13 ust. 2 lit. a rozporządzenia 2016/679, który to przepis ma wprost zastosowanie do zbierania danych za

[26] Por. pkt 119–121 opinii rzecznika generalnego przedstawionej w dniu 21 marca 2019 r. w sprawie C-673/17, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:62017CC0673 [dostęp: 10.11.2021]; dalej: opinia rzecznika generalnego.

[27] W wersji angielskojęzycznej punkt trzeci wyroku brzmi: "Article 5(3) of Directive 2002/58, as amended by Directive 2009/136, must be interpreted as meaning that the information that the service provider must give to a website user includes […] whether or not [podkr. autora] third parties may have access to those cookies".

[28] Zob. P. Fajgielski, *Ogólne*…, s. 236; por. też K. Wiedemann, *The ECJ's Decision*…

pomocą technologii typu cookies w przypadku zakwalifikowania ich jako danych osobowych, a który stanowi, że przy pozyskiwaniu danych osobowych – w celu zapewnienia rzetelności i przejrzystości przetwarzania – należy podać informacje dotyczące okresu przechowywania tych danych, a jeżeli nie jest to możliwe, to kryteria ustalania tego okresu[29].

Powyższe oznacza, że operatorzy witryn internetowych muszą zidentyfikować wszystkie typy plików cookies jakie są wykorzystywane na ich stronach internetowych, a następnie określić czas ich funkcjonowania, a także zidentyfikować podmioty trzecie, które mogą uzyskać dostęp do danych zawartych w tych plikach, aby następnie móc przekazać stosowne informacje użytkownikom.

Literatura

Barcelo R., Ibraimova A., Yaltaghian E., *The Planet49 Decision: Key Takeaways*, „The National Law Review" z dnia 2 października 2019 r., https://www.natlawreview.com/article/planet49-decision-key-takeaways [dostęp: 10.11.2021].

Lubasz D., *Komentarz do art. 4 pkt 11* [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Litwiński P., Barta P., Kawecki M., *Komentarz do art. 4* [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018.

Litwiński P., Barta P., Kawecki M., *Komentarz do art. 6* [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Wiedemann K., *The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado About Nothing?*, „International Review of Intellectual Property and Competition" 2020, nr 51, https://link.springer.com/article/10.1007/s40319-020-00927-w [dostęp: 10.11.2021].

Zanfir-Fortuna G., *Planet49 CJEU Judgment brings some 'Cookie Consent' Certainty to Planet Online Tracking,* http://www.pdpecho.com [dostęp: 10.11.2021].

[29] Z kolei choć w art. 10 dyrektywy 95/46 nie został sformułowany wprost obowiązek wskazania okresu przetwarzania danych, to jednak wymagano podania wszelkich dodatkowych informacji niezbędnych do zapewnienia rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą. Tego typu informacją potencjalnie mogła być w określonych sytuacjach również informacja o czasie trwania przetwarzania danych.

Streszczenie

Michał Miłosz

Warunki wyrażenia zgody na użycie plików typu cookies

W glosie został poddany analizie wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 1 października 2019 r. w sprawie C-673/17. Komentowane orzeczenie stanowi pierwszą wypowiedź TSUE w kwestii warunków wyrażenia zgody na użycie tzw. plików cookies w urządzeniach końcowych użytkowników, której wymóg uzyskania wynika w prawie unijnym z art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, uwzględniające przepisy ogólnego rozporządzenia o ochronie danych. Tezy wyrażone w glosowanym wyroku TSUE wyznaczają kierunek wykładni przepisów znajdujących zastosowanie przy instalowaniu plików cookies, i tym samym powinny oddziaływać na praktykę pozyskiwania zgód użytkowników na wykorzystywanie tego typu technologii. W przyszłości na tę praktykę istotny wpływ będzie miało również uchwalenie, a następnie wejście w życie procedowanego obecnie projektu rozporządzenia o prywatności i łączności elektronicznej. Rozporządzenie to będzie zawierać rozbudowaną regulację dotyczącą korzystania z możliwości urządzeń końcowych użytkowników do przetwarzania i przechowywania oraz gromadzenie informacji z tych urządzeń obejmujące również stosowanie plików cookies.

Słowa kluczowe: cookies; zgoda; warunki i forma zgody; wyraźne działanie potwierdzające; zgoda nieskuteczna; RODO.

Summary

Michał Miłosz

Consent for the Use of Cookies

The commented decision of the Court of Justice of the European Union of October 1st, 2019, case C-673/17 is the first ruling regarding conditions for giving consent for the use of "cookies" in end-user devices, the requirement of which is provided for in EU law under Article 5 (3) of the Directive on privacy and electronic communications, that takes into consideration the provisions of the General Data Protection Regulation. Theses expressed in the commented decision of the CJUE set the direction for the interpretation of the provisions applicable to the installation of cookies and thus should affect the practice of obtaining users' consent to use this type of technology. In the future, this practice will also be significantly influenced by the adoption and subsequent entry into force of the currently pending draft regulation of the European Parliament and of the Council on the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on privacy and electronic communications), which will include an extensive regulation on the use of the capabilities of end-users' devices for processing and storage, as well as collecting information from these devices, including the use of cookies. This commentary contains an analysis of the abovementioned decision of the Court of Justice of the EU.

Keywords: cookies; consent; conditions and form of consent; clear affirmative action; ineffective consent; GDPR.

Pierwsza administracyjna kara pieniężna nałożona na podmiot z sektora publicznego

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie
z dnia 26 sierpnia 2020 r., II SA/Wa 2826/19

1. **Czynności o charakterze techniczno-organizacyjnym leżą w gestii administratora danych osobowych, ale nie mogą być dobierane w sposób całkowicie swobodny i dobrowolny, bez uwzględnienia stopnia ryzyka czy charakteru chronionych danych osobowych. Bez wątpienia środki podejmowane przez skarżącego nie zapewniły bezpieczeństwa, co należycie wykazał organ (…).**
2. **(…) Prawidłowo organ ocenił naruszenie art. 5 ust. 1 lit. e w związku z art. 5 ust. 2, tj. zasady ograniczenia przechowywania oraz art. 24 rozporządzenia 2016/679 poprzez brak odpowiednich polityk, dotyczących przetwarzania danych osobowych w BIP Urzędu Miejskiego w A. pod kątem ich aktualności i celowości publikacji oraz określających terminy usunięcia danych osobowych. Zasada określona mianem „ograniczenia przechowywania", określona w art. 5 ust 1 lit. 3 rozporządzenia 2016/679 stanowi, iż „dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane". Nadto „dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania"). Zgodnie z tą zasadą, po osiągnięciu celów, w jakich przetwarzane są dane osobowe, powinny zostać one usunięte albo skasowane.**

Marlena Sakowska-Baryła
m.sakowskabaryla@kancelariasbc.pl
Uczelnia Łazarskiego
ORCID: 0000-0002-3982-976X

https://doi.org/10.26881/gsp.2021.4.10

Wojewódzki Sąd Administracyjny w Warszawie wyrokiem z dnia 26 sierpnia 2020 r., II SA/Wa 2826/19[1] oddalił skargę Burmistrza Aleksandrowa Kujawskiego na decyzję Prezesa Urzędu Ochrony Danych Osobowych z dnia 18 października 2019 r., ZSPU.421.3.2019, w której organ nadzorczy, stwierdzając szereg naruszeń przepisów RODO[2], obok zastosowania uprawnień naprawczych zastosował administracyjną karę pieniężną w kwocie 40.000 zł. Wskazaną decyzję uznać należy za istotną nie tylko z tego względu, że jest ona pierwszą w Polsce decyzją Prezesa Urzędu Ochrony Danych Osobowych (Prezes UODO), nakładającą administracyjną karę pieniężną w sektorze publicznym. To bowiem jednocześnie decyzja, która odnosi się do kwestii zastosowania przepisów RODO do przetwarzania danych osobowych, jakie ma miejsce przy realizacji prawa dostępu do informacji publicznej, a także dobrze obrazuje kilka innych zagadnień doniosłych przy organizacji systemu ochrony danych osobowych w sektorze publicznym, które wcześniej nie zawsze były postrzegane jako pierwszoplanowe.

W wyroku w sprawie II SA/Wa 2826/19 WSA w Warszawie w pełni podzielił argumentację Prezesa UODO, dlatego też w niniejszej glosie nie sposób obyć się bez sięgania po ustalenia zawarte w tej decyzji. Choć w chwili złożenia tekstu do publikacji przedmiotowy wyrok nie jest prawomocny, to jednak ze względu na istotne wątki podejmowane w sprawie, warto przyjrzeć się ustaleniom dokonanym przez WSA w Warszawie oraz przez organ nadzorczy na kanwie stanu faktycznego, który w znacznej mierze odnosi się do pewnych specyficznych dla sektora publicznego operacji przetwarzania danych osobowych oraz uwarunkowań techniczno-organizacyjnych, które należą do kluczowych dla podmiotów z sektora publicznego.

Stan faktyczny

Jak wynika z analizowanego uzasadnienia wyroku WSA w Warszawie, wydanie decyzji przez Prezesa UODO było poprzedzone kontrolą tego organu, którą objęty został sposób przetwarzania danych osobowych przez Burmistrza Aleksandrowa Kujawskiego (Burmistrz) w ramach procesu wysyłki korespondencji i prowadzenia Biuletynu Informacji Publicznej (BIP), a także sposób prowadzenia rejestru czynności przetwarzania oraz dokumentowania naruszeń ochrony danych osobowych. Na podstawie zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Burmistrz, jako administrator, naruszył przepisy o ochronie danych osobowych, w związku z czym Prezes UODO wszczął w tym przedmiocie postępowanie administracyjne zakończone wspomnianą we wstępie decyzją, w której Prezes UODO stwierdził naruszenie przez Burmistrza przepisów:

[1] Wyrok WSA w Warszawie z dnia 26 sierpnia 2020 r., II SA/Wa 2826/19, LEX nr 3067899.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1 ze zm.; dalej: RODO).

1) art. 5 ust. 1 lit. a oraz lit. f w zw. z art. 5 ust. 2 RODO, tj. zasady zgodności z prawem i zasady poufności oraz art. 28 ust. 3 rozporządzenia 2016/679, poprzez udostępnianie danych osobowych na rzecz kilku zewnętrznych podmiotów bez podstawy prawnej, tj. bez uprzedniego zawarcia z ww. podmiotami umów powierzenia danych osobowych, o której mowa w art. 28 ust. 3 rozporządzenia 2016/679, w związku z prowadzeniem strony internetowej BIP Urzędu Miejskiego w Aleksandrowie Kujawskim;
2) art. 5 ust. 1 lit. e w związku z art. 5 ust. 2, tj. zasady ograniczenia przechowywania oraz art. 24 RODO poprzez brak odpowiednich polityk dotyczących przetwarzania danych osobowych w BIP Urzędu Miejskiego w Aleksandrowie Kujawskim pod kątem ich aktualności i celowości publikacji oraz określających terminy usunięcia danych osobowych;
3) art. 5 ust. 1 lit. f w związku z art. 5 ust. 2 RODO, tj. zasady integralności i poufności, zasady prawidłowości, oraz art. 24 RODO poprzez nieprzeprowadzenie analizy ryzyka związanego z korzystaniem przez Burmistrza z kanału YouTube w celu transmisji nagrań z obrad Rady Miasta Aleksandrowa Kujawskiego;
4) art. 5 ust. 1 lit. f w związku z art. 5 ust. 2 RODO, tj. zasady integralności i poufności, oraz art. 32 RODO poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych mających na celu zabezpieczenie danych osób fizycznych w związku z przechowywaniem nagrań sesji Rady Miasta wyłącznie na serwerach YouTube, bez wykonywania i przechowywania kopii zapasowych tych nagrań w zasobach własnych Urzędu Miejskiego w Aleksandrowa Kujawskiego;
5) art. 5 ust. 2 RODO, tj. zasady rozliczalności oraz art. 30 ust. 1 lit. d oraz lit. f RODO, poprzez niewskazanie w rejestrze czynności przetwarzania danych osobowych, dla czynności związanych z publikacją informacji na stronie BIP Urzędu Miasta w Aleksandrowie Kujawskim, wszystkich odbiorców danych oraz niewskazanie dla tych czynności przetwarzania planowanego terminu usunięcia danych w sposób zapewniający przetwarzanie danych zgodnie z zasadą ograniczonego przechowywania.

W związku z tak scharakteryzowanymi naruszeniami Prezes UODO nakazał Burmistrzowi dostosowanie operacji przetwarzania danych osobowych do przepisów RODO, w terminie 60 dni od dnia, w którym przedmiotowa decyzja stanie się ostateczna, poprzez:

1) zaprzestanie udostępniania danych osobowych na rzecz zewnętrznych podmiotów, bez podstawy prawnej, tj. bez uprzedniego zawarcia umów powierzenia danych osobowych z ww. podmiotami, o której mowa w art. 28 ust. 3 rozporządzenia 2016/679, w związku z prowadzeniem strony internetowej BIP Urzędu Miejskiego w Aleksandrowie Kujawskim;
2) wdrożenie polityk:
   a) określających okresy przetwarzania danych w BIP Urzędu Miejskiego w Aleksandrowie Kujawskim zgodne z przepisami prawa lub niezbędne do realizacji celów, dla których dane są przetwarzane;
   b) zapewniających przestrzeganie terminów usuwania danych;

3) przeprowadzenie analizy ryzyka w związku z publikacją nagrań sesji rady miejskiej i wdrożenie odpowiednich środków organizacyjnych i technicznych w związku z przetwarzaniem danych osobowych na kanale YouTube w związku z transmisją nagrań sesji rady miejskiej oraz przechowywaniem nagrań na serwerach YouTube;
4) wdrożenie odpowiednich środków organizacyjnych i technicznych mających na celu zabezpieczenie danych osób fizycznych pochodzących z nagrań sesji Rady Miasta Aleksandrowa Kujawskiego poprzez zapewnienie dostępności kopii zapasowych w zasobach własnych Urzędu Miejskiego w Aleksandrowie Kujawskim;
5) ujęcie w rejestrze czynności przetwarzania danych osobowych, dla czynności przetwarzania związanych z prowadzeniem BIP, informacji o:
   a) wszystkich odbiorcach danych, którym dane zostały lub zostaną ujawnione, zgodnie z art. 30 ust. 1 lit. d RODO;
   b) planowanych terminach usunięcia danych, zgodnie z art. 30 ust. 1 lit. f RODO.

Ponadto, za naruszenie przepisów art. 5 ust. 1 lit. a, e oraz lit. f, art. 5 ust. 2, art. 28, art. 30 ust. 1 lit. d oraz lit. f, a także art. 32 RODO, Prezes UODO nałożył na Burmistrza karę pieniężną w kwocie 40.000 zł.

Ponieważ, kwestionując decyzję Prezesa UODO, Burmistrz podniósł zarzut naruszenia przy jej wydaniu prawa materialnego, w tym art. 2 ust. 2 lit. a RODO, przez jego niewłaściwe zastosowanie w związku z art. 1 ust. 1 w związku z art. 168 u.o.d.o.[3], co doprowadziło do wydania zaskarżonej decyzji stwierdzającej naruszenie art. 5, WSA w Warszawie argumentację tę uznał za całkowicie nietrafną i wskazał, że wyłączenia, określone w art. 2 ust. 2 lit. a RODO, jako mające charakter wyjątkowy, nie mają zastosowania w analizowanej tu sprawie. Sąd odniósł się zatem do poszczególnych zarzutów dotyczących uchybień w procesie przetwarzania.

Każde z przywołanych ustaleń zasługuje na odnotowanie i refleksję, ponieważ dotyczy organizacji systemu ochrony danych osobowych w procesie współstosowania przepisów RODO z przepisami ustawy o dostępie do informacji publicznej[4], a nadto dotyka specyfiki stosowania RODO w sektorze publicznym, potwierdzając tezę, że nie w każdym przypadku procedury kształtowane w tym zakresie przez ten akt i przepisy krajowe są spójne.

Dostęp do informacji publicznej a zakres zastosowania przepisów RODO

U podstaw analizowanego wyroku WSA w Warszawie oraz poprzedzającej ten wyrok decyzji Prezesa UODO legło generalne założenie, wedle którego przepisy RODO mają zastosowanie w przypadku przetwarzania danych osobowych, jakie ma miejsce przy realizacji prawa dostępu do informacji publicznej. Tym samym, WSA w Warszawie nie

[3] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2019 r. poz. 1781; dalej: u.o.d.o.).

[4] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (tekst jedn.: Dz. U. z 2020 r., poz. 2176 ze zm.; dalej: u.d.i.p., ustawa o dostępie do informacji publicznej).

podzielił zapatrywania, że przetwarzanie danych osobowych na potrzeby dostępu do informacji publicznej nie jest objęte zakresem zastosowania przepisów RODO, co było podstawowym zarzutem wysuwanym przez stronę skarżącą, która oparcia dla tego zarzutu poszukiwała w treści art. 2 ust. 2 lit. a RODO, zgodnie z którym rozporządzenie to nie ma zastosowania do przetwarzania danych osobowych w ramach działalności nieobjętej zakresem prawa UE. Strona skarżąca starała się zatem wykazać, że zasady dostępu do informacji publicznej są przykładem działalności nieobjętej prawem Unii Europejskiej, co powoduje, że w tym zakresie przepisy RODO nie znajdują zastosowania. Tak postawiona teza odzwierciedla jedno z dwóch przeciwstawnych stanowisk, jakie rysują się w tym względzie w polskiej nauce prawa.

W literaturze wyraża się bowiem zarówno takie stanowisko, którego argumentacja przebiega zgodnie z zapatrywaniami wyrażanymi przez stronę skarżącą w analizowanej sprawie[5], jak i odmienne – przyjmowane przez sąd i organ nadzorczy w przedmiotowej sprawie, wedle którego RODO ma zastosowanie do przetwarzania danych osobowych, jakie odbywa się przy realizacji dostępu do informacji publicznej[6]. Dotyczy to przy tym zarówno ujawniania danych osobowych zawartych w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym – do czego wprost odnosi się art. 86 RODO, jak i przetwarzania danych osobowych, które w tym obszarze ma charakter akcesoryjny, a więc odbywa się w związku z obsługą procesów zapewniania dostępu do informacji publicznej w trybach i formach określonych w ustawie o dostępie do informacji publicznej[7].

Argumentując za zastosowaniem RODO do przetwarzania danych osobowych przy realizacji dostępu do informacji publicznej, WSA w Warszawie wskazał, że art. 2 RODO wyznacza materialny zakres jego stosowania, zaś wykładnia wyłączenia wynikającego z art. 2 ust. 2 lit. a tego aktu musi zostać dokonana z uwzględnieniem wykładni systemowej i celowościowej, co prowadzi do wniosku, że intencją prawodawcy unijnego nie było zawężenie stosowania ochrony danych osobowych, a wręcz przeciwnie – zwiększenie jej zakresu i stosowania, zaś sposób interpretacji przyjęty przez skarżącego spowodowałoby, że dane osobowe właściwie nie podlegałyby ochronie.

---

[5] Zob. P. Barta, P. Litwiński, *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021, s. 607–609; WSA w Olsztynie w wyroku z dnia 19 października 2018 r., II SA/Ol 542/18, CBOSA, wskazał, że przepisy RODO nie znajdują zastosowania do udostępniania danych osobowych w ramach dostępu do informacji publicznej, ale bez wskazania szerszego uzasadnienia tak postawionej tezy.

[6] Zob. G. Sibiga, I. Małobęcka-Szwast, *Relacje prawa do informacji publicznej oraz prawa do ochrony danych osobowych w świetle ogólnego rozporządzenia o ochronie danych (RODO)* [w:] *Polskie przepisy o ochronie danych osobowych. Aktualne problemy prawnej ochrony danych 2019*, red. G. Sibiga, M. Praw. 2019, nr 22 – dodatek, s. 61–66; M. Jabłoński, *Rola i znaczenie RODO w procesie definiowania gwarancji niezależności i spójności krajowego systemu ochrony danych osobowych* [w:] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017; M. Sakowska-Baryła, komentarz do art. 86 [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. *eadem*, Warszawa 2018, s. 611–612.

[7] Zob. M. Sakowska-Baryła, komentarz do art. 86 [w:] *Ogólne rozporządzenie*…, s. 612.

Sąd podniósł, że ustawodawca konkretyzuje wyłączenia stosowania przepisów w art. 6 RODO, a przeciwna wykładnia przepisów – w sposób przyjęty przez skarżącego – prowadziłaby do interpretacji *ad absurdum*, gdzie zastosowanie przepisów RODO ograniczone byłoby do bardzo wąskiego zakresu obowiązywania prawa Unii Europejskiej. Tymczasem – jak wskazuje WSA w Warszawie – wprowadzenie RODO miało na celu zwiększenie, a nie drastyczne ograniczenie ochrony danych osobowych. Jednocześnie argumentów na rzecz stosowania przepisów RODO do przetwarzania danych osobowych przy zapewnianiu dostępu do informacji publicznej, WSA poszukuje w treści art. 8 ust. 1 Karty praw podstawowych UE[8], zgodnie z którym każdy ma prawo do ochrony danych osobowych, które go dotyczą, oraz w art. 16 ust. 1 TFUE[9] stanowiącym, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących, jak również w przepisach Konstytucji RP[10], wskazując na zakładaną przez te akty „szeroką ochronę danych osobowych".

W ślad za wywodem organu nadzorczego, WSA w Warszawie przyjął, że norma wynikająca z art. 16 ust. 1 TFUE (oraz analogiczna z art. 8 Karty Praw Podstawowych UE), ma status normy bezpośrednio skutecznej, stając się autonomiczną podstawą uprawnień osób fizycznych w zakresie ochrony danych osobowych. Bezpośrednio skuteczna norma traktatowa chroni osoby fizyczne również w sytuacjach, kiedy nie będą one mogły korzystać z ochrony gwarantowanej przez akty prawa wtórnego. Treść art. 16 ust. 2 TFUE jednoznacznie wskazuje, że zasady ochrony danych osobowych określone w treści aktów prawa wtórnego będą miały zastosowanie w odniesieniu do danych osobowych osób fizycznych przetwarzanych przez instytucje, organy, jednostki organizacyjne Unii Europejskiej oraz państwa członkowskie, ale jedynie w zakresie, w jakim działania te będą służyć stosowaniu prawa Unii Europejskiej.

Choć tak wyrażone stanowisko zasadniczo zasługuje na aprobatę, to jednak sposób argumentacji przyjęty przez WSA może wzbudzać pewien niedosyt, ponieważ – przywołując przepisy UE oraz powołując się na względy słuszności – sąd ten wyczerpująco nie wyjaśnia, co przemawia za tym, by nie podzielić stanowiska strony skarżącej. Znacznie bardziej pogłębionych analiz w tym względzie dokonali Grzegorz Sibiga i Iga Małobęcka-Szwast, wychodząc od założenia, że udostępnianie danych osobowych w dokumentach urzędowych podlega przepisom RODO jako szczególna kategoria przetwarzania, o której mowa w jego rozdziale IX – Przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem, w art. 86, pomimo tego, że prawo unijne nie reguluje wprost dostępu do informacji publicznej w państwach członkowskich. Jednak w przypadku gdy ujawnieniu w ramach krajowych systemów dostępu do informacji publicznej podlegają dane osobowe, to RODO znajduje zastosowanie przez wzgląd

[8] Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 303 z 2007 r., s. 1 ze zm.).

[9] Traktat ustanawiający Europejską Wspólnotę Gospodarczą (Dz. U. z 2004 r. Nr 90, poz. 864/2 ze zm.) zmieniony przez art. G lit. A pkt 1 Traktatu o Unii Europejskiej (Dz.U.04.90.864/30) w związku z przystąpieniem Polski do Unii Europejskiej; zmieniony przez art. 2 pkt 1 Traktatu z Lizbony zmieniającego Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską (Dz.U.UE.C.07.306.1) z dniem 1 grudnia 2009 r.

[10] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.).

na kilka przesłanek uzasadniających zajęcie takiego właśnie stanowiska[11]. Autorzy ci słusznie wskazują, że w zakresie, w jakim w ramach dostępu do informacji publicznej dochodzi do ujawnienia danych osobowych, ma miejsce również przetwarzanie danych osobowych i ingerencja w prawo do ochrony danych osobowych, a co za tym idzie – ma się tu do czynienia z ingerencją w prawo podstawowe, gwarantowane każdemu w art. 16 TFUE oraz art. 8 KPP. Stąd w tym wąskim zakresie, w jakim dochodzi do ujawnienia danych osobowych, krajowy system dostępu do informacji publicznej odzwierciedlony w Polsce głównie w przepisach u.d.i.p. podlega prawu unijnemu, które chroni prawo podstawowe do ochrony danych osobowych, a gwarancje ochrony tego prawa uszczegóławia RODO. Taka konkluzja pozostaje uzasadniona ze względu na brzmienie art. 86 i wskazany wyżej tytuł rozdziału IX RODO, w którym ów przepis się znajduje. W ten sposób prawo oddziałuje zatem na tę część krajowego systemu dostępu do informacji publicznej, w której dochodzi do ujawnienia danych osobowych, a więc kolizji między ochroną danych osobowych a dostępem do informacji publicznej i RODO i znajduje zastosowanie w tego rodzaju sprawach właśnie z tego względu, że w ramach dostępu do informacji publicznej może dochodzić do ingerencji w prawo do ochrony danych osobowych[12]. Tezę o zastosowaniu RODO do ujawniania danych osobowych zawartych w „dokumentach urzędowych" potwierdzają również te przepisy RODO, które odwołują się wprost do rozdziału IX. Ma to miejsce w treści art. 6 ust. 2 i 3, a także w art. 83 ust. 5 lit. d RODO, przez co prawodawca unijny wprost ustanawia wymagania względem podstaw prawnych przetwarzania danych osobowych w sytuacjach związanych z przetwarzaniem, takich jak udostępnianie danych osobowych w dokumentach urzędowych, o którym mowa w art. 86 RODO. Nadto, na tle analizowanego wyroku istotna jest właśnie regulacja zawarta w art. 83 ust. 5 lit. d RODO, który przewiduje możliwość nałożenia przez organ nadzorczy administracyjnej kary pieniężnej w przypadku naruszenia wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego na podstawie rozdziału IX, w tym art. 86 RODO. Stąd naruszenie obowiązków wynikających z prawa krajowego, przyjętych na podstawie art. 86 RODO, może pociągnąć za sobą odpowiedzialność w postaci nałożenia na administratora przez organ nadzorczy administracyjnej kary pieniężnej[13].

Argumentów na rzecz dopuszczalności stosowania RODO do przetwarzania danych osobowych przy dostępie do informacji publicznej doszukiwać się można także w bliskim powiązaniu systemu dostępu i ponownego wykorzystywania informacji sektora publicznego, które z założenia jest oparte właśnie na systemie dostępu do informacji publicznej. Choć prawo unijne nie zawiera kompleksowej regulacji dotyczącej dostępu do informacji publicznej, to poprzednio w dyrektywie 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego[14], zaś obecnie w dyrektywie Parlamentu Euro-

[11] Zob. G. Sibiga, I. Małobęcka-Szwast, *Relacje*…, s. 63.
[12] *Ibidem*, s. 64.
[13] *Ibidem*.
[14] Dz. Urz. UE L 345, s. 90 ze zm.

pejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (wersja przekształcona)[15] dookreśla się zasady takiego dostępu w sprawie ponownego wykorzystywania informacji sektora publicznego.

Zarówno w RODO, jak i w powyższych dyrektywach wskazuje się, że dostęp do informacji publicznej i ponowne wykorzystanie informacji sektora publicznego tworzą razem nierozerwalną całość, a ponowne wykorzystanie informacji sektora publicznego nie mogłoby istnieć bez krajowych systemów dostępu do dokumentów urzędowych. W RODO zatem oba te reżimy względem prawa do ochrony danych osobowych potraktowane są łącznie, co powoduje, że przepisy regulujące publiczny dostęp do dokumentów urzędowych oraz ponowne wykorzystanie informacji sektora publicznego mają przewidywać niezbędne uwzględnienie prawa do ochrony danych osobowych na podstawie RODO, co – siłą rzeczy – odbywa się poprzez uwzględnianie zasad wynikających z tego rozporządzenia przy wykonywaniu obu tych praw dostępowych. Powyższe argumenty można zestawić również z orzecznictwem TSUE dotyczącym zakresu zastosowania Karty Praw Podstawowych, z którego wynika m.in., że choć dana działalność nie wiąże się z wykonywaniem i nie narusza norm prawa UE, może ona mieścić się „w zakresie prawa UE", ponieważ istnieje wystarczający związek („łącznik") między aktem prawa krajowego a aktem prawa unijnego[16].

Przywołana argumentacja zdaje się potwierdzać słuszność przyjęcia przez WSA w Warszawie, że w analizowanej sprawie nie zachodzi wyłączenie stosowania RODO, o jakim mowa w art. 2 ust. 2 lit. a RODO, choć jednocześnie – dla uzupełnienia tychże ustaleń – wskazać należy, że wypełniając zapowiedź z art. 86 RODO, państwa członkowskie powinny stworzyć szczególne regulacje w zakresie dostępu i ujawniania dokumentów urzędowych, spełniające wytyczne zawarte w art. 6 ust. 2 i 3 RODO, a wcześniejsze normy regulujące dostęp do dokumentów urzędowych i ich ujawnianie mogą nadal obowiązywać, pod warunkiem że wypełniają wymogi określone w tychże przepisach[17]. Biorąc pod uwagę treść art. 5 ust. 2 u.d.i.p., w którym mowa wyłącznie o prywatności osoby fizycznej jako przesłance ograniczenia dostępu do informacji publicznej oraz fakt, że w rzeczonej ustawie w ogóle nie posłużono się taką kategorią pojęciową, jak „dane osobowe", można mieć wątpliwości co do tego, czy u.d.i.p. w obecnym kształcie odpowiada wymogom wynikającym z RODO. Taki stan rzeczy powoduje, że w dalszym ciągu aktualne są postulaty wprowadzenia do tej ustawy przepisów mających na celu dostosowanie określonych w niej mechanizmów ochrony sfery informacyjnej jednostki do wymogów RODO. W orzecznictwie sądów administracyjnych relacje prawa do informacji oraz prawa do ochrony danych osobowych w dalszym ciągu ustala się zatem w oparciu o jego powiązania z prawem do prywatności[18]. Z pewnością nie

[15] Dz. Urz. UE L 172, s. 56.

[16] *Ibidem*, s. 65–66 i przywołane tam orzecznictwo.

[17] Zob. N. Zawadzka, komentarz do art. 86, uw. 5 [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

[18] Zob. G. Sibiga, *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych osobowych – wybrane zagadnienia*

jest to rozwiązanie zadowalające choćby z tego względu, że prawo do ochrony danych osobowych oraz prawo do prywatności stanowią osobne prawa podstawowe, mające podobny, ale nie ten sam przedmiot ochrony, a nadto ochrona danych osobowych rozciąga się nie tylko na dane osobowe ze sfery prywatności, ale obejmuje także te, które nie należą do tej sfery[19]. W tym stanie rzeczy znacznie bardziej adekwatna wydaje się konstrukcja współstosowania RODO oraz u.d.i.p. jako aktów zabezpieczających wykonywanie dwóch informacyjnych uprawnień jednostki, które niekiedy pozostają ze sobą w konflikcie[20], ale zasadniczo wymagają jednoczesnego wykonywania w aspekcie proceduralnym, na co wskazują zarówno analizowane ustalenia decyzji Prezesa UODO, jak i potwierdzające je argumenty wysuwane w uzasadnieniu glosowanego wyroku WSA w Warszawie.

Współstosowanie przepisów RODO i u.d.i.p.

Choć w analizowanym wyroku WSA w Warszawie sąd nie posługuje się tym pojęciem, jego ustalenia w sprawie w istocie stanowią odzwierciedlenie tezy, że także w bieżącym stanie prawnym przepisy o ochronie danych osobowych oraz o dostępie do informacji publicznej są współstosowane[21]. Stanowisko to ma rację bytu właśnie w warunkach sprawy analizowanej przez WSA w Warszawie oraz decyzji Prezesa UODO, wydanej w związku z niezgodnym z RODO przetwarzaniem danych osobowych przez Burmistrza, która to niezgodność dotykała zarówno sfery dopuszczalności przetwarzania – jego niezbędności i zgodności z prawem dokonywanych operacji przetwarzania danych, jak i obszaru rozwiązań techniczno-organizacyjnych.

Wyrok WSA w Warszawie, a wcześniej poprzedzająca go decyzja Prezesa UODO, odnosi się do zagadnienia współstosowania RODO oraz u.d.i.p. jako aktów, które regulują procedury dysponowania informacjami charakteryzowanymi jako dane osobowe oraz informacje publiczne w pewnym wspólnym obszarze oddziaływania, i których przepisy zasadniczo mają być realizowane równocześnie, urzeczywistniając odpowiednio prawo do ochrony danych osobowych oraz prawo dostępu do informacji publicznej. Trzeba mieć na względzie, że RODO i u.d.i.p. regulują odmienną materię, poprzez wskazanie procedur postępowania z informacjami innego rodzaju, w innych celach oraz dla

---

[w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*, red. *idem*, „Biblioteka Monitora Prawniczego" 2016, s. 20; wyrok WSA w Warszawie z dnia 29 września 2020 r., II SAB/Wa 225/20, LEX nr 3077523; wyrok WSA w Szczecinie z dnia 15 października 2020 r., II SA/Sz 624/20, LEX nr 3088437.

[19] Zob. M. Czerniawski, *Ochrona danych osobowych w prawie międzynarodowym* [w:] *Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2020, s. 21; M. Wilbrandt-Gotowicz, *Prywatność osoby fizycznej jako ograniczenie jawności informacji publicznych (w świetle orzecznictwa sądów administracyjnych)* [w:] *Jawność i jej ograniczenia. Znaczenie orzecznictwa*, red. G. Szpor, t. 4, red. M. Jaśkowska, Warszawa 2014, s. 165.

[20] Zob. P. Fajgielski, komentarz do art. 86 [w:] *idem*, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, LEX/el.

[21] M. Sakowska-Baryła, komentarz do art. 86 [w:] *Ogólne rozporządzenie*…, s. 612.

realizacji zasadniczo odmiennych interesów – indywidualnego jednostki oraz interesu publicznego, do którego zresztą RODO odnosi się wprost w motywie 154, wskazując, że publiczny dostęp do dokumentów urzędowych można uznać za interes publiczny.

Unormowania te mają pewien wspólny obszar, który rysuje się wyraźniej, gdy ujawnieniu podlegać mają dane osobowe, ale obejmuje także sferę organizacji i zabezpieczeń we wszystkich przypadkach, gdy przy zapewnianiu dostępu do informacji publicznej w rachubę wchodzi przetwarzanie danych osobowych. Sfera rozwiązań organizacyjnych i technicznych na sam zakres ujawnianych w ramach dostępu do informacji publicznej może mieć pośredni wpływ, czego dobrym przykładem jest odpowiednie udokumentowanie powierzenia przetwarzania w związku z prowadzeniem BIP w infrastrukturze informatycznej zewnętrznego podmiotu, co miało miejsce w analizowanej sprawie. Może być i tak, że przetwarzanie odbywa się nie tyle w ramach ujawniania danych osobowych zawartych w informacji publicznej, ale ma miejsce akcesoryjnie, jak dzieje się chociażby z danymi osobowymi osób wnioskujących o udostępnienie informacji publicznej. Wszakże i ich prawo do ochrony danych osobowych musi być respektowane.

Współstosowanie przepisów RODO i u.d.i.p. oznacza stan, w którym jednocześnie podmioty zobowiązane na gruncie u.d.i.p. powinny realizować przewidziane w tej ustawie uprawnienia dostępowe, przestrzegając jednocześnie zasad ochrony danych uregulowanych w RODO poprzez ocenę dopuszczalności przetwarzania danych oraz wprowadzenie odpowiednich zabezpieczeń, powołanie inspektora ochrony danych, prowadzenie adekwatnej dokumentacji pozwalającej wykazać zgodność działania z RODO, wykonywanie praw osób, których dane dotyczą, prowadzenie rejestru czynności przetwarzania, wdrażanie polityk z zakresu ochrony danych osobowych itp.

Stosowanie procedur ochrony danych osobowych pod rządami RODO w związku z zapewnianiem dostępu do informacji publicznej, podobnie jak w poprzednim stanie prawnym, dotyczy zatem dwóch obszarów – pierwszy to obszar ustaleń dotyczących dopuszczalności ujawniania danych osobowych wchodzących w skład informacji publicznej; drugi to obszar procedur technicznio-organizacyjnych, który można określić „administrowaniem”[22]. Analizowany wyrok WSA w Warszawie oraz poprzedzająca go decyzja Prezesa UODO dobrze obrazują założenie, że organy i podmioty zobowiązane na gruncie u.d.i.p. oraz sądy orzekające w sprawach przetwarzania danych osobowych przy wykonywaniu praw dostępowych muszą brać pod uwagę m.in. zasady rozliczalności wynikające z art. 5 ust. 1 RODO, w tym m.in. zasadę minimalizacji danych, zgodnie z którą dane osobowe mają być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane czy też zasadę ograniczenia czasowego przetwarzania, co siłą rzeczy ma istotny wpływ na zakres udostępnianych danych osobowych, w tym danych o osobach pełniących funkcje publiczne, co dobrze

[22] Zob. M. Sakowska-Baryła, *Dostęp do informacji publicznej a ochrona danych osobowych*, Wrocław 2014, s. 76 i n.; *eadem*, *Problem współstosowania ustawy o dostępie do informacji publicznej i ustawy o ochronie danych osobowych* [w:] *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, red. A. Mednis, Warszawa 2016, s. 173 i n.

zobrazowane zostało w ustaleniach dokonanych przez sąd i organ nadzorczy w analizowane sprawie[23].

Zakres stwierdzonych przez Prezesa UODO uchybień w procesie przetwarzania danych osobowych przez Burmistrza, pozwala na wskazanie pewnych obszarów stosowania procedur ochrony danych osobowych przy realizacji dostępu do informacji publicznej, gdzie właśnie można mówić o współstosowaniu przepisów RODO i u.d.i.p.

Stosowanie zasad rozliczalności przetwarzania danych osobowych

Wyrok wydany w sprawie II SA/Wa 2826/19 przez WSA w Warszawie potwierdza argumentację Prezesa UODO w zakresie zastosowania przy realizacji dostępu do informacji publicznej określonych w art. 5 RODO zasad dotyczących przetwarzania danych osobowych nazywanych zwykle „zasadami rozliczalności przetwarzania". W ten sposób WSA w Warszawie wyraził aprobatę dla szerokiego zastosowania procedur ochrony danych osobowych do procesów udostępniania informacji publicznej, nie ograniczając go tylko do samego aktu ujawniania danych osobowych zawartych w dokumentach urzędowych, które posiada organ lub podmiot publiczny, lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym. Zasady rozliczalności przetwarzania danych osobowych są bowiem sformułowane w sposób na tyle szeroki i uniwersalny, że oddziałują nie tylko na obszar ustaleń co do dopuszczalności przetwarzania danych osobowych – w tym konkretnym przypadku ich udostępnienia w ramach informacji publicznej, ale również na ten obszar, który odnosi się do kwestii organizacyjnych, dokumentacyjnych, technicznych zabezpieczeń, wprowadzanych procedur. Warto zatem wspomnieć, że zgodnie z art. 5 ust. 1 RODO dane osobowe muszą być:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu");
3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one

[23] M. Sakowska-Baryła, komentarz do art. 86 [w:] *Ogólne rozporządzenie*…, s. 612.

przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");

6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

Jak natomiast stanowi art. 5 ust. 2 RODO, administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

Ustalenia dokonane przez WSA w Warszawie, a wcześniej przez Prezesa UODO, pozwalają wyrazić pogląd, że zarówno ten sąd, jak i organ nadzorczy stoją na stanowisku, że RODO oddziałuje i na tę część krajowego systemu dostępu do informacji publicznej, w której dochodzi do ujawnienia danych osobowych, i na ten obszar, w którym procedury ochrony danych osobowych mają za zadanie określić sposób powinnego zachowania podmiotu zobowiązanego w obszarze niejako administracyjnym, gdzie należy:

- dokonać odpowiednich czynności mających na celu zabezpieczenie danych osobowych i systemów informatycznych, służących ich przetwarzaniu;
- dokonać oceny ryzyka naruszeń praw lub wolności osób fizycznych, sporządzić polityki;
- uzupełnić rejestry czynności przetwarzania;
- zawrzeć umowy powierzenia przetwarzania danych osobowych;
- dokonać inwentaryzacji zasobów;
- zawrzeć umowy dotyczące zapewnienia infrastruktury informatycznej wykorzystywanej strony internetowej w postaci Biuletynu Informacji Publicznej;
- faktycznie zaprzestać przetwarzania danych, które staje się nieuzasadnione w związku z upływem czasu.

Owe administracyjne czynności administratora tylko pośrednio wpływają na treść, postać i zakres danych osobowych ujawnianych w ramach dostępu do informacji publicznej, do czego wprost odnosi się art. 86 RODO, stanowiąc, że dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny, w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem UE lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy tego rozporządzenia.

Jednakże, biorąc pod uwagę zakres regulacji RODO oraz przewidzianych w nim procedur przetwarzania danych osobowych, można uznać, że ów obszar godzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych, dookreślonym w RODO nie tylko w aspekcie dopuszczalności przetwarzania,

ale i środków bezpieczeństwa o charakterze technicznym i organizacyjnym odpowiadającym charakterowi, zakresowi, kontekstowi i celom przetwarzania oraz ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, powinien rozciągać się także na te ostatnie – „wykonawcze" („administracyjne") uwarunkowania. Ochrona danych osobowych bowiem to zespół procedur postępowania z danymi osobowymi pozwalających ustalić, kiedy i na jakich warunkach korzystanie z nich jest legalne, oraz jakie prawa przysługują osobie fizycznej, w związku z przetwarzaniem jej danych osobowych. To procedury, które w praktyce chronią obydwie strony stosunku informacyjnego – i osobę, której dane dotyczą, i podmiot, który je przetwarza poprzez wyznaczenie wyraźnych reguł jego działania, a także poprzez wprowadzenie gwarancji o charakterze instytucjonalnym na czele z niezależnym organem nadzorczym wyposażonym w odpowiednie w tym względzie kompetencje. Ujęcie to odpowiada przybliżonej wcześniej konstrukcji współstosowania przepisów o ochronie danych osobowych oraz o dostępie do informacji publicznej, gdzie dostęp do informacji ma być realizowany przy jednoczesnym uwzględnieniu zasad ochrony danych, w tym wskazanych w art. 5 RODO, z którymi korespondują inne przepisy RODO i wynikające z nich obowiązki, czego wyraz odnaleźć można w sposobie formułowania zarzutów przez organ nadzorczy, który wskazując na naruszenia przepisów RODO, zwykle w pierwszej kolejności przytacza stosowną jednostkę redakcyjną art. 5 RODO, łącząc jej regulację z bardziej szczegółowym („merytorycznym") przepisem tego aktu.

Zgodzić się jednocześnie należy z WSA w Warszawie, że zasady wskazane w art. 5 RODO mają charakter samoistny i są wiążącymi normami prawnymi, określającymi konkretne normy postępowania w przedmiotowym zakresie. Mogą pełnić rolę subsydiarną w stosunku do innych przepisów, zwłaszcza przy ich interpretacji i stosowaniu norm prawnych dotyczących ochrony danych osobowych, jednak równie istotna jest ich funkcja jako norm nadrzędnych nad innymi przepisami. Prawodawca podkreśla ich szczególne znaczenie, określając je mianem „zasad"[24], przy czym tak administrator, jak i organ nadzorczy są zobowiązani do przestrzegania zawartych w tym przepisie zasad, a wszelkie wyłączenia mają charakter absolutnie wyjątkowy. Sąd słusznie podkreśla przy tym, że przy stosowaniu art. 5 ust. 1 RODO administrator ma znaczną swobodę w zakresie stosowanych rozwiązań, ale jednocześnie jednak ponosi odpowiedzialność za naruszenie przepisów o ochronie danych osobowych i – jak wynika z art. 5 ust. 2 RODO – to administrator danych powinien wykazać, a zatem udowodnić, że

[24] Na temat „zasady prawa" szerzej zob. R. Dworkin, *The model of rules*, „The University of Chicago Law Review" 1967, no. 1, s. 14 i n; R. Alexy, *A Theory o f Constitutional Rights*, przekł. J. Rivers, Oxford 2002; *idem*, *On the structure of legal principles*, „Ratio Juris" 2000, nr 3, s. 290 i n.; M. Kordela, *Możliwość konstruowania ogólnej teorii zasad prawa. Uwagi do koncepcji Roberta Alexy'ego*, RPEiS 2007, z. 2, s. 11 i n.; G. Maroń, *Formuła ważenia zasad prawa jako mechanizm usuwania ich kolizji na przykładzie koncepcji Roberta Alexy'ego*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego" 2009, nr 7, s. 86 i n.; E.G. Nalbandian, *Notes on Roland Dworkin's theory of law*, „Mizan Law Review" 2009, vol. 3, no. 2, s 370 i n., file:///C:/Users/msako/AppData/Local/Temp/145475-Article%20Text-384713-1-10-20161008.pdf [dostęp: 22.06.2021]; L. Leszczyński, G. Maroń, *Zasady prawa. Ujęcie dogmatyczno-porównawcze*, „Studia Iuridica Lublinensia" 2016, vol. 25, s. 317 i n.

przestrzega przepisów określonych w art. 5 ust. 1 RODO, czego w analizowanej sprawie nie dokonał Burmistrz Aleksandrowa Kujawskiego.

Analizowany wyrok WSA w Warszawie oraz poprzedzająca go decyzja Prezesa UODO potwierdzają zatem tezę, że zastosowanie RODO przy realizacji prawa dostępu do informacji publicznej odnosi się nie tylko do swoistego jądra tej relacji, gdzie dostęp do informacji publicznej krzyżuje się z prawem do ochrony danych osobowych, ale również do uwarunkowań proceduralnych, które określone zostały w RODO i które pozostają współstosowane z tymi przepisami u.d.i.p., które określają tryby i formy realizacji dostępu do informacji publicznej.

Powierzenie przetwarzania danych osobowych w związku z prowadzeniem BIP

W analizowanym wyroku, WSA w Warszawie podzielił zapatrywanie Prezesa UODO, że naruszeniem art. 5 ust. 1 lit. a oraz lit. f w zw. z art. 5 ust. 2 RODO jest udostępnianie danych osobowych zewnętrznym podmiotom w związku z prowadzeniem strony internetowej BIP Urzędu Miejskiego w Aleksandrowie Kujawskim bez uprzedniego zawarcia z tymi podmiotami umów powierzenia danych osobowych, w rozumieniu art. 28 ust. 3 RODO, kwalifikując to udostępnienie jako dokonane bez podstawy prawnej. Ze stanowiskiem tym należy się zgodzić, co więcej – korzystanie z zewnętrznego podmiotu dostarczającego rozwiązań technicznych do prowadzenia BIP jest jednym z bardziej powszechnych przykładów powierzenia przetwarzania danych osobowych w sektorze publicznym[25].

Powierzenie przetwarzania danych osobowych to stan faktyczny, jaki istnieje w konkretnych okolicznościach relacji pomiędzy administratorem a podmiotem przetwarzającym, czy też niekiedy pomiotami przetwarzającymi, jak ma to miejsce w analizowanej sytuacji, z którym to stanem faktycznym RODO wiąże określone obowiązki prawne każdego z podmiotów pozostających w tej relacji. Istotą powierzenia przetwarzania danych osobowych jest zlecenie na zewnątrz czynności przetwarzania danych osobowych – usługi wymagającej przetwarzania danych, w ramach której, przetwarzanie to jest elementem podstawowym lub co najmniej niezbędnym[26]. Tak jest właśnie w przypadku przetwarzania danych osobowych w ramach BIP, przy czym nie ma znaczenia, że informacje udostępniane w tym urzędowym publikatorze z zasady są jawne i powszechnie dostępne. Pamiętać trzeba bowiem, że zasady ochrony danych

[25] Zob. M. Sakowska-Baryła, *Powierzenie przetwarzania danych osobowych w sektorze publicznym* [w:] *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, red. M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda, Wrocław 2017, s. 13.

[26] Zob. M. Sakowska-Baryła, *Powierzenie przetwarzania w administracji publicznej* [w:] M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*, Wrocław 2018, s.108–110.

osobowych odnoszą się do każdej kategorii danych osobowych – także tych, które z założenia mają być powszechnie dostępne i z którymi łatwo się zapoznać.

Biorąc pod uwagę treść art. 28 RODO, nie sposób zatem kwestionować, że w przypadku powierzenia zewnętrznemu podmiotowi lub podmiotom prowadzenia BIP przez Burmistrza, to on właśnie jako administrator powinien zadbać o to, aby to powierzenie spełniało wymogi wynikające z przepisów prawa. Chodzi tu przede wszystkim o zawarcie pisemnej umowy powierzenia przetwarzania danych osobowych (art. 28 ust. 9 RODO), o treści odpowiadającej wymaganiom określonym w art. 28 ust. 3 RODO, a także o to, aby być w stanie wykazać dokonanie weryfikacji podmiotu przetwarzającego, co zakłada się w art. 28 ust. 1 RODO.

Choć powyższe ustalenia należy uznać za oczywiste, to jednak warte uwagi są okoliczności, w jakich do rzeczonego powierzenia prowadzenia BIP na zewnątrz doszło w analizowanej sprawie. W uzasadnieniu decyzji Prezesa UODO wskazuje się bowiem, że w trakcie kontroli ustalono, że ów BIP Urzędu Miejskiego w Aleksandrowie Kujawskim był prowadzony w formule dość często spotykanej w praktyce, gdzie dostarczanie takiej usługi zapewniane jest przez zewnętrzny podmiot, w ramach realizacji pewnego szerszego zamysłu organizacyjnego i finansowego, gdzie faktycznie bywa, iż umowa dotycząca realizacji tej usługi zawierana jest przez podmiot, który finansuje przedsięwzięcie, zaś poszczególni – pomniejsi – administratorzy wielokrotnie nie zawierają ani umów dotyczących ogólnie świadczenia usług, ani powierzenia przetwarzania. Jak czytamy w decyzji Prezesa UODO, w toku jego kontroli ustalono, że w związku z dostarczeniem oprogramowania dotyczącego utworzenia regionalnego biuletynu informacji publicznej, zawarta została umowa pomiędzy Województwem Kujawsko-Pomorskim a konsorcjum podmiotów, w której nie zostały ujęte postanowienia dotyczące ochrony danych osobowych ani nie została zawarta umowa o powierzeniu przetwarzania danych osobowych związana ze świadczeniem usług serwisowych na rzecz Urzędu Miejskiego w Aleksandrowie Kujawskim. Siłą rzeczy zatem w toku kontroli nie przedstawiono umowy pomiędzy Województwem Kujawsko-Pomorskim a Burmistrzem Miasta Aleksandrowa Kujawskiego, ani nie wykazano innego instrumentu prawnego, z którego wynikałoby, że udostępnienie serwera oraz dostarczenie oprogramowania służącego do utworzenia regionalnego biuletynu informacji publicznej realizowane jest przez Województwo Kujawsko-Pomorskie na rzecz Urzędu Miejskiego w Aleksandrowie Kujawskim. Szersze analizy tak zarysowanego stanu faktycznego znacząco wychodziłyby poza zakres prowadzonych tu rozważań, niemniej problem braku umów powierzenia w sytuacjach, gdy mamy do czynienia z relacją na swój sposób kaskadową – kiedy kto inny przedsięwzięcie finansuje, a kto inny z niego korzysta, bądź też gdy np. województwo, gmina, czy powiat nabywają usługę dla jednostek organizacyjnych powiązanych ze sobą na różne sposoby (wspólnym budżetem, relacjami organizacyjnymi, uczestnictwem we wspólnym projekcie unijnym), w praktyce okazuje się kwestią nieincydentalną. W tym stanie rzeczy konieczne wydaje się zalecać staranne przygotowanie takich przedsięwzięć, także w obszarze ochrony danych osobowych oraz umowne potwierdzenie relacji w odniesieniu do wszystkich pozostających w niej administratorów.

Naruszenie zasady ograniczenia czasowego przetwarzania danych osobowych

W analizowanym wyroku, WSA w Warszawie z aprobatą odniósł się do ustaleń Prezesa UODO, co do naruszenia przez Burmistrza art. 5 ust. 1 lit. e w zw. z art. 5 ust. 2, tj. zasady ograniczenia przechowywania, oraz art. 24 RODO poprzez brak odpowiednich polityk dotyczących przetwarzania danych osobowych w BIP Urzędu Miejskiego w Aleksandrowie Kujawskim pod kątem ich aktualności i celowości publikacji oraz określających terminy usunięcia danych osobowych. W wyniku oględzin strony BIP Urzędu Miejskiego w Aleksandrowie Kujawskim ustalono bowiem, że wśród zamieszczonych tam informacji pozostawały dokumenty zawierające dane osobowe, tj. oświadczenia majątkowe oraz informacje o wynikach naborów na wolne stanowiska, gdzie najstarsze informacje dotyczyły naborów przeprowadzonych w 2012 r. i zawierały informacje o wybranych kandydatach w zakresie: imię i nazwisko oraz miejsce zamieszkania w rozumieniu przepisów kodeksu cywilnego[27], zaś najstarsze zamieszczone na archiwalnej stronie BIP tego urzędu oświadczenia majątkowe dotyczyły 2010 r., co spowodowało stwierdzenie przez organ nadzorczy naruszenie przepisów RODO.

Powyższe zagadnienie wydaje się szczególnie kontrowersyjne z tej racji, że w przepisach u.d.i.p., ani też w innych przepisach przewidujących umieszczanie informacji w BIP zwykle nie wskazuje się, po jakim czasie informacje te mają być z tego publikatora usunięte. Zgodnie z argumentacją Prezesa UODO, podzielaną przez WSA w Warszawie, ów brak określonych przepisami prawa okresów przetwarzania udostępnionych informacji (zawierających dane osobowe) nie powoduje jednak, że informacje takie można przetwarzać bezterminowo. Wobec powyższego, administrator, zgodnie z zasadą ograniczonego przechowywania (art. 5 ust. 1 lit. e RODO), powinien w tym zakresie kierować się przepisami z innych aktów prawa, z których wynika czas, przez jaki może przetwarzać dane osobowe, a w przypadkach, w których prawo nie reguluje okresu retencji danych, po przeprowadzeniu analiz powinien określić ten okres tak, aby przetwarzanie danych było zgodne z celami, dla których realizacji je pozyskano.

Nie jest to zresztą jedyny wyrok odnoszący się do tego zagadnienia. Zasada ograniczenia czasowego wynikająca z art. 5 ust. 1 lit. e RODO była przedmiotem analiz WSA w Warszawie w sprawie II SA/Wa 1810/19, która dotyczyła kwestii nadmiernego czasowo udostępniania w BIP danych osobowych osoby, która ubiegała się o stanowisko sędziego. Dokonując oceny stanu faktycznego, WSA argumentował, że cel, jakim było udostępnienie informacji o wynikach konkursu na stanowisko sędziego, został już osiągnięty z uwagi na upływ prawie siedmiu lat od przyjęcia opublikowanej w BIP uchwały[28].

Należy podzielić zdanie WSA w Warszawie wyrażone w obydwu sprawach, że cel przetwarzania nie może funkcjonować i być oceniany w oderwaniu od okoliczności przetwarzania, a ustalając ten cel, należy odwołać się do okoliczności konkretnej

[27] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tekst jedn.: Dz. U. z 2020 r., poz. 1740 ze zm.).
[28] Zob. wyrok WSA w Warszawie z dnia 29 stycznia 2020 r., II SA/Wa 1810/19, LEX nr 3041123.

sprawy, aby właściwie określić upływ spodziewanego terminu użyteczności danych. Tyle tylko, że kwestia przynajmniej przybliżonego określenia terminu usunięcia danych z BIP oraz wyraźne wskazanie, że tego typu usunięcie w ogóle jest możliwe, powinna być przesądzona wprost w przepisach prawa. Zważyć bowiem należy, że określanie celu przetwarzania danych osobowych przez administratora także w kontekście realizacji dostępu do informacji publicznej może następować inaczej w zależności od tego, jakie przesłanki w tej mierze będą brane pod uwagę przez administratora. Tymczasem, zważywszy na to, że dostęp ten jest realizowany przez kategorie podmiotów zobowiązanych, określonych w art. 4 u.d.i.p., które z założenia są do siebie podobne i realizują podobne cele, czas przetwarzania przez nie danych osobowych także powinien być podobny, a przy samodzielnie dokonywanych ustaleniach nie jest. Co więcej, obawa przed administracyjną karą pieniężną w związku ze zbyt długim przetwarzaniem danych w BIP może prowadzić z kolei do zdewaluowania założenia wynikającego z u.d.i.p., że to właśnie bezwnioskowe udostępnianie informacji w BIP jest podstawową formą zapewniania dostępu do informacji publicznej. W literaturze wskazuje się nawet na zasadę pierwszeństwa bezwnioskowego uzyskiwania informacji publicznej[29].

Wojewódzki Sąd Administracyjny w Warszawie w analizowanym tu wyroku potwierdził zatem słuszność sformułowanego przez Prezesa UODO zarzutu naruszenia art. 24 RODO poprzez brak odpowiednich polityk dotyczących przetwarzania danych osobowych w BIP Urzędu Miejskiego w Aleksandrowie Kujawskim pod kątem ich aktualności i celowości publikacji oraz określających terminy usunięcia danych osobowych, a w konsekwencji także słuszność nakazania przez Prezesa UODO dostosowania operacji przetwarzania danych osobowych do RODO, poprzez wdrożenie polityk określających okresy przetwarzania danych w BIP zgodne z przepisami prawa lub niezbędne do realizacji celów, w których dane są przetwarzane, zapewniających przestrzeganie terminów usuwania danych.

Na tle tychże ustaleń uzasadnione wydaje się poczynienie także pewnej krytycznej uwagi odnoszącej się do dokumentacyjnego aspektu przestrzegania zasad ochrony danych osobowych w sektorze publicznym. Odnotować trzeba bowiem, że w analizowanej sprawie doszło do sformułowania wobec Burmistrza zarzutu braku rzeczonej polityki, co poczytane zostało jako naruszenie RODO, a w konsekwencji wpłynęło na sformułowanie nakazu wdrożenia takiego dokumentu. Problem jednak w tym, że z żadnego z przepisów RODO nie sposób wyprowadzić wniosku, że posiadanie nominalnie takiej właśnie polityki jest obowiązkiem administratora. W zastrzeżeniu tym nie chodzi o to, aby kwestionować przyjęty w RODO otwarty sposób sformułowania wymogów w zakresie wprowadzanych rozwiązań technicznych i organizacyjnych, ponieważ ma on swoje istotne walory. Niemniej jednak brak bliższego skategoryzowania obowiązków technicznych i organizacyjnych w przypadku administratorów z sektora publicznego prowadzi do tego, że niemożliwe jest ustalenie katalogu obowiązków z zakresu ochrony danych osobowych, ciążących na administratorze, co jednak powinno być

[29] Zob. M. Bernaczyk, *Obowiązek bezwnioskowego udostępniania informacji publicznej*, Warszawa 2008, s. 150–156.

standardem w przypadku administratorów z sektora publicznego. Jeśli bowiem do kategorii administratorów zalicza się organy władzy publicznej i podmioty publiczne, to podstawową zasadą ich funkcjonowania jest działanie na podstawie i w granicach prawa. Tym samym, powinno być dla nich przewidywalne, jakie konkretnie obowiązki na nich ciążą, jakich dokładnie procedur mają przestrzegać i jakie polityki mają stworzyć. Tymczasem zakres koniecznych rozwiązań w postaci środków technicznych i organizacyjnych składających się na system ochrony danych osobowych, w RODO określa się w sposób otwarty, a o tym, czego na podstawie RODO można wymagać od będących administratorami organów lub podmiotów publicznych, wielokrotnie dowiedzieć się można dopiero z treści uzasadnień decyzji organu nadzorczego, bądź też jego stanowisk publikowanych na stronie internetowej. To źródła wiedzy przydatne w praktyce, ale niemające cech prawa powszechnie obowiązującego. W tym stanie rzeczy nie można poczynić wyczerpujących ustaleń, czy organ władzy publicznej lub inny podmiot publiczny zrealizował ciążące na nim obowiązki. W analizowanej sprawie Prezes UODO stwierdził m.in. brak u Burmistrza – publicznego administratora – „procedur wewnętrznych dotyczących przeglądu zasobów opublikowanych w BIP pod kątem zapewnienia przetwarzania danych, zgodnie z zasadą ograniczonego przechowywania, w wyniku czego na stronie BIP Urzędu Miejskiego w Aleksandrowie Kujawskim publikowane są dokumenty zawierające dane osobowe przez okres dłuższy niż wynika to z przepisów prawa", a z brakiem tym powiązał zastosowanie środków naprawczych z art. 58 ust. 2 RODO. Trzeba jednak wskazać, że przepisy RODO oraz przepisy prawa krajowego nie przewidują wprost posiadania tego rodzaju procedury przez wójta, burmistrza czy prezydenta miasta. Zarzut naruszenia przepisów RODO w tym względzie i okoliczność wydania ostatecznej decyzji administracyjnej wskazującej na naruszenia prawa i nakładającej administracyjną karę pieniężną siłą rzeczy przekładają się ustalenia dotyczące wypełnienia swoich obowiązków przez osoby fizyczne i ich odpowiedzialność. To niezwykle istotne w sektorze publicznym choćby z uwagi na zasady odpowiedzialności karnej funkcjonariuszy publicznych za niedopełnienie obowiązków, bądź też zasady odpowiedzialności za naruszenie dyscypliny finansów publicznych[30].

Brak wdrożenia odpowiednich środków technicznych i organizacyjnych oraz brak analizy ryzyka

Zarówno WSA w Warszawie, jak i Prezes UODO w analizowanej sprawie odnotowali naruszenia w postaci niewdrożenia odpowiednich środków technicznych i organizacyjnych mających na celu ochronę praw lub wolności osób fizycznych w związku z przechowywaniem nagrania sesji wyłącznie na serwerach YouTube, bez wykonywania kopii nagrań sesji Rady Miejskiej Aleksandrowa Kujawskiego, znajdujących się we własnych

[30] Zob. M. Sakowska-Baryła, *Specyfika stosowania RODO przez organy i podmioty publiczne* [w:] *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*, red. G. Sibiga, M. Praw. 2020, nr 23 – dodatek, s. 33.

zasobach Urzędu Miejskiego. Taki stan rzeczy w ocenie sądu i organu nadzorczego uzasadniał postawienie skarżącemu Burmistrzowi zarzutu naruszenia art. 5 ust. 1 lit. f, w związku z art. 5 ust. 2 RODO, a więc zasady integralności i poufności, oraz art. 32 RODO poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych, mających na celu zabezpieczenie danych osób fizycznych w związku z przechowywaniem nagrań sesji Rady Miasta wyłącznie na serwerach YouTube, bez wykonywania i przechowywania kopii zapasowych tych nagrań w zasobach własnych Urzędu Miejskiego. W ocenie sądu, przekazanie danych osobowych podmiotowi zewnętrznemu, który transmituje posiedzenia organów w ogólnodostępnej sieci jaką jest internet, gdzie przetwarzane są dane osobowe, spowodowało naruszenie przepisów o ochronie danych osobowych, a środki, które należało podjąć, winny być proporcjonalne do wskazanego wysokiego ryzyka. Sąd podniósł, że z chwilą zakończenia nagrania było ono zapisane jedynie na stronie YouTube, a u skarżącego nie pozostawała żadna kopia zapasowa, co – zdaniem Sądu – naruszało w sposób jednoznaczny i ewidentny przepisy art. 32 ust. 1 lit. b i lit. c RODO. Przy tym sąd zaakcentował, że ewentualna awaria techniczna serwisu internetowego, może spowodować utratę nagrania i uniemożliwić administratorowi danych osobowych przywrócenie ich dostępności, w efekcie podmiot zobowiązany nie będzie mógł zapewnić poufności, integralności, dostępności i odporności systemów i usług przetwarzania. Dlatego w ocenie sądu, organ w sposób prawidłowy i zgodny z obowiązującymi przepisami wykazał naruszenie przez skarżącego przepisów RODO.

Trudno nie przyznać racji temu wywodowi, aczkolwiek argumentacja ta nie jest zupełna, a przy tym, wziąwszy pod uwagę to, że w przypadku zlecania na zewnątrz usługi utrzymania BIP, zarówno organ nadzorczy, jak i sąd dobitnie akcentowali brak legalizacji takiego udostępniania danych, dziwić może, że w przypadku przekazywania danych do YouTube nie pogłębiono już argumentacji. Ani WSA w Warszawie, ani Prezes UODO nie dokonali analizy roli, w jakiej występuje podmiot będący właścicielem tego serwisu. Jak słusznie wskazują Jan Byrski i Henryk Hoser, trudno przyjąć, że jest on wyłącznie podmiotem przetwarzającym (skoro może np. potencjalnie samodzielnie usuwać opublikowane nagrania), stąd należałoby co najmniej rozważyć, czy nie powinien on występować w roli współadministratora (wspólnie z podmiotem prowadzącym kanał) – zarówno w odniesieniu do danych osób, które znajdują się na nagraniach, jak również osób, które odtwarzają nagrania zamieszczone na zewnętrznym serwisie. Zastrzeżenia i niedosyt wywołuje to, że ani Prezes UODO, ani sąd w ogóle nie przeanalizowali tej istotnej kwestii, choć ma ona niepoślednie znaczenie dla określenia obowiązków spoczywających na Burmistrzu (podmiot prowadzący kanał), jak również na podmiocie odpowiedzialnym za serwis YouTube[31].

[31] Zob. J. Byrski, H. Hoser, *Pierwsza administracyjna kara pieniężna Prezesa UODO nałożona na podmiot publiczny*, „Informacja w Administracji Publicznej" 2020, nr 1, s. 14–15.

Brak analizy ryzyka w związku z korzystaniem z kanału YouTube

Jak argumentował WSA, przepis art. 32 RODO nie wymaga od administratora wdrożenia jakichkolwiek środków technicznych i organizacyjnych, które mają stanowić środki ochrony danych osobowych, ale wymaga wdrożenia środków adekwatnych, a taką adekwatność oceniać należy pod kątem sposobu i celu, w jakim dane osobowe są przetwarzane, ale też należy brać pod uwagę ryzyko związane z przetwarzaniem tych danych osobowych, które to ryzyko charakteryzować się może różną wysokością. Przyjęte środki mają mieć charakter skuteczny, w konkretnych przypadkach niektóre środki będą musiały być środkami o charakterze niwelującym niskie ryzyko, inne zaś – muszą niwelować ryzyko wysokie, ważne jednak jest, aby wszystkie środki (a także każdy z osobna) były adekwatne i proporcjonalne do stopnia ryzyka.

Na tym tle wydaje się zasadne stawianie Burmistrzowi zarzutu nieprzeprowadzenia analizy ryzyka w związku z korzystaniem z kanału YouTube w celu realizacji obowiązku prawnego wynikającego z art. 8 ust. 2 u.d.i.p., a więc naruszenia prawa materialnego, tj. art. 5 ust. 1 lit. f w zw. z art. 5 ust. 2 i art. 24 RODO. W tym przypadku sąd nie miał wątpliwości, że wdrożone przez Burmistrza procedury nie zapewniły w pełni bezpieczeństwa danych osobowych. W ocenie sądu, wdrożenie takiej analizy zminimalizowałoby ryzyko powstania uchybień w procesie przetwarzania danych osobowych, stąd pod tym właśnie kątem należy rozpatrywać ewentualną konieczność tworzenia odpowiedniej procedury systemu bezpieczeństwa i ochrony danych osobowych. Wskazanie na konieczność wprowadzenia takiej właśnie procedury nie powinno dziwić, ani być kwestionowane ze względu na niewątpliwą spójność analizy ryzyka, czy też innych procedur z tego zakresu z ogólnym zamysłem związanym ze stosowaniem przepisów RODO, jakim jest proaktywna postawa administratora i wdrażania środków techniczno-organizacyjnych, adekwatnych do tego ryzyka . Odnotować jednak należy, że zarówno Prezes UODO, jak i WSA odnoszą się do analizy ryzyka w zakresie korzystania z kanału YouTube, uznając najpewniej, że korzystanie przez administratora z zasobów i narzędzi oferowanych przez podmioty zewnętrzne może wiązać się z – jak to określił organ nadzorczy, a później WSA – „wyższym ryzykiem naruszenia ochrony danych osobowych" ze względu na fakt, że środki organizacyjne i techniczne wykorzystywane do ochrony danych osobowych opublikowanych na YouTube zostały określone i wdrożone przez Google LLC (z siedzibą w USA), właściciela YouTube. Dla porządku podnieść wypada, że w art. 24, art. 25, art. 32 oraz w art. 3 RODO jest mowa o „ryzyku naruszenia praw lub wolności osób fizycznych", nie zaś o „ryzyku ochrony danych osobowych", jakim to terminem posłużył się sąd i organ nadzorczy. Ponadto, w ich orzeczeniach brak głębszej refleksji, z jakich powodów korzystanie przez administratora z zasobów i narzędzi oferowanych przez podmioty zewnętrzne, w tym przypadku przez podmiot prowadzący kanał YouTube, może wiązać się z wyższym ryzykiem nie tyle naruszenia ochrony danych osobowych, co naruszenia praw lub wolności osób fizycznych. Określenie „wyższe ryzyko" jest przy tym wątpliwe o tyle, że na gruncie RODO gradacja ryzyka nie obejmuje takiego poziomu jak owo „wyższe ryzyko". Właściwie z treści RODO

wyprowadzać można wniosek, że doniosłe przy stosowaniu tego aktu są trzy stany: brak ryzyka, ryzyko i wysokie ryzyko[32]. Czy zatem „wyższe ryzyko", jest „ryzykiem wysokim" nie można się dowiedzieć ani z wyroku WSA w Warszawie, ani z decyzji Prezesa UODO, a przesądzenie tego byłoby wskazane, zwłaszcza że zgodnie z art. 35 RODO, z wysokim ryzykiem wiąże się obowiązek przeprowadzenia i udokumentowania oceny skutków dla ochrony danych osobowych.

Braki w rejestrze czynności przetwarzania

Trudno podawać w wątpliwość stwierdzenie przez organ nadzorczy naruszenia przez Burmistrza art. 5 ust. 2 RODO w związku z art. 30 ust. 1 lit. d oraz lit. f RODO poprzez niewskazanie w rejestrze czynności przetwarzania danych osobowych dla czynności związanych z publikacją informacji na stronie BIP Urzędu Miasta w Aleksandrowie Kujawskim, wszystkich odbiorców danych oraz niewskazanie dla tych czynności przetwarzania planowanego terminu usunięcia danych w sposób zapewniający przetwarzanie danych, zgodnie z zasadą ograniczonego przechowywania. Stwierdzenie tego naruszenia odzwierciedla to, że organ nadzorczy przedmiotem swoich ustaleń czyni skrupulatność prowadzenia tego rejestru oraz wskazuje, że adnotacje w nim sporządzane powinny być możliwie konkretne i wyczerpujące. Sąd wskazał przy tym, że administrator, który nie wykaże w rejestrze czynności kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione, oraz nie wskaże planowego terminu usunięcia poszczególnych kategorii danej (pod warunkiem, że jest to możliwe – a w niniejszej sprawie taka możliwość istniała), narusza bezpośrednio przepisy dotyczące ochrony danych osobowych, za których przestrzeganie jest odpowiedzialny. Sąd wyprowadza z tego słuszny wniosek, że każdy z obowiązków wynikających z art. 30 ust. 1 RODO musi zostać zrealizowany: naruszeniem przepisu jest niewykonanie choćby jednego z obowiązków wskazanego przy prowadzeniu rejestru czynności przetwarzania danych osobowych.

Administracyjna kara pieniężna

Ponieważ za naruszenie przepisów art. 5 ust. 1 lit. a, e oraz lit. f, art. 5 ust. 2, art. 28, art. 30 ust. 1 lit. d i lit. f oraz art. 32 RODO Prezes UODO nałożył na Burmistrza Aleksandrowa Kujawskiego karę pieniężną w kwocie 40 tys. zł, WSA w Warszawie ocenił, mając na uwadze charakter dokonanych naruszeń oraz ilość przepisów prawa materialnego w zakresie ochrony danych osobowych, których naruszenia dopuścił się skarżący, że owa kara pieniężna jest karą adekwatną, proporcjonalną i nałożona została w sposób

[32] Zob. A. Mednis, *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych*, M. Praw. 2016, nr 20 – dodatek, s. 29.

prawidłowy. Organ należycie uzasadnił wymiar kary, biorąc pod uwagę bardzo długi czas trwania naruszeń, umyślny ich charakter, wysoki stopień odpowiedzialności administratora oraz brak jego współpracy z organem po wszczęciu postępowania. Maksymalna kara za stwierdzone naruszenia wynosi 100 tys. zł, na skarżącego nałożono tylko 40% możliwej kary, co pozwala ocenić ją jako skuteczną, proporcjonalną i odstraszającą.

Rzecz jasna, zarówno z podstawami do nałożenia administracyjnej kary pieniężnej w tym przypadku, jak i z jej wysokością można polemizować. Istotne wątpliwości budzi choćby to, czy rzeczona kara rzeczywiście jest proporcjonalna do „przewinienia" skarżącego. Można uznać także, że kwota kary jest nader wysoka, zważywszy na treść i charakter danych, dotkniętych naruszeniem RODO. Dane te bowiem w znaczącej części stanowiły informacje powszechnie dostępne, z mocy prawa podlegające udostępnieniu, choć rzeczywiście dyskusyjną kwestią pozostaje ich przechowywanie wyłącznie w zasobach YouTube, czy też poniechanie zawarcia umowy powierzenia przetwarzania danych, podczas gdy obowiązek taki istniał również pod rządami poprzednio obowiązujących przepisów prawa. Wydaje się jednak, że najistotniejszym czynnikiem, przemawiającym za jej wymierzeniem była prewencja zarówno indywidualna, jak i generalna. Jak bowiem argumentował w zaskarżonej decyzji organ nadzorczy, „odstraszający charakter kary pieniężnej wiąże się z zapobieganiem naruszeniom w przyszłości oraz przykładanie większej wagi do realizacji zadań administratora. Kara ma odstraszać zarówno administratora, przed ponownym naruszeniem, jak i inne podmioty. Nakładając decyzją administracyjną karę pieniężną za naruszenie przepisów o ochronie danych osobowych Prezes Urzędu Ochrony Danych Osobowych wziął pod uwagę oba aspekty: po pierwsze – charakter represyjny, Burmistrz naruszył przepisy ogólnego rozporządzenia o ochronie danych, po drugie – charakter prewencyjny, zarówno Burmistrz, jak i inni administratorzy, będą skutecznie zniechęceni do naruszania w przyszłości prawa ochrony danych osobowych, jednocześnie dokładając większej staranności przy realizacji swoich obowiązków wynikających z ogólnego rozporządzenia o ochronie danych".

Przytoczona argumentacja organu nadzorczego wydaje się równocześnie dobrym podsumowaniem prowadzonych tu rozważań. Z jednej strony bowiem, analizowane orzeczenia mają wymiar indywidualny dla ukaranego administratora, z drugiej zaś – orzeczenia te niewątpliwe kierują uwagę na zwiększenie staranności przy wykonywaniu wynikających z RODO obowiązków ciążących na publicznych administratorach.

Literatura

Barta P., Litwiński P., *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021.

Bernaczyk M., *Obowiązek bezwnioskowego udostępniania informacji publicznej*, Warszawa 2008.

Byrski J., Hoser H., *Pierwsza administracyjna kara pieniężna Prezesa UODO nałożona na podmiot publiczny*, „Informacja w Administracji Publicznej" 2020, nr 1.

Czerniawski M., *Ochrona danych osobowych w prawie międzynarodowym* [w:] *Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2020.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Jabłoński M., *Rola i znaczenie RODO w procesie definiowania gwarancji niezależności i spójności krajowego systemu ochrony danych osobowych* [w:] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017.

Mednis A., Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych, M. Praw. 2016, nr 20 – dodatek.

Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. M. Sakowska-Baryła, Warszawa 2018.

Sakowska-Baryła M., *Dostęp do informacji publicznej a ochrona danych osobowych*, Wrocław 2014.

Sakowska-Baryła M., *Powierzenie przetwarzania danych osobowych w sektorze publicznym* [w:] *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, red. M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda, Wrocław 2017.

Sakowska-Baryła M., *Problem współstosowania ustawy o dostępie do informacji publicznej i ustawy o ochronie danych osobowych* [w:] *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, red. A. Mednis, Warszawa 2016.

Sakowska-Baryła M., *Specyfika stosowania RODO przez organy i podmioty publiczne* [w:] *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*, red. G. Sibiga, M. Praw. 2020, nr 23 – dodatek.

Sibiga G., *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych osobowych – wybrane zagadnienia*, [w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*, red. *idem*, „Biblioteka Monitora Prawniczego" 2016.

Sibiga G., Małobęcka-Szwast I., *Relacje prawa do informacji publicznej oraz prawa do ochrony danych osobowych w świetle ogólnego rozporządzenia o ochronie danych (RODO)* [w:] *Polskie przepisy o ochronie danych osobowych. Aktualne problemy prawnej ochrony danych 2019*, red. *idem*, M. Praw. 2019, nr 22 – dodatek.

Wilbrandt-Gotowicz M., *Prywatność osoby fizycznej jako ograniczenie jawności informacji publicznych (w świetle orzecznictwa sądów administracyjnych)* [w:] *Jawność i jej ograniczenia*, red. G. Szpor, t. 4, *Znaczenie orzecznictwa*, red. M. Jaśkowska, Warszawa 2014.

Streszczenie

Marlena Sakowska-Baryła

Pierwsza administracyjna kara pieniężna nałożona na podmiot z sektora publicznego

Glosa poświęcona została omówieniu wyroku WSA w Warszawie, a także poprzedzającej go decyzji Prezesa Urzędu Ochrony Danych Osobowych w sprawie na styku ochrony danych osobowych oraz dostępu do informacji publicznej. Orzeczenia te można uznać za doniosłe o tyle, że

dotyczą udostępniania danych osobowych w Biuletynie Informacji Publicznej, kwestii retencji danych osobowych leżącej w gestii podmiotu publicznego w przypadku, gdy przepisy nie precyzują czasu upubliczniania danych w tymże publikatorze, zabezpieczenia danych, w tym wdrożenia procedur, których prowadzenie nie zostało wprost przewidziane w ustawie, powierzenia przetwarzania danych osobowych w warunkach działalności podmiotów publicznych, a wreszcie dość newralgicznego zagadnienia, jakim jest zastosowanie RODO do przetwarzania danych osobowych w związku z realizacją dostępu do informacji publicznej. Na kanwie tych orzeczeń możliwe jest prześledzenie istotnych kwestii współstosowania przepisów RODO z przepisami regulującymi zagadnienia dostępu do informacji publicznej na wielu płaszczyznach – zarówno w obszarze dopuszczalności przetwarzania danych osobowych oraz zasad rozliczalności, jak i w obszarze techniczno-organizacyjnym.

Słowa kluczowe: informacja publiczna; administracyjna kara pieniężna; sektor publiczny; RODO; Biuletyn Informacji Publicznej; bezpieczeństwo danych, oświadczenia majątkowe.

Summary

Marlena Sakowska-Baryła

First Administrative Fine Imposed on a Public Sector Entity

The text discusses the judgement of the Voivodeship Administrative Court in Warsaw and the preceding decision of the President of the Personal Data Protection Office concerning the issue of personal data protection and access to public information. These rulings can be considered important as they concern the access to personal data in the Public Information Bulletin, the issue of retention of personal data which are within the competence of a public entity when the regulations do not specify the time of making the data public in that publication, data security, including the implementation of procedures, the performance of which is not directly provided by the law, entrusting the processing of personal data in the conditions of activity of public entities, and finally quite a sensitive issue which is the application of GDPR to the processing of personal data in relation to the exercise of access to public information. On the basis of these rulings, it is possible to trace significant issues of co-application of the provisions of GDPR with the provisions regulating the issues of access to public information at many levels – both in the area of admissibility of personal data processing and the principles of accountability, as well as in the technical and organisational.

Keywords: public information; administrative fine; public sector; GDPR; Public Information Bulletin; data security, assets declaration.

Realizacja obowiązków administratora danych w związku z powierzeniem przetwarzania danych osobowych, odpowiedzialność podmiotu przetwarzającego oraz model współpracy między tymi podmiotami

Decyzja Prezesa Urzędu Ochrony Danych Osobowych
z dnia 11 lutego 2021 r., DKN.5130.2024.2020

1. **Obowiązkiem administratora (…) przy dokonywaniu oceny proporcjonalności zabezpieczeń jest branie pod uwagę czynników i okoliczności dotyczących przetwarzania (np. rodzaj, sposób przetwarzania danych) i ryzyka, jakie się z nim wiąże. Jakiekolwiek zmiany w procesie przetwarzania danych osobowych są okolicznością szczególnie obarczającą administratora odpowiedzialnością za zmaterializowanie się zagrożeń związanych z niedopełnieniem powyższych obowiązków. Zapewnienie odpowiedniego bezpieczeństwa danym osobowym, na każdym etapie przetwarzania, powinno być przedmiotem szczególnej troski administratora.**
2. **(...) Koniecznością staje się możliwość udowodnienia przed organem nadzorczym, że wprowadzone rozwiązania, mające na celu zapewnienie bezpieczeństwa danych osobowych, są adekwatne do poziomu ryzyka, jak również uwzględniają charakter danej organizacji oraz wykorzystywanych mechanizmów przetwarzania danych osobowych. Administrator samodzielnie ma przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka.**

Edyta Bielak-Jomaa
Uniwersytet Łódzki
ejomaa@wpia.uni.lodz.pl
ORCID: 0000-0002-9217-7959

https://doi.org/10.26881/gsp.2021.4.11

1. Uwagi wstępne

Komentowana decyzja odnosi się do bardzo istotnego – z praktycznego punktu widzenia – zagadnienia, jakim jest prawidłowa realizacja ciążących na administratorze danych obowiązków w związku z powierzeniem przetwarzania danych osobowych, odpowiedzialności podmiotu przetwarzającego oraz modelu współpracy między tymi podmiotami. Glosowane rozstrzygnięcie porusza także inną ważną i w praktyce trudną kwestię – przeprowadzenie przez administratora oceny ryzyka, ale ta pozostaje nieco na uboczu rozważań prowadzonych w niniejszym opracowaniu.

Tytułem wprowadzenia godzi się przypomnieć najbardziej istotne aspekty analizowanego rozstrzygnięcia organu nadzorczego. W dniu 11 lutego 2021 r. Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO), wydał decyzję, mocą której ukarał Krajową Szkołę Sądownictwa i Prokuratury – administratora danych osobowych, karą 100 tys. zł za brak realizacji ciążących na niej obowiązków administratora, czego skutkiem było naruszenie ochrony danych osobowych dotyczące ponad 50 tys. osób, m.in. sędziów, prokuratorów, asesorów prokuratury, referendarzy sądowych, kuratorów, polegające na nieuprawnionym dostępie do bazy danych Krajowej Szkoły Sądownictwa i Prokuratury (KSSiP)[1]. Kategorie danych, których dotyczyło naruszenie obejmowały: imiona i nazwiska, adresy e-mail, numery telefonów, adresy zamieszkania, miejsca pracy oraz ich adresy, adresy IP, daty pierwszego i ostatniego logowania, hasła i numery różnego rodzaju komunikatorów, numery PESEL. Naruszenie spowodowało, w ocenie Prezesa UODO, wysokie ryzyko wystąpienia negatywnych skutków w przyszłości, wynikających z charakteru danych, dużej liczby podmiotów danych, prawdopodobnie złej woli osoby, która w sposób nieuprawniony uzyskała do nich dostęp.

Krajowa Szkoła Sądownictwa i Prokuratury zgłosiła Prezesowi UODO naruszenie ochrony danych osobowych, w którym wskazano, że administrator został powiadomiony przez Komendę Główną Policji o pojawieniu się w internecie danych osobowych związanych z domeną kssip.gov.pl. Tego samego dnia administrator stwierdził naruszenie ochrony danych osobowych. Po zapoznaniu się z rodzajem danych ustalił, że są to dane z bazy danych witryny szkolenia.kssip.gov.pl powstałe w trakcie testowej migracji do nowej platformy szkoleniowej ekssip.kssip.gov.pl. W celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków wobec osób, których dane dotyczą, administrator wysłał zgłoszenie do administracji forum publikującego odnośnik do bazy danych z żądaniem zablokowania informacji oraz do administracji portalu udostępniającego plik z danymi – o zablokowanie możliwości pobierania. Ponadto, usunął wszystkie hasła na nowej platformie i umieścił informację o konieczności zmiany hasła przy logowaniu do nowej platformy. Stwierdzając wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, rozpoczął informowanie wszystkich osób, których naruszenie dotyczy, o zaistniałej sytuacji.

[1] Zob. glosowana decyzja DKN.5130.2024.2020, https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020 [dostęp: 20.11.2021].

Zdaniem Prezesa UODO, KSSiP naruszyła szereg przepisów RODO[2]: art. 5 ust. 1 lit. f, art. 25 ust. 1, art. 28 ust. 3, art. 32 ust. 1 i 2, poprzez:

a) niezastosowanie odpowiednich środków technicznych i organizacyjnych mających zapewnić zdolność do ciągłego zapewnienia poufności usług przetwarzania;
b) brak testowania i oceny skuteczności środków technicznych i organizacyjnych, mających na celu zapewnienie bezpieczeństwa danych osobowych znajdujących się w kopii bazy danych platformy szkoleniowej Krajowej Szkoły Sądownictwa i Prokuratury;
c) niewłaściwe uwzględnienie ryzyka związanego ze zmianami w procesie przetwarzania;
d) powierzenie przetwarzania danych osobowych z naruszeniem art. 28 ust. 3 RODO:
   – bez umownego zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora;
   – bez określenia w umowie powierzenia przetwarzania danych osobowych kategorii osób;
   – bez doprecyzowania rodzaju danych osobowych przez wskazanie ich kategorii.

Administrator, bez względu na to, czy jest jedynym podmiotem przetwarzającym dane osobowe, czy tez powierza dane, albo ich część do przetwarzania innemu podmiotowi, ponosi odpowiedzialność za ich bezpieczeństwo. Przepisy rozporządzenia 2016/679 zobowiązują więc zarówno administratorów, jak i podmioty przetwarzające do przyjęcia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych. W analizowanym rozstrzygnięciu, Prezes UODO uznał, że administrator – KSSIP nie zapewnił bezpieczeństwa danych (poprzez niezastosowanie odpowiednich środków technicznych i organizacyjnych służących poufności przetwarzania, brak testowania i oceny skuteczności tych środków oraz niewłaściwe uwzględnienie ryzyka związanego ze zmianami w procesie przetwarzania danych), co było spowodowane niezgodnością z przepisami RODO zawartej umowy powierzenia oraz zakresem odpowiedzialności stron tej umowy.

2. Obowiązki administratora

W przywołanej decyzji Prezes UODO kilkukrotnie wskazał na obowiązki administratora w przetwarzaniu danych osobowych, przede wszystkim w kontekście stosowania środków technicznych i organizacyjnych, o których mowa w art. 24, art. 25 i art. 32 RODO. Zgodnie z art. 24 ust. 1 RODO, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1; dalej: RODO; rozporządzenie 2016/679).

prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem, i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

W świetle glosowanej decyzji, oznacza to, że KSSiP, przy dokonywaniu oceny proporcjonalności zabezpieczeń powinna uwzględnić czynniki i okoliczności dotyczące przetwarzania (np. rodzaj danych osobowych, sposób przetwarzania danych) i ryzyko, jakie się z nim wiąże. Słusznie podkreślił Prezes UODO, że wdrożenie odpowiednich zabezpieczeń stanowi obowiązek będący przejawem realizacji ogólnej, określonej w art. 5 ust. 1 lit. f RODO, zasady integralności i poufności, zgodnie z którą dane osobowe powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Środki te powinny być zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą. Powinny one zatem uwzględniać, zgodnie z art. 25 ust. 1 rozporządzenia 2016/679, stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania.

Administrator zobowiązany jest ponadto do zastosowania środków technicznych i organizacyjnych odpowiadających ryzyku (adekwatnych do tego ryzyka) naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia (art. 32 ust. 1 RODO). Oznacza to, że odpowiedzialny administrator powinien wpierw określić poziom ryzyka, jakie wiąże się z przetwarzaniem danych osobowych, by móc następnie zdecydować, jakie odpowiadające temu ryzyku (minimalizujące je), środki techniczne i organizacyjne zastosować. Znajduje to potwierdzenie w wyroku wojewódzkiego sądu administracyjnego z dnia 3 września 2020 r.[3] Sąd orzekł w nim, że administrator samodzielnie ma przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka. Uwzględnić, przy tym powinien ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. W innym orzeczeniu sąd orzekł, że w art. 32 rozporządzenia 2016/679 nie wymaga się od administratora danych wdrożenia jakichkolwiek środków technicznych i organizacyjnych, które mają stanowić środki ochrony danych osobowych, ale wymaga wdrożenia środków adekwatnych. Taką adekwatność oceniać należy pod kątem sposobu i celu, w jakim dane osobowe są przetwarzane, ale też należy brać pod uwagę ryzyko związane

[3] Wyrok WSA w Warszawie z dnia 3 września 2020 r., II SA/Wa 2559/19, LEX nr 3077973.

z przetwarzaniem tych danych osobowych, które to ryzyko charakteryzować się może różnym poziomem[4].

Analiza ryzyka powinna mieć także znaczenie przy wyborze podmiotu przetwarzającego oraz przy określeniu warunków umowy powierzenia. Zgodnie z art. 28 ust. 1 rozporządzenia 2016/679, administrator powinien korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą[5]. Realnemu zapewnieniu tego wymogu służy uprawnienie administratora do uzyskania od podmiotu przetwarzającego wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz uprawnienie do przeprowadzania audytów, w tym inspekcji. Jak wskazuje się w motywie 81 RODO, aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. Administrator musi więc nie tylko sprawdzić prawidłowość i adekwatność środków bezpieczeństwa zastosowanych przez podmiot przetwarzający, ale także móc wykazać, że weryfikacji takiej dokonał, np. poprzez dokonanie audytu albo żądanie od podmiotu przetwarzającego dowodu, że taki audyt się odbył, i raportu z jego przeprowadzenia[6]. Tymczasem, w prezentowanej sprawie, administrator nie mógł wykazać się ani posiadaniem odpowiedniej dokumentacji potwierdzającej przyjęcie i wdrożenie środków zabezpieczenia technicznego i organizacyjnego, zgodnie z przepisami RODO, co świadczy o naruszeniu przepisów i skutkuje brakiem kontroli administratora nad przetwarzaniem danych osobowych, ani także – co jest kluczowe z punktu widzenia analizowanego rozstrzygnięcia – wskazaniem przesłanek weryfikacji podmiotu przetwarzającego. Warte podkreślenia jest stanowisko Prezesa UODO, który uznał, że wybór nawet profesjonalnego hostingodawcy posiadającego niezbędne certyfikaty przy określonych zabezpieczeniach dostępu do systemu oraz przy ograniczeniu kontaktu między pracownikami administratora i podmiotu przetwarzającego nie jest gwarancją minimalizowania ryzyka ewentualnego naruszenia bezpieczeństwa danych, na co wskazywał administrator. Słusznie zauważył też, że nie wyczerpuje to w żaden sposób obowiązku przeprowadzenia analizy ryzyka, która w tym przypadku jest nieadekwatna zarówno w odniesieniu do charakteru podejmowanych czynności w związku z migracją, jak i charakteru zawartej umowy usługi hostingu.

---

4 Wyrok WSA w Warszawie z dnia 26 sierpnia 2020 r., II SA/Wa 2826/19, LEX nr 3067899.

5 Wyrok WSA w Warszawie z dnia 27 października 2020 r., II SA/Wa 2559/19, LEX nr 3100511.

6 M. Krzysztofek, *Warunki dopuszczalności powierzenia – lista kontrolna*, ABI Ekspert 2017, nr 4, s. 19.

Prezes UODO zarzucił KSSiP, że brak angażowania podmiotu przetwarzającego w proces migracji oraz nieudzielenie pełnych informacji o podejmowanych czynnościach i oczekiwanych rezultatach, spowodowało, że administrator nie miał wiedzy, czy przetwarzane dane osobowe są odpowiednio zabezpieczone. Prowadzi to do stwierdzenia, że KSSiP nie podjęła wystarczających działań mających na celu zweryfikowanie bezpieczeństwa środowiska przetwarzania zarówno przed rozpoczęciem działań migracyjnych, jak i po ich zakończeniu, a w szczególności nie zweryfikowała lokalizacji kopii bazy danych.

3. Umowa powierzenia

W opisywanym przypadku dużą rolę odgrywa też zakres i poziom usług wynikający z umowy hostingowej. Kwestię tę podkreślono w uzasadnieniu decyzji o nałożeniu na administratora kary. Jak wynika z treści, podmiot przetwarzający jako wykonawca usługi hostingowej, został wyłoniony w postępowaniu o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego[7]. Prezes UODO, powołując się na treść art. 28 ust. 3 RODO, wskazał, że umowa ma na celu zapewnienie precyzyjnego ustalenia granic działania podmiotu przetwarzającego, powinna zatem kompleksowo regulować, co jest podstawą umowy powierzenia ze względu na związanie podmiotu przetwarzającego z celem ustalonym przez administratora, oraz wskazywać treść. Artykuł 28 ust. 3 RODO, w sposób rozbudowany determinuje treść umowy, która musi zawierać przedmiot i czas trwania przetwarzania; charakter i cel przetwarzania; rodzaj danych osobowych; kategorie osób, których dane dotyczą; obowiązki i prawa administratora. W literaturze podkreśla się, że określenie celu i charakteru przetwarzania oraz rodzaju danych osobowych sprowadzać się powinno do doprecyzowania, jakie kategorie danych i po co zostały powierzone do przetwarzania, a także w jaki sposób mają być przetwarzane. Precyzyjna regulacja w tym zakresie konieczna jest ze względu na związanie podmiotu przetwarzającego ustalonym przez administratora celem[8].

W glosowanej decyzji w sposób niewystarczający określono zakres powierzanych danych. Wskazano bowiem, że „podmiot przetwarzający w ramach świadczenia usługi hostingowej przetwarzał będzie powierzone dane osobowe zwykłe obejmujące zbiory danych osobowych niezbędne do wykonywania prac w systemie informatycznym na rzecz administratora". Krajowa Szkoła Sądownictwa i Prokuratury, powierzając przetwarzanie danych osobowych, nie wskazała w umowie powierzenia kategorii osób oraz nie doprecyzowała rodzaju danych osobowych przez podanie ich kategorii. Opisując przetwarzanie danych, umowa powinna bowiem również odwoływać się do kategorii danych osobowych, jeśli można je doprecyzować. O ile w przypadku przetwarzania danych związanych np. z usługą poczty elektronicznej, trudno jest jednoznacznie taki

[7] Ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 1843).

[8] K. Witkowska-Nowakowska, *Komentarz do art. 28 RODO* [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 639.

zakres wskazać, o tyle w przypadku przetwarzania danych w celach związanych z funkcjonowaniem platformy szkoleniowej KSSiP, informacje takie, jako możliwe do określenia, powinny być w niej zawarte.

Ponadto, jak wskazano w decyzji, administrator nie zawarł w umowie zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora, co stanowi wymóg wynikający z art. 28 ust. 3 pkt a rozporządzenia 2016/679. Trudno nie podzielić stanowiska Prezesa Urzędu, że określenie sposobu zgłaszania (pisemnie, faksem, pocztą elektroniczną) usterek związanych z usługami hostingowymi, w tym ich niedostępność, nie jest wystarczające do uznania tego postanowienia za udokumentowane polecenie administratora. Udokumentowane polecenie administratora oznacza bowiem możliwość przetwarzania danych na podstawie udokumentowanych instrukcji i wskazówek administratora. Co prawda prawodawca unijny, wprowadzając obowiązek dokumentowania wszystkich wskazówek, nie przesądził, jaką ma mieć ono formę, to jednak warto zauważyć, że zastrzeżenie możliwości działania podmiotu przetwarzającego wyłącznie na udokumentowane polecenie administratora może zostać implementowane do umowy na etapie jej tworzenia. Skoro w art. 28 ust. 3 lit. a RODO wymaga się, by sama umowa powierzenia miała formę pisemną, w tym elektroniczną, to należy przyjąć, że w jej ramach ustanowiony powinien zostać generalny obowiązek działania na udokumentowane polecenie administratora, natomiast dopuszczalne wydaje się przyjęcie, że same wskazówki kształtowane być mogą na późniejszym etapie w formie ustalonej przez strony stosunku powierzenia. Istotne jest natomiast, by wszelkie polecenia administratora były konsekwentnie dokumentowane[9]. Takich działań nie wykonał administrator, bowiem ani umowa nie zawierała ogólnego polecenia, ani na późniejszym etapie jej realizacji administrator nie przekazał żadnych wskazówek procesorowi, które to polecenie by dokumentowały.

4. Model współpracy administratora z podmiotem przetwarzającym

Konsekwencją zawarcia umowy powierzenia jest zbudowanie prawidłowego modelu współpracy między stronami umowy. W komentowanej decyzji, Prezes UODO poświęcił uwagę ocenie współpracy między KSSIP a podmiotem przetwarzającym. Zasady i zakres współpracy wynikać powinny z treści umowy powierzenia, winny być bowiem one efektem wzajemnych relacji, obowiązków i odpowiedzialności stron umowy powierzenia. Dla prawidłowej realizacji umowy kapitalne znaczenie ma dodatkowo określenie kanałów komunikacyjnych między administratorem i podmiotem przetwarzającym. W analizowanym rozstrzygnięciu model współpracy administratora z procesorem był nieskuteczny. Brak zrozumienia przez administratora roli, jaką on pełni w relacji z podmiotem przetwarzającym, doprowadziły do naruszenia ochrony danych osobowych. Krajowa Szkoła Sądownictwa i Prokuratury zarówno przed naruszeniem

[9] *Ibidem*, s. 640.

ochrony danych, jak i po jego stwierdzeniu nie miała pełnej świadomości, jak kształtują się prawa i obowiązki pomiędzy nią a podmiotem przetwarzającym.

Podmiot przetwarzający wskazywał, że kilkukrotnie strony prowadziły korespondencję mającą na celu jasne wskazanie kwestii działań podmiotu przetwarzającego nad systemem hostującym, a obszarem danych i aplikacji klienta, którym podmiot przetwarzający się nie zajmował, i do którego wglądu nie posiadał. Z okoliczności sprawy wynikało, że pracownicy KSSiP zarówno przed naruszeniem ochrony danych, jak i po jego stwierdzeniu, nie mieli pełnej świadomości, jak kształtują się prawa i obowiązki pomiędzy administratorem a podmiotem przetwarzającym. Administrator wielokrotnie oczekiwał wykonywania zadań wykraczających poza zakres tej umowy. Podmiot przetwarzający nie znał struktury i konfiguracji autorskich aplikacji instalowanych przez administratora na tych zasobach, w tym nie miał obowiązku, bez wiedzy administratora i na udokumentowane jego polecenie, prowadzenia czynności konfiguracyjnych w zakresie dostępu do katalogów czy baz danych, z których aplikacje te korzystają. Zgodnie z istotą świadczonej usługi, administrator dysponuje pełną wiedzą o tym, jakie dane osobowe przetwarza, w jaki sposób, w jakiej lokalizacji (w ramach udostępnionych zasobów) i za pomocą jakich narzędzi. Jedynie na udokumentowane polecenie administratora podmiot przetwarzający może dokonywać ingerencji w zakresie wynikającym z charakteru świadczonych usług i zawartej umowy.

Kolejnym zagadnieniem, na jakie zwrócił uwagę Prezes UODO, jest język komunikacji między stronami umowy powierzenia. Administrator posługiwał się określoną nomenklaturą i oznaczeniami (np. baza danych PROD PS, „stara" platforma szkoleniowa, platforma e-learning, baza szkoleniowa), która dla dostawcy usług hostingowych, z uwagi na charakter świadczonej usługi, w opinii procesora, była nieprawidłowa i niezrozumiała. Rodziło to problemy interpretacyjne i oznaczało oczekiwanie administratora do wykonywania przez podmiot przetwarzający czynności poza określone w umowie. Przepisy rozporządzenia 2016/679, jak wskazano w komentowanej decyzji, dają pewną swobodę w zakresie kształtowania relacji między administratorem a podmiotem przetwarzającym. Należy więc oczekiwać, że administrator wypracuje model współpracy z podmiotem przetwarzającym, który będzie zapewniał przetwarzanie zgodne z przepisami o ochronie danych osobowych, a w szczególności będzie umożliwiał realizację zasady rozliczalności wyrażoną w art. 5 ust. 2 RODO. O ile zatem strony umowy ustaliły kanały komunikacji oraz wyznaczyły osoby wykonujące czynności związane z realizacją umowy, o tyle osoby wskazane przez KSSiP nadal nie miały świadomości, jak kształtują się prawa i obowiązki pomiędzy administratorem a podmiotem przetwarzającym. Uprawniona jest więc konstatacja, że osoby wyznaczone do kontaktu z podmiotem przetwarzającym, powinny zostać uprzednio poinformowane o zakresie usług świadczonych przez podmiot przetwarzający i o obowiązkach leżących po stronie administratora. Treść porozumienia natomiast nie powinna budzić wątpliwości, a zatem strony powinny używać i posługiwać się pojęciami zrozumiałymi dla obu stron, co może skutecznie minimalizować ryzyko naruszenia ochrony danych osobowych.

Brak współpracy na poziomie poprawnej komunikacji, błędne polecenia wydawane podmiotowi przetwarzającemu, fałszywa ocena ról, zadań i zakresu obowiązków określonych w umowie powierzenia prowadzą w konsekwencji do braku właściwej, odpowiedzialnej weryfikacji tego, czy zlecona czynność została wykonana, i czy została wykonana prawidłowo. Trzeba zaznaczyć, że administrator jest inicjatorem podejmowanych działań jako podmiot decydujący o celach i sposobach przetwarzania. Zgodnie z umową o świadczenie usług, to jemu zostało udostępnione środowisko, w którym tego przetwarzania dokonuje, i to administrator w pierwszej kolejności odpowiada za bezpieczeństwo przetwarzanych danych, a jak wynika z umowy, w razie konieczności korzysta z pomocy podmiotu przetwarzającego.

5. Odpowiedzialność podmiotu przetwarzającego

Całościowa ocena stanu faktycznego analizowanej sprawy wymaga zrecenzowania działań podmiotu przetwarzającego, w kontekście ich wpływu na naruszenie ochrony danych osobowych. W glosowanej decyzji, zdaniem organu nadzorczego, podmiot przetwarzający wypełniał obowiązki wynikające z umowy powierzenia i umowy głównej, a także stosował przyjęte przez siebie środki organizacyjne, mające na celu zapewnienie bezpieczeństwo systemów informatycznych. To administrator nie podjął się analizy, czy wskazując podmiotowi przetwarzającemu miejsce do wykonania kopii zapasowej bazy danych, nie naraża danych osobowych w niej zawartych na naruszenie ich poufności; nie poinformował podmiotu przetwarzającego o istotności podejmowanych działań pod kątem ochrony danych osobowych.

Prezes UODO uznał, że co prawda z art. 28 ust. 3 lit. f RODO wynika obowiązek podmiotu przetwarzającego wspierania administratora w wywiązywaniu się z obowiązków określonych w art. 32–36 tego rozporządzenia, jednak opatrzony jest on warunkami, które należy za każdym razem uwzględnić, tj. charakter przetwarzania oraz dostępne podmiotowi przetwarzającemu informacje. W umowie powierzenia określono, że podmiot przetwarzający pomaga w tym zakresie „w miarę możliwości". Krajowa Szkoła Sądownictwa i Prokuratury jednak w zleceniach nie zwróciła się z prośbą o uprzednie zweryfikowanie bezpieczeństwa wskazanej lokalizacji oraz nie poinformowała podmiotu przetwarzającego o okolicznościach prowadzonych czynności, tj. prowadzonej migracji, której przedmiotem są dane osobowe, oraz że proces ten musi zapewniać ich odpowiednie bezpieczeństwo. Podmiot przetwarzający, nie dysponując takimi informacjami, nie może za każdym razem domyślać się charakteru wykonywanej czynności i każdą operację wykonywać, uprzednio weryfikując, czy ma do czynienia z danymi osobowymi, oraz czy środowisko i zasoby, udostępnione zgodnie z umową administratorowi, są prawidłowo i bezpiecznie skonfigurowane. Kontekst prowadzonych działań był znany wyłącznie administratorowi, i to na nim spoczywa bezwzględny obowiązek upewnienia się, czy prowadzone czynności nie będą narażały osób, których przetwarzanie danych dotyczy, na naruszenie ich praw lub wolności.

Prezes UODO uznał, że za całość operacji związanych z wykonaniem kopii bazy danych i przekazaniem jej do serwera docelowego, odpowiedzialny był KSSiP, podmiot przetwarzający nie był angażowany ani informowany o charakterze podejmowanych czynności, i realizował zadania wynikające z umowy o świadczenie usług, np. czynności w ramach wsparcia technicznego. Nie dopatrzył się również okoliczności, które pozwoliłyby stwierdzić, że procesor nie zapewniał wystarczających gwarancji dla bezpieczeństwa danych osobowych oraz nie udostępniał administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 rozporządzenia 2016/679 bądź uniemożliwiał administratorowi przeprowadzanie audytów, w tym inspekcji. W konsekwencji, Prezes UODO umorzył postępowanie administracyjne wobec podmiotu przetwarzającego.

Uważam, że kwestia umorzenia postępowania wobec podmiotu przetwarzającego powinna być jednak skomentowana. W ocenie Prezesa UODO, procesor wypełniał obowiązki wynikające z umowy powierzenia i umowy głównej, a także stosował przyjęte przez siebie środki organizacyjne mające na celu zapewnienie bezpieczeństwa systemów informatycznych. Zdaniem Prezesa UODO, to administrator nie podjął się analizy, czy wskazując podmiotowi przetwarzającemu miejsce do wykonania kopii zapasowej bazy danych, nie naraża danych osobowych w niej zawartych na naruszenie ich poufności. Warto jednak zwrócić uwagę, że podmiot przetwarzający powinien pomagać administratorowi także w realizacji obowiązków wynikających z art. 32–36 RODO, a odnoszących się do: bezpieczeństwa przetwarzania, zgłaszania naruszeń ochrony danych organowi nadzorczemu, zawiadamiania osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, oceny skutków dla ochrony danych oraz uprzednich konsultacji. Jak wskazuje się w literaturze, ustalenie zasad partycypacji podmiotu przetwarzającego w realizacji tych zadań ma szczególnie istotne znaczenie z perspektywy administratora, rozliczanego przez organ nadzorczy z ich realizacji. Słusznie podkreśla się, że ze zobowiązaniem podmiotu przetwarzającego do wsparcia w wykonywaniu wskazanych powyżej obowiązków współgrają normy adresowane bezpośrednio do tego podmiotu, mieszczące się w art. 32–36 RODO. W konsekwencji, poza nałożeniem na podmiot przetwarzający obowiązku zastosowania odpowiednich środków bezpieczeństwa wynikającego z art. 32 RODO, wskazać należy w tym aspekcie na zobowiązanie podmiotu przetwarzającego do obowiązków implikujących konieczność przeprowadzenia kompleksowej, rzetelnej i wyczerpującej analizy procesów przetwarzania i całego kontekstu, w jakim to przetwarzanie się odbywa. Do takiego całościowego zbadania danego przetwarzania niezbędne jest uzyskanie przez administratora szeregu informacji, w tym m.in. w zakresie stosowanych środków bezpieczeństwa, certyfikacji w określonych obszarach, zidentyfikowanych po stronie podmiotu przetwarzającego zagrożeń i ryzyk związanych z przetwarzaniem[10]. O ile zatem należy zgodzić się ze stanowiskiem Prezesa UODO, że odpowiedzialność za wyciek

[10] K. Witkowska-Nowakowska, *Komentarz do art. 28 RODO*…, s. 642–643, M. Sakowska-Baryła, komentarz do art. 28 [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. *eadem*, Warszawa 2018, s. 327–328.

ponosi uczelnia, trudno podzielać opinię, że procesor, który zarządzał zasobami serwerowymi, nie ponosi żadnej winy, a więc także odpowiedzialności za wyciek danych. W przedstawionej sprawie działania podmiotu przetwarzającego określić można jako bierne zachowanie. Wykonywał on działania ograniczone do poleceń administratora, odmawiając wykonania polecenia lub żądając jego doprecyzowania, w sytuacji gdy były one niejasne albo nieprecyzyjne. W mojej ocenie, takie zaangażowanie podmiotu przetwarzającego, w tej konkretnie sprawie, nie spełniało obowiązku udzielania pomocy, do którego zobowiązany jest podmiot przetwarzający na mocy art. 28 ust. 3 lit. f RODO. W doktrynie wskazuje się, że naruszenie obowiązku pomocy administratorowi nie musi prowadzić do naruszenia obowiązku realizacji praw podmiotów danych przez administratora, ale wówczas, gdy administrator będzie mógł zrealizować te obowiązki nawet przy braku pomocy procesora[11]. W tym określonym przypadku działanie administratora doprowadziło jednak do naruszenia bezpieczeństwa danych osobowych, należałoby zatem podjąć próbę odpowiedzi na pytanie, czy do naruszenia doszłoby, gdyby procesor w sposób bardziej aktywny udzielał pomocy administratorowi oraz czy nie wpływało to na rozmiar i skalę naruszenia. Jednak, trzeba przypomnieć, że administrator dokonał wyboru profesjonalnego podmiotu (z zachowaniem formalnych wymogów), miał więc słusznie prawo oczekiwać od niego wsparcia na wysokim poziomie fachowości. Warto również zwrócić uwagę na to, że przepis ten (art. 28 ust. 3 lit. f RODO) uzależnia pomoc udzielną administratorowi od charakteru przetwarzania i dostępnych informacji, jakie posiada procesor. Prawodawca europejski nie ogranicza zakresu pomocy do informacji uzyskanych od administratora. Gdyby jednak nawet rozumienie „dostępnych informacji" zawęzić tylko do tych otrzymywanych od administratora, to uważam, że w tej sprawie należy przyjąć, że podmiot przetwarzający na podstawie nieprecyzyjnych komunikatów, jakie otrzymywał od pracowników administratora miał podstawę do uznania, że po stronie administratora występują problemy ze zrozumieniem jego roli, uprawnień i możliwości działania. To już powinno uruchomić po stronie procesora decyzję o wsparciu KSSiP w zakresie zapewnienia bezpieczeństwa danych osobowych przetwarzanych w ramach usługi hostingowej. Dodatkowo, umorzenie postępowania wobec podmiotu przetwarzającego może być niezrozumiałe również z tego powodu, że pracownik tego podmiotu otrzymał zarzuty karne związane z nielegalnym udostępnieniem danych osobowych z bazy danych KSSiP. Moim zdaniem, w tych warunkach nie sposób uznać, że procesor, przetwarzając dane z upoważnienia KSSiP, nie naruszył obowiązków podmiotu przetwarzającego, do jakich obowiązany jest mocą przepisów RODO[12].

[11] M. Gumularz, P. Kozik, *Odpowiedzialność administracyjna przy powierzaniu*, ABI Ekspert 2017, nr 4, s. 11.

[12] Poza zakresem rozważań pozostaje oczywiście problematyka ewentualnej odpowiedzialności cywilnej procesora wobec administratora danych.

6. Uwagi końcowe

Na koniec warto zaznaczyć, że analizowana decyzja jest kolejną świadczącą o tym, że przyczyn nałożenia przez organ nadzorczy administracyjnej kary finansowej, jest zwykle co najmniej kilka. Administrator w tej sprawie popełnił szereg błędów: nie uwzględnił zasady *privacy by design* – poprzez brak odpowiedniego zabezpieczenia danych osobowych już w fazie projektowania, przyjął nieprawidłową metodę współpracy z podmiotem przetwarzającym, nie wdrożył prawidłowych technicznych środków zabezpieczeń i nie uwzględnił ryzyka. Szczególną uwagę należy także zwrócić na niezrealizowanie przez administratora obowiązku kontroli procesu przetwarzania danych w całym ich cyklu. Obowiązków tych nie można sprowadzać wyłącznie do formalnego wypełniania zadań wynikających z przepisów, przygotowania dokumentacji, zawarcia umowy powierzenia, udostępnienia danych czy wprowadzenie systemów i certyfikowanych rozwiązań technicznych. Administrator musi wziąć odpowiedzialność za proces przetwarzania danych, oceniając konkretną sytuację z uwzględnieniem wszystkich okoliczności i relacji zachodzących między wszystkimi uczestnikami przetwarzania. Oczywiście nie każda, nawet błędna decyzja administratora musi prowadzić do naruszenia bezpieczeństwa danych i powodować odpowiedzialność administratora, jednak w rezultacie na poziom bezpieczeństwa danych osobowych zawsze w efekcie największy wpływ mają decyzje administratora. Dlatego Prezes Urzędu Ochrony Danych Osobowych w swoich rozstrzygnięciach wspomina nie tylko o konieczności posiadania procedur, ale też potrzebie rzeczywistego testowania i weryfikacji bezpieczeństwa, bo jest to niezbędne z punktu widzenia realizacji zasady rozliczalności.

Literatura

Gumularz M., Kozik P., *Odpowiedzialność administracyjna przy powierzaniu*, ABI Ekspert 2017, nr 4, s. 11.

Krzysztofek M., *Warunki dopuszczalności powierzenia – lista kontrolna*, ABI Ekspert 2017, nr 4, s. 19.

Sakowska-Baryła M., komentarz do art. 28 [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. *eadem*, Warszawa 2018.

Witkowska-Nowakowska K., *Komentarz do art. 28 RODO* [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Streszczenie

Edyta Bielak-Jomaa

Realizacja obowiązków administratora danych w związku z powierzeniem przetwarzania danych osobowych, odpowiedzialność podmiotu przetwarzającego oraz model współpracy między tymi podmiotami

Przedstawiona glosa dotyczy decyzji Prezesa Urzędu Ochrony Danych Osobowych nakładającej karę finansową na administratora – Krajową Szkołę Sądownictwa i Prokuratury. Administrator ukarany został za nieprawidłową realizację ciążących na nim obowiązków związanych z powierzeniem przetwarzania danych osobowych, odpowiedzialności podmiotu przetwarzającego oraz modelu współpracy między administratorem a podmiotem przetwarzającym. Odpowiedzialny administrator powinien określić poziom ryzyka, jakie wiąże się z przetwarzaniem danych osobowych, aby zastosować środki organizacyjne i techniczne adekwatne do tego ryzyka. Analiza ryzyka powinna mieć miejsce także przy wyborze podmiotu przetwarzającego, oraz określaniu warunków umowy powierzenia. Z jej treści powinny wynikać także zasady i zakres współpracy, która ma określać wzajemne relacje, obowiązki i odpowiedzialność stron umowy powierzenia. Dla prawidłowej realizacji umowy znaczenie ma dodatkowo określenie kanałów komunikacyjnych między administratorem i podmiotem przetwarzającym.

Słowa kluczowe: administracyjna kara finansowa; administrator; przetwarzający; przetwarzanie danych osobowych; analiza ryzyka; umowa powierzenia przetwarzania; RODO.

Summary

Edyta Bielak-Jomaa

Fulfillment of the Obligations of Data Controller in Connection with the Entrustment of Personal Data Processing, the Responsibility of the Processor and the Model of Cooperation Between These Entities Decision of the President of the Personal Data Protection Office of 11 February 2021, DKN.5130.2024.2020

This commentary concerns the decision of the President of the Personal Data Protection Office imposing a financial penalty on the controller – the National School of Judiciary and Public Prosecution. The controller was fined for incorrect performance of its duties related to the outsourcing of personal data processing, the responsibility of the processor and the model of cooperation between the controller and the processor. The controller in charge should determine the level of risk involved in processing of personal data in order to apply organisational and technical measures appropriate to those risks. The risk analysis should also take place when choosing the processor and defining the conditions of the entrustment agreement. The content of the agreement should also determine the principles and scope of cooperation i.e. mutual relations, duties and responsibilities of the parties to the entrustment agreement. For the proper implementation of the agreement it is also important to determine the communication channels between the controller and the processor.

Keywords: administrative fine; controller; processor; personal data processing; risk analysis; controller-processor agreement; GDPR.

Naruszenia bezpieczeństwa danych osobowych przez firmy kurierskie

Decyzja Prezesa Urzędu Ochrony Danych Osobowych
z dnia 22 kwietnia 2021 r., DKN.5130.3114.2020

W ocenie Prezesa UODO, Spółka w sposób niewystarczający dokonywała oceny skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania danych osobowych znajdujących się na dokumentach dostarczanych klientom Spółki za pośrednictwem podmiotu świadczącego usługi kurierskie, co stanowi naruszenie art. 24 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679. (…) Spółka pomimo wdrożenia polityki oraz procedur ochrony danych osobowych związanych ze zgłaszaniem naruszeń, a także zawarcia umowy powierzenia przetwarzania danych osobowych z podmiotem przetwarzającym, nie wypracowała odpowiednich mechanizmów mających na celu kontrolę realizacji przez podmiot przetwarzający swoich zobowiązań.

Paweł Litwiński
Uniwersytet SWPS
litwinski@bartalitwinski.pl
ORCID: 0000-0002-4293-1917

https://doi.org/10.26881/gsp.2021.4.12

Decyzją z dnia 22 kwietnia 2021 r. (Decyzja) Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) stwierdził naruszenie przez Cyfrowy Polsat S.A. z siedzibą w Warszawie (Spółka) art. 24 ust. 1 i art. 32 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[1] (ogólne rozporządzenie o ochronie danych) (RODO) i nałożył na Spółkę administracyjną karę pieniężną w wysokości 1.136.975 zł.

[1] Dz. Urz. UE L 119 z 2016 r., s. 1, Dz. Urz. UE L 127 z 2018 r., s. 2 oraz Dz. Urz. UE L 74 z 2021 r., s. 35.

Stan faktyczny sprawy

Decyzja została wydana w stosunkowo prostym stanie faktycznym, który jednak – jak się wydaje – ustalony został przez Prezesa UODO w sposób wybiórczy, z pominięciem istotnych okoliczności, o czym dalej. Otóż Spółka korzysta z usług podmiotu świadczącego usługi kurierskie, który w tym zakresie pełni rolę podmiotu przetwarzającego dane osobowe (tak jest traktowany przez Spółkę, a ta kwalifikacja nie została w żaden sposób zakwestionowana przez Prezesa UODO). W toku świadczonych usług kurierskich dochodziło do naruszeń bezpieczeństwa danych osobowych, polegających na „utracie przez kurierów dokumentów zawierających dane osobowe klientów lub na wydaniu przez kurierów niewłaściwej osobie dokumentów zawierających dane osobowe w postaci: imienia i nazwiska, adresu zamieszkania lub pobytu, numeru PESEL, adresu e-mail, serii i numeru dowodu osobistego bądź innego dokumentu tożsamości, numeru telefonu oraz danych dotyczących łączących strony umów"[2]. W stosunku do tych naruszeń Spółka wykonywała obowiązki zgłaszania naruszeń oraz zawiadamiania o naruszeniach osób, których dane dotyczą. Analiza informacji zawartych w zgłoszeniach oraz materiału dowodowego zebranego w postępowaniu pozwoliła Prezesowi UODO na przyjęcie, że „Spółka w sposób niewystarczający dokonywała oceny skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych znajdujących się na dokumentach dostarczanych klientom Spółki za pośrednictwem podmiotu świadczącego usługi kurierskie, co stanowi naruszenie art. 24 ust. 1 oraz art. 32 ust. 1 i 2 [RODO]"[3]. Innymi słowy, zdaniem Prezesa UODO, choć naruszeń dopuszczała się firma kurierska, to na Spółce ciążył prawny obowiązek zapewnienia bezpieczeństwa danych osobowych przetwarzanych w imieniu Spółki przez firmę kurierską.

Status firmy kurierskiej w świetle przepisów o ochronie danych osobowych

Analizę Decyzji wypada rozpocząć od najistotniejszego problemu, tj. od prawidłowej kwalifikacji prawnej firmy kurierskiej z perspektywy przepisów o ochronie danych osobowych. Istnieją w tym zakresie dwie możliwości: uznanie firmy kurierskiej za administratora danych osobowych albo za podmiot przetwarzający dane osobowe. Kwalifikacji tej trzeba przy tym dokonać oddzielnie w stosunku do trzech grup danych osobowych: danych osobowych nadawcy, danych osobowych odbiorcy oraz danych osobowych, które mogą być zawarte w przemieszczanej przesyłce.

[2] Decyzja, s. 2.
[3] *Ibidem*, s. 11.

Do rozstrzygnięcia sformułowanego wyżej problemu kluczowy wydaje się status firmy kurierskiej z perspektywy przepisów ustawy – Prawo pocztowe[4]. Otóż firmy kurierskie, którym przysługuje status operatora pocztowego w rozumieniu art. 3 pkt 12 u.p.p., dysponują ustawowym, bo wynikającym z art. 42 tejże ustawy, tytułem prawnym do przetwarzania danych osobowych przekazywanych w przesyłkach pocztowych, a także danych osobowych nadawcy i odbiorcy przesyłki. W tym zakresie nie działają więc w imieniu nadawcy przesyłki, a w imieniu własnym[5], nie sposób więc przyznać im statusu podmiotu przetwarzającego dane osobowe. Oznacza to, że podmioty świadczące usługi kurierskie powinny zostać uznane za administratorów danych osobowych, z pewnością w zakresie danych osobowych nadawców i odbiorców przesyłek – o czym w dalszej części glosy.

Mimo tego, że stwierdzenie takie nie pada wprost, a może być wyprowadzane jedynie z czynionych przez organ nadzorczy rozważań dotyczących podstawy przetwarzania danych osobowych, status administratora danych osobowych operatora pocztowego w stosunku do danych osobowych odbiorcy przesyłki został potwierdzony przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO) w decyzji z dnia 2 lipca 2013 r.[6] Odpowiadając natomiast na pytanie[7] dotyczące zadań Inspektora Ochrony Danych Osobowych (IODO), Prezes UODO stwierdził wprost, że „Poczta Polska i inni operatorzy pocztowi w związku z wykonywaniem usług pocztowych są administratorami danych osobowych nadawców i adresatów przesyłek". W tym samym wpisie uznano jednak, że przekazanie do odkażania (fumigacji) pudeł zawierających dokumenty w sytuacji, gdy pudła są zamknięte, zapieczętowane i nie są na żadnym etapie odkażania otwierane przez pracowników zleceniobiorcy, należy uznać za przypadek powierzenia przetwarzania danych, co wydaje się stanowiskiem co najmniej kontrowersyjnym, jako że w takiej sytuacji ma się do czynienia wyłącznie z operacją wykonywaną na rzeczy (pudło), bez dostępu do danych osobowych i bez operacji wykonywanych na tychże danych. Z innego założenia, jak się wydaje, wyszedł w tym zakresie bawarski organ nadzorczy, który uznał, że czyszczenie strojów roboczych, mających plakietkę z nazwiskiem, nie stanowi operacji powierzenia przetwarzania danych osobowych zawartych na tejże plakietce[8].

---

[4] Ustawa z dnia 23 listopada 2012 r. – Prawo pocztowe (tekst jedn.: Dz. U. z 2020 r., poz. 1041 ze zm.; dalej: u.p.p.).

[5] Działanie w imieniu administratora danych jest istotną cechą podmiotu przetwarzającego – dokonuje on czynności przetwarzania „w imieniu administratora", a więc sam nie decyduje o celu i sposobach przetwarzania, lecz realizuje cele wyznaczone przez administratora (zob. P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 124).

[6] DOLiS/DEC-708/13/41776; interesujące jest przy tym, że podstawą przetwarzania danych osobowych nadawcy i odbiorcy przesyłki przez operatora pocztowego jest w ocenie organu nadzorczego realizacja przez operatora pocztowego własnego prawnie uzasadnionego interesu związanego z doręczaniem przesyłek.

[7] Wpis na stronie https://uodo.gov.pl/pl/225/1467 z dnia 24 marca 2020 r. [dostęp: 22.11.2021].

[8] Bayerisches Landesamt für Datenschutzaufsicht, *FAQ zur DS-GVO*, https://www.lda.bayern.de [dostęp: 22.11.2021].

Jednocześnie jednak można odnaleźć i takie decyzje organu nadzorczego, w których firma kurierska uznana została za przetwarzającego dane osobowe na zlecenie nadawcy, który uznany został za administratora danych. W szczególności w decyzji z 21 września 2011 r.[9] stwierdzono wprost, że „spółka miała prawo do powierzenia w drodze umowy, na podstawie art. 31 ustawy [o ochronie danych osobowych z 1997 r.], dane osobowe do przetwarzania firmie kurierskiej w celu wykonywania usług miejskich i krajowych w zakresie przewożenia przesyłek". Status firm kurierskich w kontekście przetwarzania przez nie danych osobowych na potrzeby świadczenia usług kurierskich jest więc w świetle Decyzji i stanowisk organu nadzorczego wyjątkowo niejasny, a znajdujące się w obrocie prawnym rozstrzygnięcia są ze sobą sprzeczne. Co dodatkowo ważne, można sformułować istotne wątpliwości co do tego, czy przemieszczenie przesyłki zawierającej dane osobowe z punktu A do punktu B, w zamkniętej kopercie, co do której istnieje obowiązek zachowania tajemnicy korespondencji i tajemnicy pocztowej, stanowi w ogóle przetwarzanie danych osobowych zawartych w tejże przesyłce. Przetwarzaniem danych osobowych są bowiem operacje wykonywane na danych osobowych, a nie na nośnikach tychże danych. Jeżeli więc usługa polega na przemieszczeniu nośnika danych osobowych, a w świetle art. 42 u.p.p. operator pocztowy nie może się zapoznać z treścią tychże danych osobowych[10], wówczas nie sposób przyjąć, że dochodzi do przetwarzania przez niego danych osobowych. Zakaz zapoznawania się przez operatora pocztowego z danymi osobowymi zawartymi w przesyłce powoduje także, że można argumentować, iż w świetle wyroku TSUE z dnia 19 października 2016 r., C-582/14, ws. *Patrick Breyer przeciwko Bundesrepublik Deutschland*, te informacje dla operatora pocztowego nie mogą być w ogóle uznane za informacje o charakterze danych osobowych. Trybunał przyjął bowiem, że informacja nie ma charakteru danych osobowych m.in. wtedy, gdy identyfikacja osoby fizycznej jest „zakazana prawem"[11], a z taką właśnie sytuacją ma się do czynienia na gruncie działalności operatorów pocztowych.

O ile więc usługa świadczona przez firmę kurierską polegała wyłącznie na doręczeniu przesyłki do adresata, a firmie tej przysługiwał status operatora pocztowego, o tyle to ona pełniła rolę administratora danych osobowych w stosunku do danych nadawcy i odbiorcy, nie zaś ukarana Spółka. W stosunku do danych osobowych przekazywanych w przesyłkach pocztowych firma ta powinna zostać także uznana za administratora danych, albo wręcz należałoby przyjąć, że nie przetwarza ona tych danych – z pewnością jednak nie dochodziłoby w ten sposób do powierzenia

[9] DOLiS/DEC-819/11.

[10] W literaturze podnosi się, że przypadki kontroli i zatrzymywania korespondencji, a więc zapoznania się z treścią korespondencji, są określone każdorazowo we właściwych przepisach ustawowych jako przepisy odrębne pozwalające na przetwarzanie danych lub przepisów stanowiących tajemnicę pocztową – zob. M. Gaj, T. Laprus-Bałuka, A. Zaborowska, *Prawo pocztowe. Komentarz*, Warszawa 2017, s. 153.

[11] Pkt 46 uzasadnienia wyroku ws. C-582/14; zob. szerzej na ten temat P. Litwiński, *Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku Trybunału Sprawiedliwości z 19.10.2016 r. w sprawie C-582/14 Patrick Breyer*, EPS 2017, nr 5.

przetwarzania danych osobowych[12]. Nie wiadomo jednak, czy na gruncie Decyzji tak właśnie przedstawiał się stan faktyczny, ponieważ brak w niej jakichkolwiek informacji na ten temat, a pojęcie „operatora pocztowego" pojawia się w Decyzji jeden raz, w następującym kontekście: „Nawiasem mówiąc, przypadki zgłaszanych naruszeń ochrony danych osobowych związanych z nieprawidłowościami po stronie operatorów pocztowych nie należą do wyjątkowych w praktyce UODO, do wyjątków należą jednak sytuacje, w których administrator nie podejmuje natychmiastowych działań związanych z zaginięciem bądź nieprawidłowym doręczeniem nadanych przez siebie przesyłek zawierających dane osobowe klientów"[13]. Mogłoby to wskazywać na traktowanie firmy kurierskiej przez Prezesa UODO jako operatora pocztowego, jednakże zamiast tego Prezes UODO przyjmuje – w ślad za stroną – że firmie kurierskiej przysługuje status podmiotu przetwarzającego dane osobowe na zlecenie Spółki. Ważne przy tym jest przywołane już wcześniej stwierdzenie zawarte w uzasadnieniu Decyzji, że naruszenia bezpieczeństwa danych osobowych polegały na utracie przez kurierów „dokumentów zawierających dane osobowe klientów" oraz na „wydaniu przez kurierów niewłaściwej osobie dokumentów zawierających dane osobowe". Jak się więc wydaje, naruszenia te dotyczyły danych osobowych zawartych w przesyłkach.

Praktyka rynkowa wskazuje na to, że istnieją przypadki, w których firma kurierska będzie świadczyła usługę przetwarzania danych osobowych na zlecenie nadawcy. Będą to usługi związane z dostarczaniem umów i innych dokumentów od nadawcy do adresata, a polegające w szczególności na weryfikacji tożsamości adresata, który w obecności kuriera podpisuje np. umowę z nadawcą, czy na uzupełnieniu niektórych danych osobowych adresata na dokumentach, które następnie są zwracane do nadawcy. Co więcej, jak wskazuje się w literaturze, część firm kurierskich zastrzega w umowach z klientami, że przejmując od nich przesyłki, działa jako administrator danych, inne firmy z kolei – że jako podmiot przetwarzający[14]. Tymczasem, na gruncie Decyzji brak jest jakichkolwiek rozważań na ten temat, a zamiast tego w sposób automatyczny przyjęto, że firma kurierska działa jako przetwarzający dane osobowe na zlecenie ukaranej Spółki, nie uzasadniając tego w żaden sposób, w szczególności nie odnosząc się do tego, jakie usługi świadczone są przez firmę kurierską. Jednocześnie status podmiotów uczestniczących w procesie przetwarzania danych osobowych jest kluczowy z punktu widzenia zakresu ciążących na nich obowiązków, a także – a może przede wszystkim – z perspektywy nałożenia kary za naruszenie tychże. Dość powiedzieć, że jeżeli na gruncie omawianej decyzji status administratora danych przysługiwał firmie kurierskiej, wówczas nałożenie kary pieniężnej na ukaraną Spółkę pozbawione byłoby jakichkolwiek podstaw prawnych – nie można jednak tej tezy zweryfikować ze względu na bardzo istotne braki w zakresie uzasadnienia Decyzji, które wynikają, jak się wydaje, z błędów poczynionych na gruncie postępowania dowodowego w sprawie.

[12] Podobnie Bayerisches Landesamt für Datenschutzaufsicht, FAQ zur DS-GVO, https://www.lda.bayern.de [dostęp: 22.11.2021].

[13] Decyzja, s. 23.

[14] J. Styczyński, *Nierejestrowane przesyłki kontrowersyjne w świetle RODO*, „Dziennik Gazeta Prawna" z dnia 2 lipca 2019 r.

Nie można także tej informacji zweryfikować, korzystając z powszechnie dostępnego rejestru operatorów pocztowych, prowadzonego przez Prezesa Urzędu Komunikacji Elektronicznej[15], ponieważ w Decyzji nie pada nazwa firmy kurierskiej, która świadczyła usługi na rzecz ukaranej Spółki. Jest to o tyle niezrozumiałe, że Prezes UODO takimi informacjami dysponował, jako że w aktach sprawy, jak wynika z uzasadnienia Decyzji, znajduje się umowa zawarta przez Spółkę z firmą kurierską[16].

Ryzyko i jego analiza

Istotne fragmenty uzasadnienia Decyzji poświęcone są temu, jakie ryzyko dla praw i wolności osób, których dane dotyczą, powstało w wyniku naruszeń bezpieczeństwa danych osobowych zaistniałych w wyniku działań firmy kurierskiej. Sprowadzić je można do następującego fragmentu pochodzącego z uzasadnienia: „Prezes UODO uznał, że naruszenie poufności danych, w szczególności danych dotyczących łącznie imienia i nazwiska, adresu zamieszkania lub pobytu, numeru PESEL, serii i numeru dowodu osobistego bądź innego dokumentu tożsamości, numeru telefonu oraz innych kategorii danych dotyczących łączących strony umów (np. ID kontraktu, numer umowy, numer dokumentu, numer sprzętowy, numer i kwota faktury VAT, numer konta do wpłat), powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w związku z czym konieczne jest zawiadomienie osoby, której dane dotyczą, o naruszeniu jej danych osobowych”[17]. Takie stanowisko wpisuje się w linię orzeczniczą Prezesa UODO, w której zakłada się konsekwentne uznawanie numeru PESEL za daną osobową o „szczególnym charakterze”[18], co przekłada się na przyjmowanie, że naruszenie poufności danych osobowych obejmujące numer PESEL powoduje powstanie wysokiego ryzyka dla praw i wolności osób, których dane dotyczą. Jako przykład tego rodzaju praktyki można wskazać wcześniejszą decyzję Prezesa UODO o nałożeniu na Towarzystwo Ubezpieczeń i Reasekuracji Warta S.A. administracyjnej kary pieniężnej[19] w wysokości 85.588 zł w związku z obowiązkami dotyczącymi zgłaszania naruszeń bezpieczeństw danych osobowych, w której przyjęto, że „(…) z uwagi na to, że wskazane naruszenie poufności danych dotyczy numerów PESEL wraz z imionami i nazwiskami, adresami zamieszkania, numerami telefonów oraz adresami poczty elektronicznej, to należy uznać, że może ono wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych”.

Poświęcenie tej kwestii kilku stron uzasadnienia decyzji wydaje się co najmniej niecelowe, jako że ukarana Spółka tak właśnie przyjmowała, dokonując zgłoszeń naruszeń

[15] Rejestr dostępny: https://bip.uke.gov.pl/rop/rejestr-operatorow-pocztowych [dostęp: 22.11.2021].
[16] Decyzja, s. 6.
[17] *Ibidem*, s. 15.
[18] Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2019, s. 165, uodo.gov.pl [dostęp: 22.11.2021].
[19] Decyzja z dnia 9 grudnia 2020 r., DKN.5131.5.2020.

bezpieczeństwa danych osobowych, co wprost przyznaje Prezes UODO w uzasadnieniu decyzji, stwierdzając, iż „Spółka wyjaśniła, że mimo to, że uzyskany wynik analizy naruszeń pozwolił określić poziom dotkliwości naruszenia ochrony danych dla osób, których dane dotyczą, jako „niski", Spółka notyfikowała jednak naruszenia, ze względu na wytyczne Prezesa Urzędu Ochrony Danych Osobowych przekazane Spółce w wystąpieniu z dnia (…) września 2018 r. (…), wskazujące na konieczność notyfikowania zdarzeń, które obejmowały nr PESEL, określając ryzyko jako „wysokie"[20]. Co jednak najistotniejsze, ani na gruncie analizowanej decyzji, ani też w treści wcześniejszych dokumentów, Prezes UODO w żaden sposób nie uzasadnia swojego stanowiska o „szczególnym charakterze" numeru PESEL i o wysokim ryzyku, jakie generują naruszenia bezpieczeństwa danych osobowych obejmujące ten numer.

Kluczowe z punktu widzenia postępowania po stwierdzeniu naruszenia bezpieczeństwa danych osobowych jest określenie poziomu ryzyka naruszenia praw i wolności osób fizycznych w wyniku incydentu. Istnieje wiele sposobów postępowania w celu ustalenia poziomu tego ryzyka. W każdym przypadku jednak, zgodnie z zaleceniami zawartymi w motywach 75 i 76 preambuły do RODO, podczas oceny ryzyka zasadniczo należy wziąć pod uwagę zarówno prawdopodobieństwo, jak i powagę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, a ryzyko naruszenia należy oszacować na podstawie obiektywnej oceny. Badając naruszenie, rozpatruje się więc w ujęciu ogólnym prawdopodobieństwo materializacji zagrożenia oraz szkody dla osób, których dane dotyczą, jakie mogą z niego wyniknąć[21]. W tym kontekście stanowisko zajęte przez Prezesa UODO w glosowanej decyzji, zgodnie z którym „dla oceny wysokiego ryzyka naruszenia praw lub wolności osób fizycznych związanego z naruszeniem ochrony danych osobowych nie ma znaczenia, czy to ryzyko się zmaterializuje, a fakt istnienia ryzyka"[22], wymaga pewnego komentarza. Otóż bowiem fakt nieziszczenia się ryzyka w istocie nie ma znaczenia dla oceny jego poziomu w kontekście naruszenia bezpieczeństwa danych osobowych – przedmiotem badania przez administratora powinien być stopień prawdopodobieństwa wystąpienia skutku w postaci ryzyka naruszenia praw i wolności osoby, której dane dotyczą[23]. Jednocześnie jednak nie można zgodzić się z twierdzeniem, że dla oceny wysokiego ryzyka naruszenia praw lub wolności osób fizycznych związanego z naruszeniem ochrony danych osobowych wyłączne znaczenie ma fakt istnienia ryzyka – ponieważ w ten sposób pomija się drugi, poza powagą ryzyka, element istotny przy ocenie poziomu ryzyka, mianowicie prawdopodobieństwo wystąpienia zdarzenia, które skutkuje ryzykiem.

---

[20] Decyzja, s. 12.

[21] Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, wersja 1.0, czerwiec 2019, s. 13, uodo.gov.pl [dostęp: 22.11.2021].

[22] Decyzja, s. 14.

[23] P. Barta, M. Kawecki, P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021, s. 352; podobnie W. Chomiczewski [w:] E. Bielak-Jomaa, D. Lubasz, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 711.

Tak jak konsekwentnie Prezes UODO łączy naruszenia bezpieczeństwa danych osobowych obejmujące numer PESEL z wysokim ryzykiem dla praw i wolności osób, których dane dotyczą, tak samo konsekwentnie organ nadzorczy nie uzasadnia swojego stanowiska. Zamiast tego przytaczane są wyłącznie potencjalne konsekwencje, jakie mogą się wiązać z takim naruszeniem – wskazuje się następujące, typowe zagrożenia dla praw i wolności osób, których dane dotyczą:

- uzyskanie przez osoby trzecie kredytów w instytucjach pozabankowych, na szkodę osoby, której dane dotyczą;
- uzyskanie dostępu do danych o stanie zdrowia osoby, której dane dotyczą w przypadku przełamania zabezpieczeń do systemu świadczeń opieki zdrowotnej lub korzystania ze świadczeń opieki zdrowotnej przysługujących tej osobie;
- korzystanie z praw obywatelskich osoby, której dane naruszono, np. wykorzystanie danych do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego;
- zarejestrowanie przedpłaconej karty telefonicznej (pre-paid), która może posłużyć do celów przestępczych;
- wyłudzenie ubezpieczenia lub środków z ubezpieczenia;
- zawarcie umów cywilnoprawnych, np. najmu nieruchomości;
- posłużenie się fałszywymi danymi, np. przy otrzymywaniu mandatu[24].

Wszystkie te przypadki można określić zbiorczo mianem przypadków kradzieży tożsamości, a więc przestępstwa, które polega na wykorzystaniu danych osobowych innej osoby, podszywającej się pod tę osobę poprzez posłużenie się nimi[25].

Zjawisko braku uzasadnienia tezy o wysokim poziomie ryzyka dla praw i wolności osób, których dane dotyczą, jakie powstaje na skutek naruszeń bezpieczeństwa danych osobowych obejmujących numer PESEL, na gruncie glosowanej decyzji[26] przybiera postać oznajmującego stwierdzenia „Prezes UODO uznał". Tymczasem w literaturze dostępne są już analizy tego problemu, które wskazują na zgoła odmienne wnioski w zakresie poziomu ryzyka. W szczególności podnosi się, że prawdopodobieństwo popełnienia przestępstwa kradzieży tożsamości w wyniku naruszenia bezpieczeństwa danych osobowych obejmującego numer PESEL wynosi nie więcej, niż 0,17% i jest to z założenia wartość zawyżona przez brak możliwości oszacowania wpływu na nią takich czynników, jak choćby masowa publiczna dostępność numerów PESEL np. w Krajowym Rejestrze Sądowym[27]. Oczywiście na gruncie analizowanej decyzji istotne znaczenie dla oceny prawdopodobieństwa ziszczenia się ryzyka dla praw i wolności osób, których dane dotyczą, ma także zakres danych osobowych, które były przedmiotem

[24] Obowiązki administratorów związane z naruszeniami ochrony danych osobowych…, s. 17.

[25] J. Grabowska, A. Kaczmarczyk, *Kradzież tożsamości z art. 190a § 1 K.K. obowiązującego kodeksu karnego*, „Kortowski Przegląd Prawniczy" 2016 nr 4, s. 86.

[26] Co nie przeszkadza Prezesowi UODO czynić zarzutu pod adresem ukaranej spółki, jakoby ta „w swych wyjaśnieniach podkreślała jedynie, że dokonała oceny zgodnie z metodą ENISA, nie wskazując jednocześnie dodatkowego uzasadnienia przyjętych przez siebie kryteriów oceny ryzyka" (Decyzja, s. 15).

[27] P. Litwiński, *PESEL, wyciek danych i ryzyko*, „Rzeczpospolita" z dnia 25 maja 2021 r.; szczegółowe rozważania na ten temat wraz z opisem zastosowanej metody badawczej i jej wyników zostaną opublikowane przez autora w czasopiśmie „ABI Expert" 2021, nr 3 (tekst złożony do druku).

naruszenia. Słusznie więc zwraca uwagę Prezes UODO, że „metoda ENISA (metoda używana do szacowania poziomu ryzyka związanego z naruszeniem) wskazuje, że ostateczna wartość punktowa dla kontekstu przetwarzania (KPD) (obrazująca poziom ryzyka) może być zwiększana bądź zmniejszana w zależności od wystąpienia różnych czynników, m.in. szerokiego zakresu danych dla jednej osoby, charakteru danych czy możliwych negatywnych skutków dla podmiotu danych oraz skali naruszonych danych (dla tej samej osoby)"[28]. Poza tak ogólnym – i przez to prawdziwym – stwierdzeniem, w decyzji brak jest jednak jakiegokolwiek konkretu obrazującego, czy tok rozumowania Prezesa UODO, prowadzący do kategorycznego wniosku przytoczonego wyżej, czy w szczególności uzasadniającego przyjęcie w tym konkretnym przypadku, że taki a nie inny zakres danych spowodował powstanie wysokiego ryzyka dla praw i wolności osób dotkniętych naruszeniem.

Obowiązek sporządzenia uzasadnienia decyzji administracyjnej nakazuje sporządzać to uzasadnienie w taki sposób, aby strony znały argumenty i przesłanki podejmowania decyzji[29]. Tymczasem, w niniejszej sprawie jest dokładnie odwrotnie – teza organu nadzorczego w zakresie poziomu ryzyka jest znana, zaś argumenty ją potwierdzające – nie.

Administrator i przetwarzający w kontekście naruszeń bezpieczeństwa danych osobowych

Zakładając, że w glosowanej decyzji prawidłowo został ustalony stan faktyczny, wypada przejść do tego, co może stanowić jej największą wartość, mianowicie do problemu współpracy pomiędzy administratorem danych a przetwarzającym, w kontekście naruszeń bezpieczeństwa danych osobowych.

Obowiązki związane z naruszeniami bezpieczeństwa danych, o których mowa w art. 33 i 34 RODO, są obowiązkami administratora danych[30]. W przypadku powierzenia przetwarzania danych osobowych, jeżeli do naruszenia bezpieczeństwa doszło w organizacji podmiotu przetwarzającego, administrator danych może wykonać swoje obowiązki o tyle tylko, o ile otrzyma stosowną informację od przetwarzającego. Ten aspekt współpracy pomiędzy administratorem a przetwarzającym znalazł wyraz w art. 28 ust. 3 lit. e RODO, zgodnie z którym przetwarzający powinien pomagać administratorowi wywiązać się m.in. z obowiązku zgłaszania naruszenia ochrony danych osobowych (art. 33 RODO) oraz z obowiązku zawiadamiania osób, których dane dotyczą, o naruszeniu ochrony danych (art. 34 RODO). Wykonując ten obowiązek,

[28] Decyzja, s. 15.

[29] J. Zimmermann, *Glosa do wyroku NSA z 19 czerwca 1997 r., V SA 1512/96*, OSP 1998, z. 2, poz. 29.

[30] W literaturze określa się administratora danych mianem „głównego adresata" tych obowiązków, jednocześnie przyjmując, że obowiązki przetwarzającego ograniczają się do zgłoszenia naruszenia administratorowi danych – zob. K. Wygoda [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 364.

przetwarzający powinien uwzględniać nie tylko charakter przetwarzania, ale również dostępne mu informacje, tj. informacje, w których jest posiadaniu, lub które, ze względu na zakres wykonywanych czynności przetwarzania, może uzyskać[31]. Ponieważ obowiązek pomagania administratorowi jest własnym obowiązkiem przetwarzającego, który wynika wprost z przepisów RODO, umowa powierzenia nie powinna powielać przepisów RODO, ale powinna zawierać szczegółową informację, jak procesor powinien pomagać administratorowi w spełnieniu wskazanych tam obowiązków[32].

Naruszenie bezpieczeństwa danych osobowych należy zgłosić Prezesowi UODO niezwłocznie, nie później jednak, niż w ciągu 72 godzin po jego stwierdzeniu przez administratora danych (art. 33 ust. 1 RODO). W decyzji zawarto szczegółowe informacje na temat statystyk terminowości zgłaszania naruszeń przez ukaraną Spółkę. I tak wskazuje się, że spośród zgłoszeń dokonanych w czerwcu 2020 r., „60% ogólnej liczby naruszeń (…) zostało zidentyfikowanych przez Spółkę powyżej 60 dni od daty zdarzenia powodującego naruszenie, zaś ponad 33% ogólnej liczby zgłoszeń stanowiły zdarzenia zidentyfikowane przez Spółkę powyżej 90 dni od daty zdarzenia". Z kolei spośród zgłoszeń dokonanych w lipcu 2020 r., „ponad 44% ogólnej liczby zgłoszeń stanowią naruszenia zidentyfikowane powyżej 60 dni od daty zdarzenia powodującego naruszenie, zaś 15% ogólnej liczby zgłoszeń stanowiły zdarzenia zidentyfikowane przez Spółkę powyżej 90 dni od daty zdarzenia powodującego naruszenie"[33]. Przyjęto również, że takie terminy dokonywania zgłoszeń wynikają z terminów przekazywania stosownych informacji przez firmę kurierską, które zostały wydłużone w ocenie ukaranej Spółki przez trwającą pandemię koronawirusa[34]. Natomiast Prezes UODO nie dał wiary wyjaśnieniom Spółki dotyczącym wpływu pandemii koronawirusa na terminowość wykonywania obowiązków związanych ze zgłaszaniem naruszeń bezpieczeństwa danych osobowych: „Zgromadzony materiał dowodowy nie mógł potwierdzić również dodatkowych wyjaśnień Spółki, że »istotny wpływ na terminowość zgłoszeń naruszeń danych osobowych dotyczących niniejszego postępowania Urzędu, dotyczących weryfikacji poprawności obsługi procesu dokumentów zwrotnych, miał okres trwającej pandemii«, ponieważ 60% ogólnej liczby naruszeń ochrony danych osobowych zgłoszonych w czerwcu 2020 r. zostało zidentyfikowanych przez Spółkę powyżej 60 dni od daty zdarzenia powodującego naruszenie, zaś ponad 33% ogólnej liczby zgłoszeń stanowiły zdarzenia zidentyfikowane przez Spółkę powyżej 90 dni od daty zdarzenia, tj. zdarzenia sprzed ogłoszenia stanu pandemii"[35]. Nie oceniając prawidłowości takiej a nie innej oceny dowodów w realiach tej sprawy, podkreślić jednak należy, że stan trwającej pandemii miał bez wątpienia wpływ na wykonywanie obowiązków związanych z naruszeniami bezpieczeństwa danych osobowych. Według danych pozyskanych przez autora w trybie dostępu do informacji publicznej, w I kwartale 2020 r.,

[31] P. Barta, M. Kawecki, P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych*…, s. 324.
[32] Wytyczne Europejskiej Rady Ochrony Danych 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO, s. 37, https://uodo.gov.pl/pl/414/1714 [dostęp: 22.11.2021].
[33] Decyzja, s. 20.
[34] *Ibidem*, s. 4.
[35] *Ibidem*, s. 5.

a więc w okresie poprzedzającym gwałtowny rozwój w Polsce pandemii, Prezesowi UODO zgłoszono 2016 przypadków naruszeń, podczas gdy w II kwartale 2020 r., czyli w czasie tzw. lockdownu, masowej pracy zdalnej[36] i skokowego wzrostu popularności usług kurierskich[37], tych naruszeń zgłoszono 1656. Jak się wydaje, tak istotny spadek liczby zgłaszanych naruszeń nie wiąże się ze wzrostem bezpieczeństwa przetwarzanych danych w czasie pandemii, a wręcz odwrotnie, ze spadkiem tegoż, na skutek masowego przechodzenia na pracę zdalną, do której organizacje nie były przygotowane, co mogło skutkować utratą kontroli nad procesami przetwarzania danych osobowych.

W opinii Grupy Roboczej Art. 29 (przejętej przez Europejską Radę Ochrony Danych), przyjmuje się, że administrator „stwierdził" wystąpienie naruszenia w momencie, w którym uzyskał wystarczającą dozę pewności co do tego, że doszło do wystąpienia incydentu bezpieczeństwa, który doprowadził do ujawnienia danych osobowych[38]. Skoro więc ukarana Spółka nie wiedziała o naruszeniu, nie mogła dokonać jego zgłoszenia – słusznie więc na gruncie niniejszej sprawy nie zarzucono Spółce dokonywania zgłoszeń z naruszeniem terminów wskazanych w RODO. Jednocześnie jednak przyjęto, że „brak szybkiej reakcji ze strony podmiotu przetwarzającego nie zdejmuje jednak z administratora odpowiedzialności za stwierdzenie naruszenia ochrony danych osobowych, bowiem zdolność do m.in. wykrywania naruszeń powinna być postrzegana jako kluczowy element środków technicznych i organizacyjnych, w tym każdej polityki w zakresie bezpieczeństwa danych"[39]. O ile bowiem w przypadku, gdy do naruszenia dochodzi w organizacji podmiotu przetwarzającego, administrator danych nie ma faktycznej możliwości dowiedzenia się o naruszeniu bez współpracy ze strony przetwarzającego, o tyle jednak to na administratorze ciążą takie obowiązki, jak:

- obowiązek korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą (art. 28 ust. 1 RODO);
- obowiązek dokonywania zgłoszeń naruszeń w terminie wynikającym z przepisów RODO.

Zwłaszcza ten pierwszy obowiązek ma kluczowe znaczenie dla prawidłowego funkcjonowania relacji pomiędzy administratorem danych a przetwarzającym. Jego treścią jest nakaz skierowany do administratora danych, aby korzystał z usług wyłącznie takich przetwarzających, którzy zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków

[36] W końcu czerwca 2020 r. udział osób, które pracowały zdalnie w związku z sytuacją epidemiczną w ogólnej liczbie pracujących objętych badaniem „Popyt na pracę", wyniósł 10,2%, a w województwie mazowieckim sięgnął niemal 25% – dane za opracowaniem Głównego Urzędu Statystycznego: Wpływ epidemii COVID-19 na wybrane elementy 10.09.2020 r. rynku pracy w Polsce w II kwartale 2020 r., stat.gov.pl [dostęp: 22.11.2021].

[37] W 2020 r. liczba przesłanych paczek wzrosła o 34,8%, a rynek usług kurierskich wzrósł o 22% w porównaniu do 2019 r., https://trans.info/pl/rynek-kurierski-w-polsce-rosnie-dwucyfrowo-wzrost-jeszcze-przyspieszy-227511 [dostęp: 22.11.2021].

[38] Wytyczne WP 250 rev. 01, s. 12, https://www.uodo.gov.pl/pl/3/1345 [dostęp: 22.11.2021].

[39] Decyzja, s. 18.

technicznych i organizacyjnych odpowiadających wymogom RODO, w tym wymogom bezpieczeństwa przetwarzania (zob. motyw 81 preambuły do RODO).

Jak wskazała Europejska Rada Ochrony Danych, obowiązek korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków, ma charakter obowiązku stałego, trwającego przez cały czas przetwarzania danych przez przetwarzającego w imieniu administratora[40]. W konsekwencji, administrator danych powinien weryfikować w odpowiednich odstępach czasu, czy przetwarzający daje takowe gwarancje, w tym poprzez przeprowadzanie audytów i inspekcji. I jeżeli administrator danych uzyska informacje o tym, że po stronie przetwarzającego dochodzi do naruszeń bezpieczeństwa danych osobowych, zwłaszcza o charakterze powtarzającym się, wówczas powinien podjąć działania zmierzające do weryfikacji, czy powierzenie przetwarzania danych temu konkretnemu podmiotowi w dalszym ciągu spełnia wymagania z art. 28 ust. 1 RODO, a więc czy przetwarzający w dalszym ciągu zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą (zakładając oczywiście, że takie gwarancje dawał z chwilą nawiązywania stosunku powierzenia). Jak się wydaje, nie można w tym kontekście mówić o „nadzorze" administratora danych osobowych nad przetwarzaniem danych w jego imieniu przez przetwarzającego, jak czyni to Prezes UODO[41], jako że nadzór oznacza – prócz uprawnień kontrolnych – także możliwość wywierania wpływu na działalność podmiotu nadzorowanego[42]. Jest tak dlatego, ponieważ w art. 28 ust. 3 lit. a RODO przyjęto, że przetwarzający może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie administratora – przetwarzać, a więc wykonywać operacje na danych osobowych, które wykonuje w imieniu administratora danych. Tymczasem zastosowanie konkretnych środków zabezpieczenia danych osobowych nie jest jako takie operacją przetwarzania i nie może być objęte poleceniem administratora, o którym mowa w art. 28 ust. 3 lit. a RODO[43]. Co więcej, obowiązek stosowania przez przetwarzającego odpowiednich środków zabezpieczenia danych osobowych jest jego własnym obowiązkiem, na co wprost wskazuje art. 28 ust. 3 lit. c RODO. Z pewnością natomiast należy wymagać reakcji ze strony administratora danych na informacje o naruszeniach bezpieczeństwa danych osobowych, do których dochodzi po stronie przetwarzającego i podjęcia działań zmierzających do sprawdzenia, czy przetwarzający należycie chroni powierzone dane osobowe.

---

[40] Wytyczne Europejskiej Rady Ochrony Danych 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO, s. 30.

[41] Decyzja, s. 22.

[42] Zob. np. definicja nadzoru autorstwa W. Dawidowicza, zgodnie z którą nadzór to "właściwość organu nadrzędnego do wywierania wpływu na działalność organu podporządkowanego" (W. Dawidowicz, *Zagadnienia ustroju administracji państwowej w Polsce*, Warszawa 1970, s. 34).

[43] Zobowiązanie do stosowania przez przetwarzającego środków zabezpieczenia danych osobowych wskazywanych przez administratora danych może wynikać z umowy łączącej strony, jednakże wtedy inna będzie jego natura (cywilnoprawna, nie zaś publicznoprawna), a stosowanie tego rodzaju rozwiązania w praktyce kontraktowej nie jest zjawiskiem powszechnym i zależy od wielu czynników, w szczególności od ew. przewagi kontaktowej administratora danych.

Niewątpliwie jedną z form sprawdzenia będzie audyt przeprowadzony przez administratora danych w organizacji podmiotu przetwarzającego[44].

Jeżeli administrator danych, w wyniku podjętych czynności uzna, że naruszenia bezpieczeństwa danych osobowych, do których dochodzi w organizacji podmiotu przetwarzającego, można wyeliminować, wówczas winien podjąć odpowiednie działania, które do tego doprowadzą: przewidziane umową lub dążąc do zmiany umowy. Jeżeli natomiast administrator danych uzna, że przetwarzający nie zapewnia już gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, w szczególności gdy ten odmawia podjęcia działań naprawczych lub zmiany umowy, jeżeli zachodzi taka konieczność, wówczas winien zakończyć korzystanie z jego usług, jako że takie przetwarzanie przestałoby spełniać warunek, o którym mowa w art. 28 ust. 1 RODO.

Co tak naprawdę wynika z decyzji ws. Cyfrowego Polsatu?

Pomijając wskazane wyżej naruszenia przepisów o postępowaniu, które w ocenie autora miały bardzo istotny wpływ na treść rozstrzygnięcia, wnioski, do których – na gruncie przepisów prawa materialnego – dochodzi Prezes UODO w glosowanej decyzji, zasługują na aprobatę. Wnioski te można w istocie sprowadzić do jednego, choć długiego, stwierdzenia, a mianowicie, że korzystanie przez administratora danych z usług podmiotu przetwarzającego, także będącego wysokiej klasy profesjonalistą, nie zwalnia tegoż administratora z ciągłego monitorowania przestrzegania przez przetwarzającego przepisów o ochronie danych osobowych i reagowania na stwierdzone nieprawidłowości, z zakończeniem stosunku powierzenia włącznie, jeżeli administrator uzna, że przetwarzający zaprzestał zapewniania gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Jeżeli administrator danych tego obowiązku nie wypełnia, wówczas narusza ciążący na nim prawny obowiązek zapewnienia bezpieczeństwa danych osobowych przetwarzanych w jego imieniu przez przetwarzającego. Takie spojrzenie na obowiązki administratora danych stanowi konsekwencję postrzegania ochrony danych osobowych jako procesu o charakterze ciągłym, którego nie można sprowadzić do jednorazowej czynności, czyli – do wyboru przetwarzającego i zawarcia z nim odpowiedniej umowy. Jednocześnie nie sposób nie zauważyć, że niewyjaśnienie statusu firmy kurierskiej z perspektywy przepisów o ochronie danych osobowych stanowi największą wadę glosowanej decyzji – jest to

[44] Prezes UODO w uzasadnieniu decyzji z 17 grudnia 2020 r., DKN.5130.1354.202, o nałożeniu kary na ID Finance Poland Sp. z o.o. uznał, że m.in. audyt RODO przeprowadzony w tej spółce będącej przetwarzającym dowodził braku naruszenia przez administratora art. 28 ust. 1 RODO – zob. P. Barta, M. Kawecki, P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych*…, s. 314.

stracona szansa na wyjaśnienie wątpliwości z tym związanych, zwłaszcza że w przeszłości zdarzały się sprzeczne ze sobą rozstrzygnięcia, które przytoczono wyżej.

Literatura

Bielak-Jomaa E., Lubasz D., *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Dawidowicz W., *Zagadnienia ustroju administracji państwowej w Polsce*, Warszawa 1970.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Gaj M., Laprus-Bałuka T., Zaborowska A., *Prawo pocztowe. Komentarz*, Warszawa 2017.

Grabowska J., Kaczmarczyk A., *Kradzież tożsamości z art. 190a § 1 K.K. obowiązującego kodeksu karnego*, „Kortowski Przegląd Prawniczy" 2016, nr 4, s. 86.

Litwiński P., *PESEL, wyciek danych i ryzyko*, „Rzeczpospolita" z dnia 25 maja 2021 r.

Litwiński P., *Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku Trybunału Sprawiedliwości z 19.10.2016 r. w sprawie C-582/14 Patrick Breyer*, EPS 2017, nr 5.

Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. M. Sakowska-Baryła, Warszawa 2018.

Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, red. P. Litwiński, Warszawa 2021.

Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2019, uodo.gov.pl [dostęp: 22.11.2021].

Styczyński J., *Nierejestrowane przesyłki kontrowersyjne w świetle RODO*, „Dziennik Gazeta Prawna" z dnia 2 lipca 2019 r.

Zimmermann J., *Glosa do wyroku NSA z 19 czerwca 1997 r., V SA 1512/96*, OSP 1998, z. 2, poz. 29.

Streszczenie

Paweł Litwiński

Naruszenia bezpieczeństwa danych osobowych przez firmy kurierskie

Decyzja Prezesa UODO z 22 kwietnia 2021 r. dotyczy naruszeń bezpieczeństwa danych osobowych, do których dochodziło w związku z korzystaniem z usług firm kurierskich. Sedno decyzji można sprowadzić do stwierdzenia, że korzystanie przez administratora danych z usług podmiotu przetwarzającego nie zwalnia tego administratora z konieczności ciągłego monitorowania przestrzegania przez przetwarzającego przepisów o ochronie danych osobowych i reagowania na stwierdzone nieprawidłowości. To reagowanie w skrajnych przypadkach może przybrać postać zakończenia stosunku powierzenia, jeżeli administrator uzna, że przetwarzający zaprzestał zapewniania gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Jeżeli administrator danych tego obowiązku nie wypełnia, wówczas narusza ciążący na nim obowiązek zapewnienia bezpieczeństwa danych osobowych przetwarzanych w jego imieniu przez przetwarzającego.

Słowa kluczowe: ochrona danych osobowych, RODO; administrator; przetwarzający; administracyjna kara finansowa, kurier, naruszenie danych.

Summary

Paweł Litwiński

Personal Data Breaches by Courier Companies

The decision of the President of the Personal Data Protection Office of April 22, 2021 concerns breaches of the security of personal data that occurred in connection with the use of courier services. The essence of the decision can be boiled down to the statement that that the use of the processor's services by the data controller does not release the controller from the necessity to constantly monitor the processor's compliance with the provisions on the personal data protection law and to react to identified violations. If the controller finds that the processor has ceased to provide guarantees for the implementation of appropriate technical and organizational measures so that the processing complies with the requirements of the GDPR, processing by the processor shall be terminated. If the data controller does not fulfill this obligation, then he breaches his obligation to ensure the security of personal data processed by the processor on his behalf.

Keywords: personal data protection; GDPR; controller; processor; administrative fine; courier; data breach.

Varia

Wojciech R. Wiewiórowski
Uniwersytet Gdański
wojciech.wiewiorowski@ug.edu.pl
ORCID: 0000-0003-2340-772X

Kalendarium wydarzeń związanych z wdrażaniem reformy ochrony danych osobowych w UE

2016

27 kwietnia 2016 r. – formalne przyjęcie tekstu RODO oraz Dyrektywy LED przez Parlament Europejski i Radę.

24 maja 2016 r. – **wejście w życie RODO i Dyrektywy LED** w dwadzieścia dni po ich opublikowaniu w Dzienniku Urzędowym UE.

12 lipca 2016 r. – decyzja wykonawcza Komisji (UE) 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA **(zob. artykuł D.J.B. Svantessona w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

19 października 2016 r. – wyrok TSUE w sprawie Patricka Breyera (C-582/14) – retencja danych telekomunikacyjnych, pojęcie danych osobowych. W 2019 r. P. Breyer wybrany został na posła do Parlamentu Europejskiego.

21 grudnia 2016 r. – wyrok TSUE w sprawie *Tele 2 Sverige AB* (C-203/15) – kluczowe orzeczenie w sprawie dostępu organów ścigania do danych osobowych oraz niezależnego nadzoru nad organami ścigania i służbami specjalnymi.

2017

1 stycznia 2017 – Komisja Europejska przedstawia projekt rozporządzenia statuującego zasady przetwarzania danych osobowych przez instytucje, organy i agencje UE (EUIGDPR).

4 maja 2017 r. – wyrok TSUE w sprawie *Rīgas satiksme* (C-13/16) – pojęcie „konieczności dla potrzeb wynikających z uzasadnionych interesów osoby trzeciej", przekazanie danych osobowych osoby odpowiedzialnej za wypadek drogowy w celu dochodzenia praw przed sądem.

26 lipca 2017 r. – opinia TSUE w sprawie projektu umowy między Kanadą a Unią Europejską w sprawie przekazywania danych dotyczących przelotu pasażera z Unii do Kanady („PNR Kanada") **(zob. artykuł A. Grzelak w niniejszym numerze „Gdańskich Studiów Prawniczych").**

20 grudnia 2017 – wyrok TSUE w sprawie *Nowak przeciwko Irlandii* (C-434/16) – dostęp do własnych danych, pojęcie danych osobowych.

2018

10 maja 2018 r. – nowa ustawa o ochronie danych osobowych.

25 maja 2018 r. – **RODO i Dyrektywa LED stają się w pełni stosowalne**. Pierwsze posiedzenie plenarne Europejskiej Rady Ochrony Danych (EROD) w Brukseli wybiera austriacką rzecznik ochrony danych Andreę Jelinek na przewodniczącą oraz zatwierdza serię osiemnastu wytycznych Grupy Roboczej Artykułu 29, dotyczących interpretacji RODO.

5 czerwca 2018 r. – wyrok TSUE w sprawie *Wirtschaftsakademie Schleswig-Holstein GmbH* (C-210/16) – dezaktywacja strony Facebooka (fanpage'a) pozwalającej na gromadzenie i przetwarzanie pewnych danych dotyczących osób odwiedzających tę stronę.

10 lipca 2018 r. – wyrok TSUE w fińskiej sprawie *Jehovan todistajat* (C-25/17) tzw. „sprawa Świadków Jehowy" – dane wrażliwe, przetwarzanie danych, pojęcie administratora.

2 października 2018 r. – wyrok TSUE w hiszpańskiej sprawie *Ministerio Fiscal* (C-207/16) – pojęcie poważnego przestępstwa stosowane w celu uzyskania przez organy ścigania dostępu do danych retencyjnych.

23 października 2018 r. – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (EUIGDPR).

14 grudnia 2018 r. – ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, wdrażająca do polskiego prawa Dyrektywę LED.

2019

23 stycznia 2019 r. – wchodzi w życie decyzja Komisji Europejskiej, stwierdzająca adekwatny stopień ochrony danych osobowych w Japonii w stosunku do systemu obowiązującego w państwa należących do EOG (pierwsza decyzja o adekwatności wydana pod rządami RODO oraz pierwsza o charakterze wzajemnym) **(zob. artykuł M. Czerniawskiego w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

14 lutego 2019 r. – wyrok TSUE w łotewskiej sprawie *Sergejsa Buividsa* (C-345/17) – kluczowe orzeczenie w sprawie granic przetwarzania danych do celów dziennikarskich oraz styku prawa do prywatności i wolności przetwarzania informacji.

21 lutego 2019 r. – ustawa o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO (tzw. ustawa sektorowa o ochronie danych osobowych).

16 maja 2019 r. – Jan Nowak obejmuje stanowisko Prezesa Urzędu Ochrony Danych Osobowych, jako pierwszy PUODO wybrany pod rządami RODO i nowej ustawy o ochronie danych osobowych.

29 lipca 2019 r. – wyrok TSUE w sprawie *Fashion ID* (C-40/27) – pojęcie administratora, współadministrowanie, pluginy na stronach WWW **(zob. artykuł X. Konarskiego w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

1 września 2019 r. – wyrok TSUE w sprawie *Planet49* (C-40/27) – zgoda na przetwarzanie danych, cookies **(zob. artykuł D. Lubasza oraz glosę M. Miłosza w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

10 września 2019 r. – Prezes Urzędu Ochrony Danych Osobowych (PUODO) wydaje decyzję w sprawie Morele.net, nakładając najwyższą jak dotąd administracyjną karę pieniężną w wysokości 660 tys. euro.

24 września 2019 r. – wyrok TSUE w sprawie *GC i innych przeciwko CNIL* (C-136/17) – prawo do bycia zapomnianym w Google oraz wyrok TSUE w sprawie *Google przeciwko CNIL* (C-507/17) – zasięg terytorialny prawa do bycia zapomnianym.

18 października 2019 r. – PUODO wydaje decyzję w sprawie BIP Aleksandrowa Kujawskiego, nakładając na burmistrza administracyjną karę pieniężną w wysokości 9.380 euro (pierwsza kara pieniężna wobec podmiotu publicznego) **(zob. glosę M.Sakowskiej-Baryły w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

12 listopada 2019 r. – EROD przyjmuje wytyczne 3/2018 w sprawie zakresu terytorialnego RODO (art. 3).

5 grudnia 2019 r. – Wojciech R. Wiewiórowski pierwszym Europejskim Inspektorem Ochrony Danych wybranym na zasadach przewidzianych w EUIGDPR.

2020

22 stycznia 2020 r. – wyrok WSA w Gorzowie Wielkopolskim (II SAB/Go 192/19) –informacja dotycząca czynności, jakie podjął administrator w związku z wejściem w życie RODO, mających na celu ochronę danych osobowych, jest informacją publiczną **(zob. artykuł G. Sibigi w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

30 stycznia 2020 r. – wyrok ETPCz w sprawie *Breyer przeciwko Niemcom* – obowiązek przechowywania danych osobowych użytkowników kart SIM do przedpłaconych telefonów komórkowych i udostępniania ich na żądanie władz, proporcjonalność do uzasadnionych celów ochrony bezpieczeństwa narodowego i zwalczania przestępczości. W 2019 r. P. Breyer wybrany został na posła do Parlamentu Europejskiego.

4 marca 2020 r. – PUODO wydaje decyzję w sprawie zastosowania biometrii wobec uczniów gdańskiej szkoły podstawowej, nie nakładając jednak administracyjnej kary pieniężnej **(zob. glosę A. Mednisa w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

4 maja 2020 r. – EROD przyjmuje wytyczne 5/2020 w sprawie zgody na podstawie RODO.

16 lipca 2020 r. – **wyrok TSUE w sprawie *Schrems II* (zob. artykuł D.J.B. Svantessona w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

11 sierpnia 2020 r. – wyrok NSA (I OSK 224/20) – zgłoszenie naruszenia ochrony danych do organu nadzorczego nie podlega przepisom o dostępie do informacji publicznej **(zob. artykuł G. Sibigi w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

8 września 2020 r. – PUODO wydaje decyzję w sprawie Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie, nakładając administracyjną karę pieniężną w wysokości 11.200 euro.

10–11 listopada 2020 r. w reakcji na orzeczenie *Schrems II* EROD przyjmuje pierwszą wersję wytycznych 1/2020 w sprawie środków, które uzupełniają narzędzia przekazywania danych w celu zapewnienia zgodności z unijnym poziomem ochrony danych osobowych (tzw. *supplementary measures*) i rozpoczyna ich konsultacje, nie wstrzymując jednak stosowania ich przy wydawaniu decyzji przez organy nadzorcze, oraz zalecenia 2/2020 w sprawie podstawowych europejskich gwarancji dotyczących środków nadzoru (tzw. *European Essential Guarantees*).

12 listopada 2020 r. – wyrok WSA w Gorzowie Wielkopolskim (II SA/Go 483/20) –informacja dotycząca czynności, jakie podjął administrator w związku z wejściem w życie RODO, mających na celu ochronę danych osobowych, jest informacją publiczną **(zob. artykuł G. Sibigi w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

7 grudnia 2020 r. – Postanowienie CNIL (francuski organ nadzorczy) w sprawie *Amazon Europe Core* (SAN-2020-013) – administracyjna kara finansowa w sprawie *cookies* **(zob. artykuł X. Konarskiego w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

15 grudnia 2020 r. – EROD przyjmuje wytyczne 6/2020 w sprawie wzajemnego oddziaływania dyrektywy PSD2 i RODO.

2021

5 stycznia 2021 r. – PUODO wydaje decyzję w sprawie Śląskiego Uniwersytetu Medycznego, nakładając administracyjną karę pieniężną w wysokości 5.500 euro.

31 stycznia 2021 r. – wyrok ETPCz w sprawie *Gafiuc przeciwko Rumunii* (59174/13) – cofnięcie akredytacji badawczej z archiwów w związku z nieprzestrzeganiem przez dziennikarza prywatności osób trzecich, obowiązek każdego podmiotu przechowującego dane osobowe do ich ochrony przed nieuzasadnionym ujawnieniem, nawet bez skargi zainteresowanych osób.

11 lutego 2021 r. – PUODO wydaje decyzję w sprawie Krajowej Szkoły Sądownictwa i Prokuratury, nakładając administracyjną karę pieniężną w wysokości 22.200 euro **(zob. glosę E. Bielak-Jomaa w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

16 marca 2021 r. – wyrok WSA w Opolu (II SAB/Op 3/21) – zarówno protokół audytowy, jak i sprawozdanie z audytu mają charakter informacji publicznej **(zob. artykuł G. Sibigi w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

22 kwietnia 2021 r. – PUODO wydaje decyzję w sprawie Cyfrowego Polsatu S.A., nakładając administracyjną karę pieniężną w wysokości 245 tys. euro **(zob. glosę P. Litwińskiego w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

20 maja 2021 r. – rezolucja Parlamentu Europejskiego w sprawie wyroku TSUE z 16 lipca 2020 r. – *Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillianowi Schremsowi* (*Schrems II*) – sprawa C-311/18 (2020/2789(RSP)).

4 czerwca 2021 r. – Komisja Europejska przyjmuje decyzje:

- w sprawie standardowych klauzul umownych dotyczących powierzenia przetwarzania danych osobowych pomiędzy administratorem a podmiotem przetwarzającym oraz
- w sprawie standardowych klauzul umownych dla międzynarodowych transferów danych osobowych.

2 czerwca 2021 r. – Sąd Administracyjny Republiki Słowenii podtrzymuje decyzję słoweńskiego organu nadzorczego, uznając, że prawo do usunięcia danych (tzw. prawo do bycia zapomnianym) nie pozwala osobie fizycznej na żądanie usunięcia danych osobowych z rejestru chrztów prowadzonego przez Kościół katolicki.

18 czerwca 2021 r. – EROD przyjmuje (po zakończeniu konsultacji) finalną wersję zaleceń 1/2020 w sprawie środków, które uzupełniają narzędzia przekazywania danych w celu zapewnienia zgodności z unijnym poziomem ochrony danych osobowych (tzw. *supplementary measures*).

28 czerwca 2021 r. – Komisja Europejska przyjmuje dwie decyzje o adekwatności ochrony danych osobowych przez Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej – po raz pierwszy osobne decyzje na podstawie RODO i dyrektywy LED **(zob. artykuł M. Czerniawskiego w niniejszym numerze „Gdańskich Studiów Prawniczych")**.

6 lipca 2021 r. – British Airways zawarło pozasądową ugodę z ofiarami wycieku danych dotyczącego ponad 420 tys. klientów. Szczegóły ugody nie są znane. Wcześniej Biuro Komisarza ds. Informacji (ICO – brytyjski organ nadzorczy) nałożył na linie lotnicze karę pieniężną wysokości 20 mln funtów za to samo zdarzenie, redukując pierwotnie planowaną sumę 183 mln funtów ze względu na zmianę sytuacji ekonomicznej linii podczas pandemii Covid-19.

22 lipca 2021 r. – Holenderski Urząd Ochrony Danych nałożył na TikTok grzywnę w wysokości 750 tys. euro za naruszenie prywatności dzieci.

7 lipca 2021 r. – EROD przyjmuje wytyczne 7/2020 w sprawie pojęć administratora danych i podmiotu przetwarzającego w RODO oraz wytyczne 4/2021 w sprawie kodeksów postępowania jako narzędzi transferu danych.

12 lipca 2021 r. – pierwsza w historii wiążąca decyzja wydana w trybie pilnym przez EROD – decyzja 1/2021 w sprawie wniosku złożonego na mocy art. 66 ust. 2 RODO przez organ nadzorczy w Hamburgu (Niemcy), dotyczącego nakazania przyjęcia ostatecznych środków w odniesieniu do Facebook Ireland Limited.

20 września 2021 r. – fiński organ nadzorczy uznaje za niezgodne z prawem przetwarzanie szczególnych kategorii danych osobowych podczas próbnego zastosowania technologii rozpoznawania twarzy przez Krajowe Biuro Śledcze Policji. Jednostka

specjalizująca się w zapobieganiu wykorzystywania seksualnego dzieci eksperymentowała z technologią rozpoznawania twarzy w identyfikacji potencjalnych ofiar.

22 października 2021 r. – EROD postanowiła o wdrożeniu pierwszego skoordynowanego działania (na podstawie art. 57 ust. 1 lit. g RODO). Jego celem jest ocena sposobu korzystania przez sektor publiczny w całej UE z usług chmurowych.

Wojciech R. Wiewiórowski
Uniwersytet Gdański
wojciech.wiewiorowski@ug.edu.pl
ORCID: 0000-0003-2340-772X

Computer Privacy and Data Protection – CPDP 2021 "Enforcing Rights in Changing World", Bruksela, 27–29 stycznia 2021 r. (sprawozdanie)

1. Odbywająca się co roku w Brukseli pod koniec stycznia konferencja *Computer Privacy and Data Protection* – CPDP odgrywa szczególną rolę wśród specjalistów od ochrony prywatności i danych osobowych, jako że łączy środowisko akademickie (z którego wywodzą się korzenie konferencji), obecnych w Brukseli polityków oraz urzędników Unii Europejskiej – której prace nad reformą prawa ochrony danych osobowych w ostatnich latach były głównym paliwem dyskusji w skali globalnej – organizacje pozarządowe wszystkich typów, środowiska biznesowe, prawników praktyków oraz indywidualnych ekspertów, z których pomocy korzystają wszystkie wcześniej wymienione podmioty. Jako wiodąca w skali Europy i świata multidyscyplinarna konferencja CPDP oferuje swym uczestnikom możliwość zapoznania się z najnowszymi osiągnięciami w zakresie legislacji, wykładni prawa, praktyki regulacyjnej oraz z dorobkiem akademickim i technologicznym w dziedzinie prywatności i ochrony danych. W atmosferze niezależności, wzajemnego szacunku i – co najważniejsze – żywej dyskusji zarówno pomiędzy uczestnikami paneli, jak i publicznością, która zawsze ma dużo czasu na zadawanie pytań prelegentom, CPDP gromadzi w Brukseli naukowców, prawników, praktyków, decydentów, przemysł i społeczeństwo.

Oczywiście w czasie pandemii konferencja CPDP 2021 – jak wiele innych – przeniosła się z gościnnych Hal Schaerbeeku do internetu. Środowiska akademickie uczelni belgijskich, niderlandzkich i brytyjskich przygotowały specjalną platformę sieciową, która umożliwiała sprawne przeprowadzenie 85 paneli odbywających się w ciągu trzech dni w pięciu równoległych ścieżkach tematycznych, w których wystąpiło ponad 400 mówców. Trudno porównywać liczby uczestników edycji 2021 z wcześniejszymi trzynastoma edycjami tejże konferencji, gdyż czym innym jest wzięcie udziału w konferencji, z którą połączyć się możemy z każdego miejsca na świecie, a czym innym – jak zazwyczaj przybycie do Brukseli i spotkanie się z setkami osób stanowiących absolutny top w naukowej dyskusji o ochronie prywatności na świecie. W konferencji wzięło

w tym roku udział ponad 1300 uczestników z 28 krajów, przy czym 70% uczestników pochodziło spoza Belgii.

Computer Privacy and Data Protection jest platformą naukową o charakterze non-profit, założoną w 2007 r. przez grupy badawcze z dwóch belgijskich uczelni: Vrije Universiteit Brussel (VUB), Uniwersytetu w Namur oraz z niderlandzkiego Uniwersytetu Tilburskiego. Od początku inicjatywie przewodzi Prof. Paul De Hert – współdyrektor *Brussels Privacy Hub* i kierownik Interdyscyplinarnego Departamentu Studiów Prawniczych (DILS-Juri) na stołecznym VUB. W kolejnych latach do platformy dołączył francuski *Institut National de Recherche en Informatique et en Automatique* (INRIA) oraz niemiecki *Fraunhofer Institut für System und Innovationsforschung*. Obecnie platformę prowadzi dwudzieścia akademickich centrów doskonałości z całego świata.

Dobrym świadectwem znaczenia żywej dyskusji prowadzonej podczas tegorocznej edycji CPDP jest fakt, że owe 1300 uczestników konferencji online zapłaciło wpisowe, mimo że wszyscy zdają sobie sprawę z tego, że w kilka miesięcy po konferencji większość 85 wykładów będzie w całości dostępna w nagraniach wideo na stronie konferencji, zaś najważniejsze naukowe prace przygotowane na konferencję opublikowane zostaną w dorocznej publikacji wydawanej przez oksfordzkie *Hart Publishing*. Mimo tego konferencja cieszy się z roku na rok coraz większą rzeszą uczestników, w której istotną rolę odgrywają Polacy. Nasz kraj reprezentowany jest na CPDP zarówno przez środowisko naukowe, jak i organizacje pozarządowe, przedstawicieli najważniejszych instytucji publicznych odpowiedzialnych za kwestie ochrony danych osobowych. Ponadto, Polacy stanowią istotną część prelegentów reprezentujących instytucje europejskie (Komisję Europejską, Radę UE oraz oczywiście biuro Europejskiego Inspektora Ochrony Danych).

2. Główny temat konferencji – "Enforcing Rights in Changing World" – trudno precyzyjnie przełożyć na język polski, jako że sformułowanie „egzekwowanie praw" nie oddaje wszystkich znaczeń angielskiego słowa *enforcement*. Nie ma jednak wątpliwości, że w ponad dwa i pół roku po pełnym rozpoczęciu stosowania ogólnego rozporządzenia o ochronie danych (RODO) najbardziej dyskutowaną i kontrowersyjną kwestią prawną i praktyczną jest działalność decyzyjna regulatorów oraz jej ocena w procedurze kontroli sądowej.

Bardzo trudno omówić tematykę konferencji, na której program składa się z 85 sesji tematycznych przeprowadzonych w ciągu trzech dni. Warto jednak zwrócić uwagę, że poza tematami dość oczywistymi ze względu na ich znaczenie w dyskusji naukowej (np. działalność decyzyjna organów ochrony danych, kontrola sądowa, kary administracyjne, transfer danych do tzw. państw trzecich) oraz kwestiami związanymi z najnowszymi planami legislacyjnymi instytucji europejskich (sztuczna inteligencja) mogliśmy zapoznać się zagadnieniami często wręcz niszowymi. Szeroko omawiano również rozwój prawa i praktyki ochrony prywatności i danych osobowych w innych częściach świata.

Do paneli poświęconych zagadnieniom będącym w jakimś stopniu „na fali" zaliczyć należy przede wszystkim sesję poświęconą zagadnieniu współistnienia prawa

do ochrony danych i innych praw podstawowych, przygotowaną przez Agencję Praw Podstawowych Unii Europejskiej (FRA) oraz Radę Europy. Najważniejszymi sesjami związanymi wprost z tematem głównym konferencji były:

- panel „Likwidacja luki w egzekwowaniu RODO i spojrzenie na model egzekwowania prawa w przyszłości", zorganizowane przez główną Europejską federację konsumencką BEUC z udziałem m.in. dr A. Jelinek – przewodniczącej Europejskiej Rady Ochrony Danych, J. Gonié ze Snap Inc (USA) oraz prof. G. Gonzalez Fuster z VUB oraz
- sesja „Nadzór organów ochrony danych w odniesieniu do dostawców usług IT w chmurze i telekomunikacji" EIOD z udziałem P. van den Berga z niderlandzkiego Ministerstwa Sprawiedliwości i Bezpieczeństwa odpowiedzialnego za umowy o usługi online dla administracji publicznej, A. Barreto Gonzaleza z Kolumbijskiego Urzędu Ochrony Danych, M. Fernández Perez z BEUC oraz A. Edmunds z Biura Kanadyjskiego Komisarza ds. Prywatności.

Druga z wymienionych sesji poświęcona była problematyce podjętej przez tzw. Forum Haskie stworzone w sierpniu 2019 r. przez przedstawicieli administracji publicznych państw członkowskich UE, instytucji europejskich oraz organizacji międzynarodowych. Wszystkie te podmioty mają stałe problemy z wyegzekwowaniem prawidłowych warunków ochrony prywatności w umowach z dużymi graczami internetowymi, takimi jak Microsoft czy Google. W praktyce organy publiczne w UE korzystają z systemów i aplikacji dostarczanych przez duże firmy, często z wbudowanymi funkcjami śledzenia i gromadzenia danych, w oparciu o jednostronnie ustalane warunki.

3. Choć tematyka związana z pandemią COVID-19 była w oczywisty sposób obecna w wielu momentach dyskusji podczas konferencji, niewiele sesji dotykało jej wprost. Swoistym wyjątkiem było omówienie kontrowersyjnej kwestii rejestracji temperatury ciała i dalszego przetwarzania danych o niej dokonywanego w miejscach publicznych, np. przy wejściu do środków komunikacji miejskiej czy do budynków publicznych szkół i uniwersytetów.

Doświadczenia czasu pandemii miały też duży wpływ na dyskusję poświęconą ochronie danych w fazie projektowania i domyślnej ochronnie danych (*data protection by design and by default*). Profesor L. Colonna ze Szwedzkiego Instytutu Badań nad Prawem i Informatyką na Uniwersytecie Sztokholmskim, Athena Bourka z Agencji UE ds. Bezpieczeństwa Cybernetycznego (ENISA), V. Buer z Norweskiego Urzęd Ochrony Danych oraz A. Klabunde (EIOD) rozważali, na ile doświadczenia tworzenia „w trybie przyspieszonym" oprogramowania, baz i systemów informacyjnych na potrzeby walki z pandemią mogą być wykorzystane w dalszym rozwoju praktyki ochrony danych już w fazie projektowania i domyślnej ochrony

4. Choć konferencja CPDP organizowana w Brukseli ze swej natury jest dość europocentryczna, to tematyka wykraczająca poza nasz kontynent jest istotną częścią programu. Do najciekawszych sesji tej edycji konferencji poświęconych zagadnieniom pozaeuropejskim zaliczyć należy sesje poświęcone:

- globalnemu zarządzaniu sztuczną inteligencją z perspektywy czterech kontynentów (Europy, Ameryki Północnej, Południowej i Azji);
- ochronie danych osobowych w Afryce i na Bliskim Wschodzie (z udziałem M. Ouedraogo Bonane – komisarz ochrony danych z Burkina Faso, jej marokańskiego odpowiednika O. Seghrouchni, S. Mohameda – dyrektora organu ochrony danych Dubajskiego Centrum Finansowego, M. Yedaly z Unii Afrykańskiej i T.A. Falconera z Afrykańskiego Centrum Praw Cyfrowych);
- roli OECD w Ameryce Łacińskiej i dynamice konwergencji regulacyjnej w zakresie ochrony danych osobowych w tym regionie oraz
- rewolucji ochrony danych w krajach BRICS (Brazylia, Rosja, Indie, Chiny, RPA).

Lata 2020–2021 to okres stałej aktywności legislacyjnej w zakresie poprawy ochrony danych w Ameryce Południowej i Środkowej, w Afryce i w Azji, wejścia w życie pierwszej brazylijskiej ustawy o ochronie danych (LGPD) i stworzenia Krajowego Urzędu Ochrony Danych (ANPD). W tym samym czasie Rosja wdraża środki intensywnie wykorzystujące sztuczną inteligencję do przetwarzania danych związanych z pandemią. Indie finalizują prace nad nową ustawą o ochronie danych i planują nową architekturę ochrony danych (*Data Empowerment and Protection Architecture* – DEPA). Chiny opublikowały swój projekt ustawy o ochronie danych osobowych i planują globalną inicjatywę na rzecz bezpieczeństwa danych. Płynie również okres *vacatio legis* dla południowoafrykańskiej ustawy o ochronie informacji osobowych (POPIA). Na co dzień większość naukowców i komentatorów patrzy na drugą stronę Atlantyku, gdzie nie tylko w Waszyngtonie, ale również w Kalifornii czy Wirginii dzieje się wiele. Doktor Gabriela Zanfir-Fortuna – rumuńska ekspertka pracująca w Stanach Zjednoczonych dla organizacji *Future Privacy Forum* zaprosiła senatora J. Bomberga, prof. A. Chandera z Uniwersytetu Georgetown, S. Schasser – Zastępcę Prokuratora Generalnego Kalifornii, L. Parnes – byłą dyrektor Biura Ochrony Konsumenta Federalnej Komisji Handlu (FTC) do dyskusji o tym, jak prywatność przeżywa w Stanach Zjednoczonych swój konstytucyjny moment. Krajobraz jest jednak bardzo złożony, a wręcz zagmatwany. Pojawiły się liczne projekty kompleksowych federalnych ustaw, ale jak na razie wydają się wszystkie tkwić w zamrażarkach na Kapitolu. Kalifornia, ojczyzna Doliny Krzemowej, jest liderem w zakresie legislacji z ustawą stanową CCPA i jej unowocześnionej wersji – CPRA – dopiero wchodzącej w życie. Uczestnicy sesji rozważali, czego świat powinien się spodziewać po Amerykanach w przyszłości i jakie są najnowsze inicjatywy w zakresie prawa prywatności na poziomie stanowym i federalnym oraz omawiali paradoks stosunkowo ostrej działalności regulacyjnej FTC mimo stosukowo wąskiej podstawy prawnej

6. Odrębna ścieżka tematyczna poświęcona była zagadnieniom zastosowania rozwiązań algorytmicznych przez organy ścigania i sądy w sprawach karnych. W jej ramach omawiano, w jaki sposób „algorytmy wymiaru sprawiedliwości" mogą obecnie wpływać na decyzje sądowe w sprawach karnych poprzez przewidywanie przyszłych zachowań przestępczych. Jak mogą przyczynić się do oceny oskarżonego poprzez oszacowanie ryzyka ponownego popełnienia przestępstwa (przedstawiano studia nt.

oprogramowania *Compass* stosowanego w Stanach Zjednoczonych), wykorzystując każdy czynnik rzekomo zwiększający dokładność (nie tylko dotychczasowe zachowanie osoby, ale również jej status finansowy, płeć czy wiek). Rozważano, na ile obrońcy mogą być świadomi stosowania takich narzędzi oceny ryzyka i na ile mogą podważyć taką ocenę, nie mając dostępu do kodu źródłowego oprogramownia. Stan zaawansowania takich technologii jest bardzo różny w różnych krajach. Odmienna jest również regulacja, praktyka i skuteczność takich narzędzi (ze swoich punktów widzenia oceny dokonali prof. dr S. Allegrezza i G. Bouchagiar z Uniwersytetu Luksemburskiego, E. Valgaeren z kancelarii STIBBE oraz B. Winters z amerykańskiej organizacji pozarządowej EPIC). Przedstawicielka Komisji Europejskiej (A. Mościbroda) omówiła, na ile UE jest przygotowana do wprowadzenia tych narzędzi do systemu karnego.

Zagadnienia retencji danych telekomunikacyjnych i internetowych wykorzystywanych w postępowaniach karnych był tematem sesji z udziałem dr N. Ní Loideáin (Uniwersytet Londyński), prof. V. Franssen, (ULiège), J. Lotarskiego (Komisja Europejska), C. Vela (hiszpański operator Telefónica), A. Buchty (EIOD) i M. Kopchevy (Rada UE). Od czasu unieważnienia przez TSUE tzw. dyrektywy retencyjnej z 2006 r. (tzw. sprawa *Digital Rights Ireland*), przyjętego z zadowoleniem przez społeczność zajmującą się ochroną danych, policja i organy sądowe oraz niektórzy przedstawiciele doktryny (w Polsce np. prof. A. Gryszczyńska) wyrażają poważne obawy dotyczące wpływu tego kroku na liczne dochodzenia w sprawach karnych. Podczas CPDP dokonano interdyscyplinarnej oceny obecnej sytuacji prawnej, biorąc pod uwagę niedawne dodatkowe rozważania TSUE w orzeczeniu *Privacy International & La Quadrature du Net* z grudnia 2020 r.

Bardzo ciekawą grupę prelegentów zgromadził tiburski instytut TILT odpowiedzialny za sesję poświęconą praktycznemu wykorzystaniu sztucznej inteligencji w nadzorze prowadzonym przez organy państwa oraz związanym z tym wyzwaniami dla prywatności. Obok prof. E. Kosty z Tilburga zasiedli w nim bowiem prof. T. Christakis (Uniwersytet Alpejski w Grenoble), P. Vogiatzoglou (Katolicki Uniwersytet Leuven), L. Houwing ze słynnej hakersko-wolnościowej organizacji *Bits of Freedom* z Niderlandów, Z. Kardasiadou (Komisja Europejska) oraz Ch.Wiese Svanberg z duńskiej policji, która nigdy nie ukrywała, że używa zaawansowanej sztucznej inteligencji oraz algorytmów uczenia maszynowego i uczenia głębokiego, jako że zwiększają one możliwości organów ścigania w zakresie nadzoru. Svanberg, który podczas duńskiej prezydencji w Radzie UE przewodniczył grupie roboczej Rady przygotowującej tzw. policyjną dyrektywę o ochronie danych, w otwarty sposób mówił o zamiarach Duńczyków w tym zakresie, jednocześnie twierdząc, że wszystkie one podlegają stałym konsultacjom społecznym. Podczas panelu omówiono wyzwania, jakie zaawansowana sztuczna inteligencja stawia przed istniejącymi zabezpieczeniami w zakresie ochrony prywatności oraz proponowano sposoby radzenia sobie z nimi w celu zapewnienia skutecznej ochrony prywatności.

Uzgadnianie działalności w tym zakresie z przedstawicielami społeczeństwa, które ma zostać poddane nadzorowi, było też głównym tematem autorskiej sesji przygotowanej przez *spiritus movens* CPDP prof. R. van Brakel, kierującą Katedrą Badań nad Nadzorem btukselskiego VUB. Czy istnieje demokratyczna inwigilacja? Jakie są możliwości

i pułapki czekające na osoby, których dane dotyczą, jeśli stworzymy system, w którym istnieć będzie demokratyczny nadzór nad wykorzystywaniem przez policję technologii inwigilacyjnych? Tym tematem zajęli się podczas ostatniej edycji CPDP prof. A. Hintz (Uniwersytet w Cardiff), Q. Eijkman (Uniwersytet Nauk Stosowanych w Utrechcie), M. Oswald (Komisja Etyki Policji West-Midlands) oraz K. Gorissen reprezentujący belgijski Organ Nadzorczy ds. Zarządzania Informacjami Policyjnymi.

7. Konferencji co roku towarzyszy szereg wydarzeń organizowanych w Brukseli jako imprezy towarzyszące CPDP (*side events*). Najważniejszym z nich był w 2021 r. *Privacy Camp* tradycyjne zorganizowany przez sieć organizacji pozarządowych skupionych wokół inicjatywy EDRi, w której bardzo aktywną rolę odgrywa polska Fundacja Panoptykon. Był on w 2021 r. poświęcony relacjom pomiędzy cyfryzacją, prawami cyfrowymi i infrastrukturą.

8. Należy mieć nadzieję, że kolejna edycja konferencji CPDP odbędzie się w styczniu 2022 r. już w normalnych warunkach w Halach Schaerbeeku, nie zaś online. Konferencja stanie się wówczas okazją dla środowiska zainteresowanego ochroną prywatności i ochroną danych osobowych do świętowania w stolicy UE dziesiątej rocznicy rozpoczęcia prac legislacyjnych nad RODO (25 stycznia 2012 r.) oraz 51. rocznicy wyłożenia do podpisów i ratyfikacji konwencji 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, która do dziś jest jedynym wiążącym międzynarodowym traktatem, który gwarantuje prawo osób fizycznych do ochrony ich danych osobowych (28 stycznia 1981 r.). Wiemy, że prof. P. De Hert i R. van Brekel zapraszają do Brukseli 26–28 stycznia 2022 r. na konferencję zatytułowaną "Data Protection & Privacy in Transitional Times".