ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4050
PRZEGLĄD PRAWA I ADMINISTRACJI CXXV
WROCŁAW 2021

https://doi.org/10.19195/0137-1134.125.18

WOJCIECH RAFAŁ WIEWIÓROWSKI
ORCID: 0000-0003-2340-772X
Uniwersytet Gdański

ADMINISTRATOR I PODMIOT PRZETWARZAJĄCY W USŁUGACH CHMUROWYCH DLA ADMINISTRACJI PUBLICZNEJ. WNIOSKI ZE SPORU MIĘDZY ADMINISTRACJĄ UNIJNĄ A MICROSOFTEM

Abstrakt: Jednym z najbardziej poważnych problemów związanych z prowadzeniem przez administrację publiczną usług elektronicznych w chmurze jest umowne zabezpieczenie praw administratora danych oraz praw osób, których dane są przetwarzane. Współpraca między organami publicznymi w państwach członkowskich UE, instytucjami UE i organizacjami międzynarodowymi przyczyniła się w latach 2019–2021 do zmiany warunków umownych, zabezpieczeń technicznych i domyślnych ustawień serwisów chmurowych tworzonych na podstawie umów między administracją publiczną a najpotężniejszymi twórcami oprogramowania i podmiotami świadczącymi usługi internetowe. W rozdziale omówiono wyniki dochodzenia, które w 2019 roku podjął Europejski Inspektor Ochrony Danych (EIOD) celem oceny prawnych i praktycznych skutków korzystania przez instytucje, organy, urzędy i agencje Unii Europejskiej z produktów i usług Microsoft. Dochodzenie pozwoliło na dokonanie kilku kluczowych ustaleń. Najważniejszym z nich było stwierdzenie, że umowa licencyjna między Microsoftem a instytucjami unijnymi pozwoliła Microsoftowi jednostronnie określać i zmieniać niektóre parametry dotyczące przetwarzania danych w imieniu instytucji oraz zmieniać umowne obowiązki w zakresie ochrony danych. Ocenie poddano również środki techniczne, które Komisja Europejska wprowadziła w celu zahamowania przepływu danych osobowych generowanych przez produkty i usługi Microsoftu — głównie danych telemetrycznych — przesyłanych do tego przedsiębiorstwa. Ocena doprowadziła do wydania ogólnego zalecenia, by wszystkie instytucje UE przeprowadziły testy z zastosowaniem zmienionego i kompleksowego podejścia, podzieliły się wiedzą i rozwiązaniami technicznymi, które opracowały w celu zapobieżenia nieuprawnionemu przepływowi danych do Microsoftu, oraz informowały się wzajemnie o wszelkich problemach związanych z ochroną danych, które identyfikują z produktami lub usługami.

Słowa kluczowe: dane osobowe, administrator, przetwarzający, chmura, elektroniczna administracja

WPROWADZENIE

Wybuch pandemii COVID-19 pozwolił docenić znaczenie poprawnie zarządzanej współpracy między administracją publiczną a dostarczycielami produktów i usług sieciowych, w szczególności takich, które mogą być używane zdalnie na przykład przy zastosowaniu technologii chmurowych. Uwypuklił też potrzebę wprowadzenia skutecznych gwarancji w zakresie ochrony danych i prywatności. Dziś, gdy narzędzia cyfrowe i sieci komunikacyjne są w coraz większym stopniu wykorzystywane do zarządzania kryzysem, w którym się znaleźliśmy, oczekuje się, że pozostaną one z nami dłużej, niż pierwotnie planowaliśmy, a cyfryzacja będzie w nadchodzących latach podstawą naszej pracy[1]. Skutki kryzysu zwiększyły presję na administrację publiczną, by maksymalizowała swoją efektywność[2], co w konsekwencji wpłynęło na prawa i wolności jednostek.

Współpraca między organami publicznymi w państwach członkowskich, instytucjami UE i innymi organizacjami międzynarodowymi ma zasadnicze znaczenie dla zagwarantowania, że umowy o usługi chmurowe zapewniają taki sam poziom ochrony praw osób fizycznych w całym Europejskim Obszarze Gospodarczym (EOG). Zmienione warunki umowne, zabezpieczenia techniczne i ustawienia uzgodnione między niderlandzkim Ministerstwem Sprawiedliwości i Bezpieczeństwa (MSiB NL) a Microsoftem w celu lepszej ochrony praw osób fizycznych pokazują, że istnieje możliwość znacznej poprawy w zakresie opracowywania umów między administracją publiczną a najpotężniejszymi twórcami oprogramowania i podmiotami świadczącymi usługi internetowe.

W tej sytuacji Europejski Inspektor Ochrony Danych (EIOD) podjął w 2019 roku z własnej inicjatywy dochodzenie mające na celu ocenę prawnych i praktycznych skutków korzystania przez instytucje, organy, urzędy i agencje Unii Europejskiej[3] z produktów i usług Microsoft[4]. Ustalenia i zalecenia wynikające z dochodzenia mogą mieć jednak znacznie szersze znaczenie i być odbiciem bardziej generalnego problemu, jakim jest zabezpieczenie umowne praw administratorów

[1] O tym jak trudno przewidzieć drogi tego rozwoju, można jednak przekonać się, czytając przewidywania rozwoju chmur i usług chmurowych w 2020 roku prowadzone na początku poprzedniej dekady przez A. Mateos, J. Rosenberg, *Chmura obliczeniowa. Rozwiązania dla biznesu*, Gliwice 2011, s. 242–243.

[2] K. Schwab, *The Fourth Industrial Revolution*, London 2017, s. 68–69.

[3] W dalszej części niniejszego rozdziału wszystkie te podmioty określane są jako „instytucje unijne" lub „administracja unijna" mimo oczywistych różnic w ich statusie. Prowadzone przez EIOD postępowanie dotyczyło bowiem zarówno Parlamentu Europejskiego czy Trybunału Sprawiedliwości UE, jak i agencji wykonawczych czy poszczególnych dyrekcji w ramach Komisji Europejskiej.

[4] Niniejszy rozdział przygotowano na podstawie dokumentu pt. *EDPS Public Paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services*, podsumowującego dochodzenie EIOD, zob. https://edps.europa.eu/sites/edp/files/publication/20-0702_edps_paper_euis_microsoft_contract_investigation_en.pdf (dostęp: 20.10.2021).

danych oraz — przede wszystkim — praw indywidualnych osób, których dane są przetwarzane, przy umowach zawieranych przez jakiekolwiek podmioty publiczne w państwach członkowskich Unii Europejskiej i Europejskiego Obszaru Gospodarczego z dostawcami usług chmurowych[5]. Regulacja wynikająca z rozporządzenia 2018/1725[6] dotyczącego zasad ochrony danych osobowych w instytucjach unijnych jest bowiem zasadniczo tożsama z tą wynikającą z RODO[7].

Dochodzenie pozwoliło na dokonanie kilku istotnych ustaleń. Najważniejszym z nich było stwierdzenie, że umowa licencyjna między Microsoftem a instytucjami unijnymi pozwoliła Microsoftowi jednostronnie określać i zmieniać niektóre parametry dotyczące przetwarzania danych w imieniu instytucji oraz zmieniać umowne obowiązki w zakresie ochrony danych. Swoboda uznania, jaką dysponował Microsoft, oznaczała w praktyce prawo do działania tak, jakby Microsoft był administratorem danych[8], co uznano za zasadniczo sprzeczne z zasadą, iż instytucja publiczna powinna być jedynym administratorem danych w zakresie, w jakim wykonuje imperium państwa[9] bądź — jak w tym przypadku — organizacji międzynarodowej[10]. Instytucje powinny zawierać z dostawcami usług chmurowych kompleksowe umowy umożliwiające im zachowanie pozycji administratora i dokumentujące polecenia instytucji UE dla podmiotów prze-

[5] Zob. A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018, s. 376–378. O różnicy między pojęciami „dostawca chmury" i „dostawca usług chmurowych" W. Wiewiórowski, *Prawne aspekty udostępniania usług administracji publicznej w modelu chmury*, [w:] *Internet — Cloud computing. Przetwarzanie w chmurze*, red. G. Szpor, Warszawa 2013, s. 119.

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23.10.2018 roku 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.U. UE L 295, 21.11.2018 r., s. 39–98. Rozporządzenie to jest odpowiednikiem RODO skierowanym do instytucji, organów i jednostek organizacyjnych Unii.

[7] O zasadach dotyczących podobnych kontraktów zawieranych przez instytucje publiczne piszą W Kuan Hen, Ch. Millard, I. Walden, *Public Sector Cloud Contracts*, [w:] *Cloud Computing Law*, red. Ch. Millard, Oxford 2013, s. 108–141. Choć praca ta pochodzi sprzed czasów RODO, główne tezy pozostają całkowicie aktualne. Zob. też Ch. Docksey, *Article 24. Responsibility of the controller*, [w:] *The EU General Data Protection Regulation (GDPR). A Commentary*, red. Ch. Kuner, Ch. Docksey, L. Bygrave, Oxford 2020, s. 555–570; oraz w tym samym komentarzu: Ch. Millard, D. Kamarinou, *Article 28. Processor*, s. 598–611.

[8] R. Marchini, *Cloud Computing: A Practical Introduction to Legal Issues*, London 2010, s. 62–63.

[9] A. Krasuski, *Chmura obliczeniowa*…, s. 80–89; *Rozporządzenie UE w sprawie ochrony danych osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018, s. 221–222. Tradycyjnie swoiste podejście do realizacji zadań publicznych przez przetwarzającego dane, ale zasadniczo zgodne z tym postulatem, przedstawia A. Sobczyk, *RODO: rozproszona władza publiczna*, Kraków 2019, s. 129–131.

[10] Zob. W. Wiewiórowski, *Prawne aspekty*…, s. 119.

twarzających[11]. Brak kontroli nad tym, z których podprzetwarzających korzystał Microsoft oraz nieprzyznanie znaczących uprawnień audytorskich były tu głównymi problemami. Instytucje unijne musiały zmierzyć się z wieloma powiązanymi wzajemnie kwestiami dotyczącymi lokalizacji danych, międzynarodowego przekazywania danych i ryzyka ich bezprawnego ujawnienia. Instytucje unijne dysponowały również niewielkimi gwarancjami w zakresie obrony swoich przywilejów i immunitetów.

Ocenie poddano środki techniczne, które Komisja wprowadziła w celu zahamowania przepływu danych osobowych generowanych przez produkty i usługi Microsoftu — głównie danych telemetrycznych — przesyłanych do tego przedsiębiorstwa. Ocena doprowadziła do wydania ogólnego zalecenia, by wszystkie instytucje UE przeprowadziły testy z zastosowaniem zmienionego i kompleksowego podejścia, podzieliły się wiedzą i rozwiązaniami technicznymi, opracowanych przez nie w celu zapobieżenia nieuprawnionemu przepływowi danych do Microsoftu, oraz informowały się wzajemnie o wszelkich problemach związanych z ochroną danych, które identyfikują z produktami lub usługami.

2. MIĘDZYINSTYTUCJONALNA UMOWA LICENCYJNA (ILA)

Umowa ILA, tworząca podstawę stosunków Microsoft z daną grupą instytucji publicznych, w omawianym przypadku z instytucjami unijnymi reprezentowanymi w negocjacjach przez jedną z dyrekcji generalnych[12], ma złożoną strukturę z mnogością powiązanych z sobą dokumentów uzupełniających i modyfikujących się wzajemnie na różne sposoby. Zasadniczo jednak składa się z trzech głównych elementów. Pierwszym z nich jest „parasolowa" umowa licencyjna, która opiera się na wielu standardowych dokumentach licencyjnych, do których instytucje UE wynegocjowały z Microsoftem zestaw dostosowanych zmian[13]. Drugim elementem jest zestaw składający się z kilku zestawów standardowych, wśród których najważniejszą rolę odgrywają warunki dotyczące produktów i warunki usług online. Zbiory standardowych warunków Microsoftu, które zostały włączone do umowy ramowej, są regularnie zmieniane przez Microsoft, a ich nowe wersje publikowane na jego stronie internetowej poświęconej licencjonowaniu. Ustalenie, które części jakiej wersji standardowego dokumentu miały zastosowanie do jakich aspektów danego produktu lub usługi firmy Microsoft, może być tym samym bar-

[11] O przedmiotowym zakresie umów zob. *Rozporządzenie UE w sprawie…*, s. 476–481.

[12] W tym przypadku Dyrekcja Generalna ds. Informatyki (DIGIT), czyli departament Komisji odpowiedzialny za świadczenie usług cyfrowych, które ułatwiają codzienne funkcjonowanie innych działów Komisji oraz instytucji UE i które usprawniają współpracę między organami administracji publicznej w krajach UE.

[13] S. Bradshaw, Ch. Millard, I. Walden, *Standard Contracts for Cloud Services*, [w:] *Cloud Computing Law*…, s. 74–75.

dzo skomplikowane. Na przykład warunki świadczenia usług online różnią się w poszczególnych usługach online w zależności od daty odnowienia lub pierwszego zakupu subskrypcji danej usługi przez danego klienta[14].

Zakres i warunki umowy powodowały, że Microsoft działał *de facto* jako administrator danych. Dodatkowo czynił to w wyjątkowo nieprzejrzysty sposób. Przede wszystkim dotyczyło to prawa do jednostronnej zmiany ustaleń „umownych" oraz braku określenia konkretnych i wyraźnie sprecyzowanych celów przetwarzania. Szczególnie skomplikowanym zagadnieniem była sprawa pierwszeństwa różnych dokumentów umownych. Umowa o partnerstwie instytucjonalnym zawierała szereg przepisów mających wpływ na to, które dokumenty mają pierwszeństwo przed którymi. Niektóre z tych klauzul były z sobą wzajemnie sprzeczne, a dokładny porządek pierwszeństwa był niejednoznaczny. Wiele wskazywało na to, że standardowe dokumenty zmieniane w stosunku do wszystkich klientów miały pierwszeństwo przed wynegocjowanymi warunkami umowy ramowej. W tej sytuacji istniało duże ryzyko, że Microsoft mógłby zmienić cele, dla których przetwarza dane osobowe, lokalizację danych oraz zasady regulujące ujawnianie i przekazywanie danych, bez możliwości współregulowania tego przez instytucje unijne. Taki poziom uznaniowości wykracza poza to, co można przypisać przetwarzającemu — w rzeczywistości czyniąc Microsoft administratorem danych.

Zakres głównych obowiązków Microsoft w zakresie ochrony danych w wynegocjowanych dokumentach ILA został ograniczony do konkretnych rodzajów przetwarzania i kategorii danych. Istniało ryzyko, że niektóre działania związane z przetwarzaniem danych w ramach umowy o partnerstwie instytucjonalnym nie mieszczą się w zakresie wynegocjowanych warunków i korzystają z niższego poziomu ochrony, określonego wyłącznie przez Microsoft. Niektóre kategorie danych gromadzonych i przetwarzanych przez dostawcę usług chmurowych nie podlegały ochronie wynikającej z umowy.

Ocena zasad przyjętych przez kontrahentów dokonana w trakcie dochodzenia pozwoliła wyróżnić cztery kategorie danych osobowych, którym przyznano różne poziomy ochrony na mocy porozumienia międzyinstytucjonalnego. Trudno jednakże powiedzieć, by Komisja Europejska była do końca świadoma tych różnic w traktowaniu poszczególnych kategorii danych. Pierwszą — najbardziej chronioną — kategorią danych osobowych były dane dostarczane z wykorzystaniem usług internetowych.

Druga kategoria obejmowała dane, które nie zostały wprost przekazane spółce Microsoft, ale zostały przez nią zgromadzone podczas korzystania przez instytucje z usług internetowych (na przykład tak zwane dane telemetryczne). Przetwarzanie tych danych było częściowo objęte warunkami świadczenia usług internetowych, a potencjalnie też uzupełnieniem dotyczącym ochrony danych (Data Protection

[14] Dla celów niniejszego uwzględniono wersje standardowych dokumentów ze stycznia 2020 roku. W trakcie dochodzenia przeanalizowano jednak również kilka wcześniejszych wersji.

Addendum). Nie podlegały zaś głównym wynegocjowanym obowiązkom wynikającym z umowy ramowej. Można było dojść do wniosku, że w wypadku danych telemetrycznych (danych o tym, że indywidualny użytkownik w ramach instytucji unijnej użył konkretnej usługi, a nawet otworzył konkretny plik w danym momencie) mamy do czynienia z „tak silną ochroną", że jedynym podmiotem mogącym te dane przetwarzać jest nie sam użytkownik czy instytucja, w której pracuje, lecz właśnie Microsoft. Trzecią kategorią danych były te, które Microsoft uzyskał, gdy instytucje UE korzystały z jego tak zwanych usług profesjonalnych. Zostały one objęte oddzielnym, lżejszym zestawem warunków ochrony danych. Nie były one również objęte głównymi wynegocjowanymi zobowiązaniami umowy ramowej. Przy przetwarzaniu tych trzech kategorii danych firma z Redmond była nie tylko przetwarzającym, ale również administratorem danych.

Ostatnią, czwartą kategorię tworzyły dane dostarczane spółce Microsoft i gromadzone przez nią, gdy instytucje unijne korzystały z produktów i oprogramowania, których Microsoft nie uważał za usługi online. Przetwarzanie danych w tej kategorii nie wchodziło w zakres żadnej z umów dwustronnych, a Microsoft przetwarzał je jako administrator danych. Do tej kategorii należały dane diagnostyczne ze wszystkich wersji systemu Windows oraz z pakietu Office (w tym z wersji Office 2016). Dane diagnostyczne pochodzące z zainstalowanych lokalnie aplikacji pakietu Office 365 ProPlus (na przykład Word, Excel, PowerPoint), które nie były usługami online, również potencjalnie należały do tej kategorii. Zważywszy na wzajemne powiązanie poszczególnych produktów, usług internetowych i usług specjalistycznych, nie było pewności, czy możliwe jest przeniesienie danych należących do najbardziej chronionej kategorii do kategorii mniej chronionej lub odwrotnie.

3. OGRANICZENIE CELU PRZETWARZANIA

Zdaniem EIOD ograniczenie celu w porozumieniu międzyinstytucjonalnym nie było dostatecznie szczegółowe i jednoznaczne[15]. Stwarzało to ryzyko rozbieżności między celami, do których według instytucji unijnych ograniczono przetwarzanie na mocy porozumienia międzyinstytucjonalnego, a celami przez Microsoft

[15] M. Koning, *The Purpose and Limitations of Purpose Limitation*, Nijmegen 2020, s. 62–64 oraz 66–68. Zob. także opinia nr 3/2013 Grupy Roboczej Artykułu 29 (poprzedniczki Europejskiej Rady Ochrony Danych — EROD) w sprawie ograniczenia celu, motywy 15–16, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (dostęp: 20.10.2021) oraz Wytyczne EROD nr 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) RODO w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, wersja 2.0 z 8.10.2019 r., motywy 6–7, tekst polski: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_pl.pdf (dostęp: 20.10.2021).

uważanymi za dozwolone na mocy tegoż porozumienia. Najbardziej wyraźnym określeniem celu w dokumentach umownych było „dostarczanie produktu lub usług profesjonalnych", co wydaje się i tak celem absurdalnie szerokim. Często cel był określony bardzo enigmatycznymi sformułowaniami. Przykładowo, wyjaśniając, czym jest „świadczenie usługi online", odwoływano się do „zapewnienia spersonalizowanych doświadczeń użytkownika". Definicja „świadczenia usługi online" była wystarczająco pojemna, by objąć analitykę danych. Wobec tego nie było jasne, czy dozwolone jest przetwarzanie danych w celach takich jak uczenie maszynowe[16] lub używanie algorytmów sztucznej inteligencji. Nie wiadomo też, na czym miało polegać „rozwiązywanie problemów", „zapewnianie możliwości funkcjonalnych" i „ciągłe doskonalenie" w odniesieniu do poszczególnych usług, szczególnie jeśli „ciągłe doskonalenie" usług zostało opisane jako „zwiększanie wydajności" i „skuteczności" użytkownika.

Jednym z najbardziej niepokojących aspektów porozumienia międzyinstytucjonalnego był fakt, że poziom uznaniowości przyznany Microsoftowi był w dużej mierze dorozumiany. Analiza przeprowadzona w trakcie dochodzenia polegała przede wszystkim na zidentyfikowaniu luk w klauzulach umownych i wyciąganiu konsekwencji z niepewności co do rzeczywistej woli stron.

4. ZALECENIA DLA INSTYTUCJI UNIJNYCH JAKO ADMINISTRATORÓW DANYCH

Zalecenia wynikające z dochodzenia koncentrują się wokół stwierdzenia, że każda instytucja unijna powinna działać jako wyłączny administrator danych osobowych związanych z korzystaniem przez nią z produktów i usług chmurowych w takim zakresie, w jakim sama wykonuje zadania w interesie publicznym lub w ramach sprawowania władzy publicznej. Tak zwana parasolowa umowa licencyjna powinna przewidywać jednoznaczny porządek pierwszeństwa dokumentów umownych. Zmiany, które instytucje wynegocjowały w stosunku do standardowych warunków dostawcy usług chmurowych, powinny zostać włączone do dokumentu umownego najwyższego rzędu. Powinny one zatem zawierać wszystkie przepisy niezbędne do zapewnienia zgodności z rozporządzeniem 2018/1725. Zmiana zobowiązań stron mających wpływ na ochronę danych zawartych w umowie o partnerstwie instytucjonalnym powinna być możliwa jedynie w drodze obopólnego porozumienia. Zakres porozumienia międzyinstytucjonalnego mający wpływ na ochronę danych powinien zostać rozszerzony tak, aby obejmował wszystkie dane osobowe, a nie tylko te dostarczane wprost przez instytucje dostawcy. Również dane osobowe generowane w wyniku korzystania przez

[16] A. Krasuski, *Status prawny sztucznego agenta. Podstawy prawne zastosowania sztucznej inteligencji*, Warszawa 2021, s. 17–20.

instytucje z wszystkich produktów i usług dostawcy, a „pojawiające się" jedynie w systemach dostawcy, powinny być traktowane jako dane osobowe podlegające umowie.

Instytucje unijne powinny również wynegocjować konkretny, wyraźny i wyczerpujący zestaw celów, obejmujący wszystkie rodzaje danych osobowych związanych z korzystaniem przez nie z produktów i usług dostawcy. Cele te powinny być ograniczone do tych, które były niezbędne dla instytucji do korzystania z tych produktów i usług[17]. Inne cele powinny być wyraźnie zabronione.

5. DOSTAWCA USŁUG CHMUROWYCH JAKO PODMIOT PRZETWARZAJĄCY

Ustanowienie instytucji unijnych jedynymi administratorami danych osobowych przetwarzanych na mocy porozumienia międzyinstytucjonalnego wymaga wyraźnego wzmocnienia ich pozycji w umowach z dostawcami produktów i usług chmurowych — takimi jak Microsoft. Wymogi dotyczące umowy między administratorem a podmiotem przetwarzającym są określone w art. 29 rozporządzenia 2018/1725[18]. Rozporządzenie wymaga, by umowa między administratorem a podmiotem przetwarzającym była wiążąca dla podmiotu przetwarzającego i administratora, by określała przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Nie ma zatem możliwości, by podmiot przetwarzający miał nieograniczone prawo do jednostronnej zmiany w umowie z administratorem. Jak wskazano, przetwarzający powinien wykonywać swe działania na danych, na podstawie udokumentowanych poleceń administratora danych[19].

Przy umowach zawieranych przez instytucje unijne nie było jasne, które elementy kontrolne wynikające z umów — jeśli w ogóle którekolwiek — mają zastosowanie do poszczególnych kategorii danych przetwarzanych przez Microsoft na mocy umowy o partnerstwie i współpracy. Choć Microsoft miał obowiązki i prawa, które można przypisać administratorowi danych na mocy porozumienia międzyinstytucjonalnego, obowiązki te nie były wyraźnie określone.

Szczególnie istotny jest tu brak kontroli nad korzystaniem z usług podwykonawców przetwarzania przez Microsoft oraz niestworzenie skutecznych uprawnień do audytu. Instytucje powinny bowiem mieć kompleksową umowę administrator–przetwarzający, obejmującą role i obowiązki obu podmiotów, przedmiot, czas trwania i charakter przetwarzania, rodzaje danych osobowych, których to

[17] M. Koning, *op. cit.*, s. 96–98.

[18] Odpowiednio art. 28 ust. 3 lit. h) RODO, a przed wejściem w życie rozporządzenia 2018/1725 art. 28 poprzedzającego go rozporządzenia nr 45/2001.

[19] Więcej o tej konstrukcji pisze w polskiej literaturze P. Litwiński, [w:] *Rozporządzenie UE w sprawie…*, s. 482–483 oraz 490.

dotyczy, kategorie podmiotów danych, których to dotyczy, obowiązki i prawa administratorów i podmiotów przetwarzających[20]. Rodzaje danych osobowych i kategorie podmiotów danych powinny być określone jak najbardziej szczegółowo, aby zapewnić zgodność z podstawowymi zasadami, takimi jak minimalizacja przetwarzania danych, ograniczenie celu i zgodność przetwarzania z prawem. Udokumentowane polecenia instytucji tworzone na mocy porozumienia międzyinstytucjonalnego powinny obejmować na przykład informacje, jakie rodzaje danych mogą być przetwarzane, kto może mieć do nich dostęp, jak i gdzie są one przechowywane, jakie środki bezpieczeństwa są stosowane, czy zezwala się na przekazywanie danych do państw trzecich[21], a jeśli tak, to do jakich odbiorców, państw i na jakich warunkach.

6. PODPRZETWARZAJĄCY

Od administratorów danych wymaga się, aby zezwalali na przetwarzanie danych w ich imieniu wyłącznie przez podmioty przetwarzające dane gwarantujące ochronę osób, których dane dotyczą. Jako przetwarzający Microsoft może oczywiście zaangażować podprzetwarzającego[22], ale może to uczynić jedynie na podstawie uprzedniej pisemnej zgody administratora danych. Jeśli robi to na podstawie ogólnego pisemnego zezwolenia, musi dać administratorowi istotną możliwość zatwierdzenia wykazu podprzetwarzających w momencie podpisywania ogólnego zezwolenia oraz istotną możliwość wniesienia sprzeciwu wobec wszelkich późniejszych zmian w podprzetwarzających, których angażuje później. Jako przetwarzający Microsoft musi też przekazać umownie swoje obowiązki w zakresie ochrony danych wynikające z umowy licencyjnej swoim podprzetwarzającym. Wśród obowiązków, które należy przekazać, są zobowiązania Microsoftu do wdrożenia środków technicznych i organizacyjnych, uważanych przez administratora danych za konieczne.

Wynegocjowane warunki ochrony danych umieszczone w umowie ramowej zawierały zdaniem przetwarzającego ogólne upoważnienie do angażowania podprzetwarzających. Jednak, podobnie jak wiele obowiązków w zakresie ochrony danych wynikających z umowy ramowej, miała ona zastosowanie wyłącznie do danych osobowych przekazywanych za pośrednictwem usług internetowych, nie zaś innych kategorii danych, opisanych na początku rozdziału. W praktyce informacje na temat nowych podprzetwarzających dostarczane instytucjom unijnym składały się z nazwy podprzetwarzającego, ogólnego rodzaju świadczonej przez

[20] A. Krasuski, *Chmura obliczeniowa…*, s. 539–581.

[21] D. Karwala, *Komercyjne transfery danych osobowych do państw trzecich*, Warszawa 2018, s. 54–58.

[22] *Rozporządzenie UE w sprawie…*, s. 474–476.

niego usługi oraz kraju jego siedziby. Nie wydaje się, by takie informacje były wystarczające. Tworząc system ogólnych upoważnień, który jednocześnie dawałby instytucjom znaczącą możliwość wyrażenia sprzeciwu wobec nowych podprzetwarzających, musiałby obejmować także informacje, jakie rodzaje przetwarzania danych należało powierzyć potencjalnym podprzetwarzającym oraz w odniesieniu do jakich konkretnych produktów i usług byłyby one wykonywane. Istotnym problemem jest również niemożność sprzeciwu, bo jedyną przewidzianą alternatywą dla instytucji unijnej było zakończenie subskrypcji całego pakietu.

7. AUDYT

Zgodnie z art. 29 ust. 3 lit. h) rozporządzenia 2018/1725[23] umowa między administratorem danych a podmiotem przetwarzającym musi zawierać dwa zobowiązania dotyczące podmiotu przetwarzającego. Po pierwsze, podmiot przetwarzający musi udostępnić administratorowi wszystkie informacje, które są niezbędne do wykazania zgodności z całym art. 29 rozporządzenia 2018/1725. Po drugie zaś, podmiot przetwarzający musi poddać się audytom i kontrolom prowadzonym przez administratora danych. W świetle zasady rozliczalności, szczegóły i zakres prawa do audytu opisany w umowie powinny odzwierciedlać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych. Tymczasem wynegocjowane warunki porozumienia międzyinstytucjonalnego powielały jedynie brzmienie obowiązków ustawowych wynikających z art. 29 ust. 3 rozporządzenia 2018/1725. Nie zawierały żadnych szczegółów dotyczących tego, czego instytucje mogą oczekiwać od dostawcy produktów i usług chmurowych w celu ich wypełnienia.

W uzupełnieniach dotyczących ochrony danych osobowych Microsoft co prawda zobowiązał się, że zorganizuje tak zwane audyty bezpieczeństwa, które zostaną przeprowadzane co najmniej raz w roku, a dokonają ich zewnętrzni audytorzy bezpieczeństwa wybrani i opłacani przez Microsoft. Nie wyjaśniono jednak, w jakim stopniu takie audyty bezpieczeństwa obejmowałyby zgodność przetwarzania z zasadami ochrony danych osobowych. EIOD uznał to za istotne przeoczenie. Warto pamiętać, że już w tak zwanym Memorandum z Sopotu[24] z 2012 roku, Grupa Berlińska[25] zaleca poddawanie dostawcy usług chmurowych

[23] Odpowiednio art. 28 ust. 3 lit. h) RODO.

[24] Dokument roboczy w sprawie przetwarzania danych w chmurze obliczeniowej — kwestii ochrony danych i prywatności Memorandum z Sopotu przyjęty przez tak zwaną Grupę Berlińską 24 kwietnia 2012 r., https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2012/2012-WP-Sopot_Memorandum-en.pdf (dostęp: 20.10.2021).

[25] Międzynarodowa Grupa Robocza ds. Ochrony Danych w Telekomunikacji (Grupa Berlińska) została założona w 1983 roku w celu polepszenia ochrony prywatności w sektorze telekomunikacji. Grupę tworzą przedstawiciele organów ochrony danych, krajowych administracji publicznych,

audytowi strony trzeciej, niezależnie od audytu przeprowadzanego przez administratora danych wobec „swoich danych". Każdy audytor kontrolujący dostawcę usług w chmurze powinien być w pełni niezależny od niego[26].

Audyty z dziedziny ochrony danych, które oceniają zgodność z obowiązkami nałożonymi przez rozporządzenie 2018/1725, mają szerszy zakres i stosują inne standardy niż audyty bezpieczeństwa. Ponadto audyty zlecone przez sam Microsoft z zakresem, który audytowany sam wybrał, nigdy nie mogłyby stanowić skutecznej realizacji uprawnień audytowych administratorów danych. Faktem jest, że uzupełnienie dotyczące ochrony danych osobowych zawierało zobowiązanie do „niezwłocznej reakcji" na wszelkie dodatkowe instrukcje dotyczące audytu, „w zakresie, w jakim wymagania klienta dotyczące audytu […] nie mogą być w uzasadniony sposób spełnione za pomocą sprawozdań z audytu, dokumentacji lub informacji dotyczących zgodności, które firma Microsoft udostępnia swoim klientom".

To sformułowanie budzi znaczące wątpliwości. Informacje dostarczone przez Microsoft i audytorów poinstruowanych przez Microsoft mogą co prawda zapewnić instytucjom unijnym pewien poziom pewności, nie mogłyby jednak zastąpić zdolności instytucji unijnych do samodzielnego gromadzenia i sprawdzania dowodów. Nie wystarcza też, by dostawca usług chmurowych „szybko reagował" na instrukcje audytowe instytucji unijnych, jeśli odpowiedzią mogłaby być odmowa zezwolenia na przeprowadzenie kontroli przez instytucje UE, gdyby jej zakres pokrywał się z zakresem własnych kontroli zlecanych przez Microsoft. Ogólnie rzecz biorąc, prawa instytucji unijnych do przeprowadzania audytu na mocy porozumienia międzyinstytucjonalnego, nie były wystarczająco solidne w świetle ryzyka związanego z przetwarzaniem danych[27].

Zrozumiałe jest jednak, że dostawca usług chmurowych prowadzonych na dużą skalę chciałby uniknąć niemożliwej do opanowania liczby różnych audytów przeprowadzanych przez różnych klientów. Rozporządzenie 2018/1725 jednak jasno stanowi, że administratorzy danych muszą mieć możliwość kontrolowania podmiotów przetwarzających i podwykonawców. Powinna istnieć możliwość zorganizowania audytów, które zadowolą wielu klientów jednocześnie.

8. LOKALIZACJA, PRZEKAZYWANIE I UJAWNIANIE DANYCH

Dochodzenie przeprowadzone przez EIOD wykazało, że instytucje unijne nie były w stanie kontrolować lokalizacji dużej części danych przetwarzanych przez

organizacji międzynarodowych oraz naukowcy z całego świata. Od początku lat dziewięćdziesiątych Grupa koncentruje się w szczególności na ochronie prywatności w internecie. Dokumenty przez nią przyjęte dostępne są na stronie https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/ (dostęp: 20.10.2021).

[26] Zob. także W. Wiewiórowski, *Prawne aspekty…*, s. 107–108.

[27] O pojęciu ryzyka *Rozporządzenie UE w sprawie…*, s. 446–448.

dostawców usług chmurowych. Nie miały również pełnej kontroli nad tym, w jaki sposób dane są przekazywane do państw trzecich. Brakowało również odpowiednich zabezpieczeń służących ochronie danych, które „opuściły" obszar Unii i EOG[28]. Instytucje unijne miały też niewielkie szanse zagwarantowania swych przywilejów i immunitetów otrzymanych na mocy Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) oraz tego, że Microsoft nie będzie ujawniał danych osobowych podmiotom trzecim w zakresie, w jakim współpracuje ze służbami specjalnymi i organami ścigania Stanów Zjednoczonych[29].

W chwili zamknięcia dochodzenia przez EIOD w marcu 2020 roku lokalizacja niektórych danych została określona w warunkach świadczenia usług internetowych. Zgodnie z nimi obowiązek przechowywania danych na terytorium unijnym miał zastosowanie jedynie do podzbioru danych dostarczonych w wyniku korzystania z niektórych „podstawowych usług internetowych". Obejmowały one usługi Microsoft Office 365 i niektóre usługi Microsoft Azure. W wypadku usług Office 365 Microsoft zobowiązał się do przechowywania jedynie zawartości skrzynki pocztowej Exchange Online, zawartości witryny SharePoint Online oraz plików przesłanych do OneDrive for Business. Dane dostarczone w wyniku korzystania z innych usług pakietu Office 365 nie zostały uwzględnione, podobnie jak informacje dotyczące tożsamości użytkownika i metadane. W wypadku usług podstawowych Microsoft Azure Core Services, takich jak Azure Active Directory (używanych do zarządzania tożsamością użytkownika w usługach Microsoft Online Services), warunki świadczenia usług online wyraźnie to określały: „Niektóre usługi mogą nie umożliwiać klientowi skonfigurowania wdrożenia w UE/EOG lub poza terytorium Stanów Zjednoczonych i mogą przechowywać kopie zapasowe w innych lokalizacjach".

Jeśli konieczny byłby transfer danych do państw trzecich lub organizacji międzynarodowych, powinien on być oczywiście przeprowadzany przy wykorzystaniu narzędzi prawnych i organizacyjnych opisanych w rozdziale piątym rozporządzenia 2018/1725, po dokonaniu udokumentowanej oceny ryzyka dla praw i wolności osób, których dane dotyczą. Decyzja, czy zezwolić na przekazanie da-

[28] S. Bradshaw, Ch. Millard, I. Walden, *op. cit.*, s. 55–56; oraz D. Karwala, *op. cit.*, s. 176–179. Zob. także Wytyczne EIOD w sprawie stosowania usług chmurowych przez instytucje i ciała UE z 16.3.2018 r., motyw 63, https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf (dostęp: 20.10.2021).

[29] S. Bradshaw, Ch. Millard, I. Walden, *op. cit.*, s. 53–55; I. Walden, *Law Enforcement Access to Data in Clouds*, [w:] *Cloud Computing Law*…, s. 285–310; 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: Transatlantic tensions, EU surveillance, and big data*, red. G. Vermeulen, E. Lievens, Antwerpen 2017, s. 171–192. Prezentowaną przez Microsoft wersję zdarzeń dotyczących gromadzenia przez służby amerykańskie danych klientów swej firmy przedstawia B. Smith, *Tools and Weapons*, London 2019, s. 10–19. Zupełnie inne stanowisko prezentują apologeci E. Snowdena w B. Gellman, *Dark Mirror. Edward Snowden and the Surveillance State*, London 2020, s. 117–150.

nych, należy w takich przypadkach do administratorów danych. Instytucje unijne podpisały umowę o partnerstwie i współpracy z Microsoft Ireland. W kontekście ILA wszelkie zabezpieczenia wprowadzone zgodnie z zasadami międzynarodowego transferu danych miały jak dotąd charakter umowny. Grupa Microsoft nie miała żadnych wiążących zasad korporacyjnych[30], zatwierdzonych w ramach RODO lub w porządku prawnym sprzed 2018 roku.

Zgodnie z uzupełnieniem dotyczącym ochrony danych przez wykonanie międzynarodowego porozumienia o ochronie danych uznano, że instytucje unijne korzystały ze standardowych klauzul umownych dotyczących międzynarodowego przekazywania danych[31], wykorzystywanych przez Microsoft Corporation. W rezultacie instytucje UE miały zarówno bezpośrednią relację z przetwarzającym, mającym siedzibę w UE (Microsoft Ireland), który mógł dokonywać międzynarodowego transferu danych do swoich podprzetwarzających, jak i bezpośrednią relację z Microsoft Corporation jako procesorem mającym siedzibę poza UE/EOG, też mogącym dokonywać dalszego międzynarodowego przekazywania danych do swoich podprzetwarzających. W rozumieniu EIOD zdecydowana większość przetwarzania danych osobowych była w praktyce dokonywana przez Microsoft Corporation, a nie przez Microsoft Ireland. Oba podmioty wykorzystywały oczywiście swoich podprzetwarzających.

Zważywszy na taką matrycę umowną, instytucje unijne potrzebowały dwóch warstw zabezpieczeń umownych. Po pierwsze, musiały one wydawać Microsoft Ireland i Microsoft Corporation polecenia dotyczące zakresu, w jakim dane osobowe mogą być przekazywane do państw trzecich, na jakich warunkach i z zastrzeżeniem jakich gwarancji. Musiały one zostać odzwierciedlone w standardowych klauzulach umownych w wypadku przekazywania danych instytucji unijnych przez Microsoft Corporation. W tym scenariuszu właściwe byłoby wykorzystanie standardowych klauzul umownych przyjętych na mocy art. 48 ust. 2 lit. b) lub c) rozporządzenia (UE) 2018/1725. Takie standardowe klauzule umowne nie zostały jeszcze wydane, ale mogłyby tymczasowo zostać zastosowane przez klauzule przyjęte na mocy decyzji Komisji 2010/87/UE, pod warunkiem uzyskania zezwolenia od EIOD na mocy art. 48 ust. 3 lit. a) rozporządzenia (UE) 2018/1725. Przy każdym rozwiązaniu nie było jednak jasne, czy polecenia instytucji unijnych zawarte w wynegocjowanych dokumentach porozumienia międzyinstytucjonalnego miały być wiążące dla Microsoft Corporation i dla Microsoft Ireland.

Administratorzy danych, którzy chcą korzystać ze standardowych klauzul umownych do przekazywania danych przyjętych przez Komisję Europejską (takich jak klauzule przyjęte na mocy decyzji Komisji Europejskiej 2010/87/UE)[32], muszą uzupełnić załączniki w celu dokładnego określenia przedmiotu, czasu trwa-

[30] D. Karwala, *op. cit.*, s. 234–239.

[31] *Ibidem*, s. 189–224.

[32] Decyzja Komisji z dnia 5 lutego 2010 roku w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane, mającym sie-

nia, charakteru i celu przetwarzania, rodzaju danych osobowych i kategorii osób, których dane dotyczą, oraz środków bezpieczeństwa mających zastosowanie do danych, które są przekazywane. Treść załączników powinna być dostosowana do każdego produktu i usługi oraz do każdego odbiorcy (w tym podwykonawców). Tylko wtedy opis może pasować do konkretnej relacji administrator–przetwarzający.

Lokalizacja i przetwarzanie danych osobowych użytkowników z instytucji unijnych i innych podmiotów danych w państwach trzecich znacząco utrudnia instytucjom wprowadzenie skutecznych środków mających na celu zapewnienie zgodności z rozporządzeniem 2018/1725. Transgraniczne przepływy danych osobowych dokonywane bez dokładnego poznania warunków prawnych w państwach trzecich (w tym państwach tranzytowych) powodują, że administratorowi danych bardzo trudno ocenić, jakie zabezpieczenia techniczne, organizacyjne, i prawne muszą zostać wdrożone przed rozpoczęciem przekazywania danych[33]. Gdy dane osobowe znajdują się poza terytorium UE/EOG, jeśli brakuje decyzji o odpowiedniej ochronie obejmującej państwo trzecie przeznaczenia lub odpowiednich gwarancji. Osoby których dane dotyczą, wówczas mogą mieć trudności z wykonywaniem swoich praw. W tych okolicznościach mogą zostać naruszone prawa osób, których dane dotyczą, prawo do złożenia skargi do niezależnego organu nadzorczego, prawo do dochodzenia na drodze sądowej zadośćuczynienia oraz prawo do dochodzenia odszkodowania.

9. ŚRODKI TECHNICZNE

W 2016 roku Komisja stwierdziła, że gromadzenie przez Microsoft danych diagnostycznych z jego oprogramowania stanowi problem w zakresie bezpieczeństwa i ochrony danych. Dotyczyło to głównie oprogramowania Office Pro Plus 2016 i Windows 10 Enterprise. Oprogramowanie to nie oferowało wbudowanych środków, służących instytucjom unijnym do całkowitego zarządzania przepływem danych diagnostycznych do Microsoftu lub wstrzymywania takiego przepływu. Prace Komisji w zakresie wykrywania i ograniczania problemów związanych z bezpieczeństwem i ochroną danych stwarzanych przez oprogramowanie Microsoftu pokazały, że na poziomie technicznym (a więc nie tylko umownym) podejście Microsoftu do dostarczania swoich produktów i usług nie było w pełni

dzibę w krajach trzecich, Dz.U. UE L 39, 12.2.2010 r., s. 5–18, omówiona dokładniej w D. Karwala, *op. cit.*, s. 205–215.

[33] W chwili zakończenia dochodzenia nie było jeszcze orzeczenia w sprawie *Schrems II*, ale znane było już odnośnie do niej stanowisko rzecznika generalnego S. Øe. Podkreślił on potrzebę zapewnienia przez administratorów ochrony danych osobowych nie tylko po przybyciu do państwa trzeciego, ale także po rozpoczęciu przekazywania, a więc także podczas tranzytu. Zob. opinia rzecznika generalnego H.S. Øe przedstawiona 19 grudnia 2019 roku w sprawie *Data Protection Commissioner przeciwko Facebook Ireland Limited i M. Schremsowi*, EU:C:2019:1145, motyw 1 i 204.

zgodne z zasadami ochrony danych w fazie projektowania i domyślnie[34]. Prace prowadzone w latach 2018–2020 na zlecenie MSiB NL i podsumowane w trzech dwukrotnie aktualizowanych ocenach wpływu produktów i usług Microsoftu na ochronę danych osobowych[35] nie tylko potwierdziły zastrzeżenia formułowane w wewnętrznych dokumentach Komisji Europejskiej, lecz także je znacząco rozbudowały i przede wszystkim przekazały do publicznej wiadomości[36]. Ponieważ administratorzy są zobowiązani do wdrożenia środków technicznych i organizacyjnych w celu zapewnienia ochrony danych już w fazie projektowania i domyślnie, EIOD wydał wytyczne dla instytucji UE, aby pomóc im w tym zakresie[37].

PODSUMOWANIE

Choć postepowanie prowadzone w latach 2019–2020 przez Europejskiego Inspektora Ochrony Danych dotyczyło tylko jednego dostawcy produktów i usług chmurowych, a jego zakres przedmiotowy odnosił się jedynie do oprogramowania i usług oferowanych w modelu Software as a Service (SaaS) na potrzeby bieżącej pracy administracji unijnej, jego konkluzje i zalecenia EIOD wobec instytucji unijnych, które chciałyby nadal korzystać z usług Microsoft, mogą być bardzo cenne dla wszystkich instytucji i podmiotów publicznych. Podobne do UE kłopoty napotkać mogą również inne organizacje międzynarodowe. Takie konstatacje doprowadziły w sierpniu 2019 roku do powołania przez EIOD i MSiB NL tak

[34] W. Wiewiórowski, *Privacy by Design jako paradygmat ochrony prywatności*, [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpor, W. Wiewiórowski, Warszawa 2012, s. 13–29; L. Bygrave, *Article 25. Data protection by design and by default*, [w:] *The EU General Data…*, s. 571–581.

[35] Najnowsze wersje tych dokumentów z 11 czerwca 2019 roku znaleźć można na stronach MSiB NL zarówno w języku niderlandzkim, jak i po angielsku. Zob. https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise (dostęp: 20.10.2021). O roli, jaką powinny odgrywać tego typu dokumenty, najobszerniej polskiej literaturze pisze M. Ganczar, *Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych*, [w:] *Internet. Przetwarzanie danych osobowych*, red. G. Szpor, K. Czaplicki, Warszawa 2019, s. 36–49.

[36] Szczegółowy opis ryzyk zamieszczono w S. Nas, *Assessment MS Office 365 Web & apps: Microsoft promises measures to mitigate 6 high privacy risks, Privacy Company Blog, 9.7.2020* https://www.privacycompany.eu/blogpost-en/assessment-of-microsoft-office-365-for-the-web-and-apps-microsoft-promises-measures-to-mitigate-high-privacy-risks (dostęp: 30.01.2021). Uzupełnieniem może być wcześniejszy wpis tej samej autorki (zarządzającej pracami prowadzonymi na zlecenie MSiB NL): S. Nas, *New DPIA on Microsoft Office and Windows software: still privacy risks remaining, Privacy Company Blog, 29.7.2019*, https://www.privacycompany.eu/blogpost-en/new-dpia-on-microsoft-office-and-windows-software-still-privacy-risks-remaining-long-blog (dostęp: 20.10.2021).

[37] Wytyczne EIOD w sprawie ochrony danych osobowych w ładzie IT i zarządzaniu IT w instytucjach UE z 23.03.2018, https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf (dostęp: 20.10.2021).

zwanego Forum Haskiego — nieoficjalnej platformy współpracy dla organów publicznych z krajów członkowskich UE, instytucji UE oraz innych organizacji międzynarodowych, służącej wymianie informacji i wzmocnieniu pozycji negocjacyjnej administracji publicznej wobec dostawców usług informacyjnych, w tym wobec dostawców usług chmurowych.

Uczestnicy Forum uważają, że dzieląc się wynikami własnych prac pomogą podmiotom publicznym negocjować warunki umowne zgodne z zasadami ochrony danych. Nie można bowiem godzić się, aby dane osób gromadzone w ramach świadczenia usług publicznych były przetwarzane przez usługodawców do ich własnych celów. Forum Haskie jest przykładem praktycznej współpracy nowoczesnych i innowacyjnych podmiotów publicznych promujących odpowiedzialne przetwarzanie danych zgodnie z wartościami europejskimi i z korzyścią dla wszystkich.

CONTROLLER AND PROCESSOR IN GOVERNMENTAL CLOUD SERVICES. LESSONS LEARNT FROM THE EU INSTITUTIONS AND MICROSOFT CASE

Summary

Contractual safeguarding of the rights of the data controller and the rights of data subjects forms one of the most serious issues concerning cloud-based e-services of public administration. Cooperation between public authorities in the EU member states, EU institutions, and international organizations has contributed in 2019–2021 to the significant change of contractual terms, technical safeguards, and default settings of cloud services created for public administrations by the most powerful software developers and internet service providers. The article discusses the results of an investigation that the European Data Protection Supervisor (EDPS) undertook in 2019 to assess the legal and practical implications of the use of Microsoft products and services by European Union institutions, bodies, offices and agencies. The investigation made several key findings. Most importantly, it found that the licensing agreement between Microsoft and the EU institutions allowed Microsoft to unilaterally define and change certain parameters for processing data on behalf of the institutions and to amend its contractual data protection obligations. It also assessed technical measures the European Commission had put in place to stem the flow of personal data generated by Microsoft's products and services — mainly telemetry data — being sent to the company. The assessment led to a general recommendation that all EU institutions test a revised and comprehensive approach, share the knowledge and technical solutions they have developed to prevent unauthorized data flows to Microsoft, and inform each other of any data protection issues they identify with products or services.

Keywords: personal data, controller, processor, cloud, e-government

BIBLIOGRAFIA

EIOD, EDPS Public Paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services, https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_paper_euis_microsoft_contract_investigation_en.pdf.

EIOD, Wytyczne w sprawie ochrony danych osobowych w ładzie IT i zarządzaniu IT w instytucjach UE z 23.3.2018, https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf.

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

Ganczar M., *Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych*, [w:] *Internet. Przetwarzanie danych osobowych*, red. G. Szpor, K. Czaplicki, Warszawa 2019, s. 36–49.

Gellman B., *Dark Mirror. Edward Snowden and the Surveillance State*, London 2020.

Karwala D., *Komercyjne transfery danych osobowych do państw trzecich*, Warszawa 2018.

Koning M., *The Purpose and Limitations of Purpose Limitation*, Nijmegen 2020.

Krasuski A., *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018.

Krasuski A., *Status prawny sztucznego agenta. Podstawy prawne zastosowania sztucznej inteligencji*, Warszawa 2021.

Marchini R., *Cloud Computing: A Practical Introduction to Legal Issues*, London 2010.

Mateos A., Rosenberg J., *Chmura obliczeniowa. Rozwiązania dla biznesu*, Gliwice 2011.

Nas S., *Assessment MS Office 365 Web & apps: Microsoft promises measures to mitigate 6 high privacy risks, Privacy Company Blog, 9.7.2020*, https://www.privacycompany.eu/blogpost-en/assessment-of-microsoft-office-365-for-the-web-and-apps-microsoft-promises-measures-to-mitigate-high-privacy-risks.

Nas S., *New DPIA on Microsoft Office and Windows software: still privacy risks remaining*, Privacy Company Blog, 29.7.2019.

Rozporządzenie UE w sprawie ochrony danych osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, red. P. Litwiński, Warszawa 2018.

Schwab K., *The Fourth Industrial Revolution*, London 2017.

Smith B., *Tools and Weapons*, London 2019.

Sobczyk A., *RODO: rozproszona władza publiczna*, Kraków 2019.

W Kuan Hen, Millard Ch., Walden I., *Public Sector Cloud Contracts*, [w:] *Cloud Computing Law*, red. Ch. Millard, Oxford 2013.

Wiewiórowski W., *Prawne aspekty udostępniania usług administracji publicznej w modelu chmury*, [w:] *Internet — Cloud computing. Przetwarzanie w chmurze*, red. G. Szpor, Warszawa 2013.

Wiewiórowski W., *Privacy by Design jako paradygmat ochrony prywatności*, [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpor, W. Wiewiórowski, Warszawa 2012.

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: Transatlantic tensions, EU surveillance, and big data*, red. G. Vermeulen, E. Lievens, Antwerpen 2017.