



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Miroslaw Wróblewski**

Warszawa,

DOL.401.60.2024

DOL.401.62.2024

Pan

Zastępca Szefa Kancelarii Sejmu RP

ul. Wiejska 4/6/8
00-902 Warszawa

Szanowny Panie Ministrze,

w związku ze skierowaniem do Sejmu Rzeczypospolitej Polskiej rządowych projektów **ustawy – Prawo komunikacji elektronicznej (druk sejmowy nr 423)** oraz **ustawy Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej (druk sejmowy nr 424)**, działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹ oraz art. 51 ustawy o ochronie danych osobowych², uprzejmie informuję, że do przedstawionego projektu ustawy – Prawo komunikacji elektronicznej Prezes Urzędu Ochrony Danych Osobowych zgłasza uprzejmie następujące uwagi.

Projekt ustawy – Prawo komunikacji elektronicznej, dalej jako: PKE, był przedmiotem uzgodnień z organem nadzorczym na rządowym etapie prac, zarówno w trakcie opiniowania projektowanej ustawy, jak i podczas komisji prawniczej. Znaczną część zagadnień związanych z problematyką prywatności i ochrony danych osobowych udało się uzgodnić z projektodawcą. Najistotniejszymi kwestiami, w których organ nadzorczy wyraża odmienne od projektodawcy stanowisko, jest nieprzeprowadzenie przez projektodawcę **testu prywatności w procesie tworzenia prawa**, w tym oceny

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 z 4.5.2016, str. 1 ze zm.).

² Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

skutków dla ochrony danych – art. 25 ust. 1³, jak i art. 35 rozporządzenia 2016/679 (w szczególności ust. 1⁴ i ust. 10⁵), w związku z przyjmowaniem podstawy prawnej przetwarzania (a przede wszystkim wprowadzenie instytucji wideoidentyfikacji abonenta – **art. 296 ust. 3 pkt 2 lit. d PKE**) oraz **powielenie w PKE niezgodnego z orzecznictwem Trybunału Sprawiedliwości UE modelu retencji i udostępniania danych telekomunikacyjnych uprawnionym podmiotom.**

Art. 47 ust. 1 projektu ustawy nakłada na przedsiębiorców telekomunikacyjnych **obowiązek przechowywania przez okres 12 miesięcy danych użytkownika końcowego, o których mowa w art. 49 ust. 1 PKE.** Są to dane użytkownika końcowego inicjującego połączenie, do którego kierowane jest połączenie, tj. data i godzina połączenia oraz czas jego trwania, rodzaj połączenia, lokalizacja telekomunikacyjnego urządzenia końcowego oraz dane jednoznacznie identyfikujące użytkownika w sieci. Art. 47 ust. 2 PKE nakłada obowiązek udostępniania tych danych uprawnionym podmiotom, a także sądowi i prokuratorowi. Uprawnione podmioty wymienione są w art. 43 ust. 1 pkt 1 lit. a PKE. Zalicza się do nich Policję, Biuro Nadzoru Wewnętrznego, Straż Graniczną, Inspektorat Wewnętrzny Służby Więziennej, Służbę Ochrony Państwa, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i Krajową Administrację Skarbową. Co do zasady projektowany przepis stanowi powielenie obowiązującego art. 180a Prawa telekomunikacyjnego. W kontekście orzecznictwa sądów międzynarodowych i zapewnienia konstytucyjności prawa krajowego i z uwzględnieniem wytycznych zawartych w motywie 41 rozporządzenia 2016/679, co do tego, że „W przypadku gdy w niniejszym rozporządzeniu jest mowa o podstawie prawnej lub akcie prawnym, niekoniecznie wymaga to przyjęcia aktu prawnego przez parlament, z zastrzeżeniem wymogów wynikających z porządku konstytucyjnego danego państwa członkowskiego. Taka podstawa prawna lub taki akt prawny powinny być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej [...] i Europejskiego Trybunału Praw Człowieka”.

³ Uwzględniając 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 zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, 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.

⁴ Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

⁵ Ust. 1–7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.

Prezes UODO, mając to na względzie, zwraca uprzejmie uwagę, że Trybunał Sprawiedliwości UE w swoich orzeczeniach – m.in. wyroku z dnia 6 października 2020 r. *La Quadrature du Net i in. przeciwko Premier ministre i in.* sprawy połączone C-511/18, C-512/18 i C-520/18⁶, wyroku z dnia 6 października 2020 r. *Privacy International przeciwko Secretary of State for Foreign and Commonwealth Affairs i in.* sprawa C-623/17⁷ oraz wyroku w sprawie Trybunału Sprawiedliwości z dnia 30 kwietnia 2024 r. w sprawie C-470/21 *La Quadrature du Net i in. przeciwko Premier ministre i Ministère de la Culture*⁸ – wskazał, że niezróżnicowane gromadzenie danych przez przedsiębiorców telekomunikacyjnych o wszystkich użytkownikach jest niezgodne z Kartą Praw Podstawowych Unii Europejskiej. Problem ten wybrzmiał również w niedawnym wyroku Europejskiego Trybunału Praw Człowieka z dnia 28 maja 2024 r. *Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce*, nr skargi 72038/17.

Aktualnie prowadzony proces ustawodawczy dotyczący Prawa komunikacji elektronicznej jest okazją do ponownego przeanalizowania modelu udostępniania uprawnionym podmiotom danych o użytkownikach i wprowadzenia dodatkowych, jasnych warunków dotyczących abonentów, których spełnienie jest niezbędne, aby uczynić zadość ww. wyrokom TSUE. W ocenie Prezesa UODO stosowany obecnie model bezwarunkowego gromadzenia danych o wszystkich użytkownikach nie zapewnia stosowania wynikających z przepisów rozporządzenia 2016/679 zasad dotyczących przetwarzania danych osobowych: zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a⁹), ograniczenia celu (art. 5 ust. 1 lit. b¹⁰), zasady minimalizacji danych (art. 5 ust. 1 lit. c¹¹) oraz ograniczenia przechowywania (art. 5 ust. 1 lit. e¹²), jak również wynikającej z art. 51 ust. 2 Konstytucji RP zasady ograniczenia gromadzenia informacji o obywatelach przez władze publiczne.

Art. 49 ust. 2 PKE stanowi, że: „Minister właściwy do spraw informatyzacji w porozumieniu z ministrem właściwym do spraw wewnętrznych oraz po zasięgnięciu opinii Ministra – Koordynatora Służb Specjalnych, jeżeli został on powołany, określi, w drodze rozporządzenia: szczegółowy wykaz danych, o których mowa w ust. 1.”. W ocenie organu nadzorczego **zamknięty katalog danych użytkownika** powinien zostać

⁶ <https://curia.europa.eu/juris/liste.jsf?num=C-511/18&language=pl>

⁷ <https://curia.europa.eu/juris/liste.jsf?num=C-623/17&language=PL>

⁸ <https://curia.europa.eu/juris/liste.jsf?num=C-470/21>

⁹ Zgodnie z zasadą zgodności z prawem, rzetelności i przejrzystości dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

¹⁰ Zgodnie z zasadą ograniczenia celu dane osobowe muszą być 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 za niezgodne z pierwotnymi celami.

¹¹ Zgodnie z zasadą minimalizacji danych dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

¹² Zgodnie z zasadą ograniczenia przechowywania 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; 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.

określony w przepisach o randze odpowiedniej, tj. spełniającej standard konstytucyjnego źródła prawa dla stanowienia praw i obowiązków, tj. **w przepisach projektowanej ustawy**, zgodnie z wymogami art. 31 i art. 51 ust. 1 i 5 Konstytucji RP. Tymczasem, projektowany przepis przez to, że nie zawiera tego katalogu, powiela blankietowe rozwiązania zawarte w art. 180c ust. 2 Prawa telekomunikacyjnego i nie zapewnia stosowania zasady zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu oraz minimalizacji danych.

Art. 57 ust. 5 PKE stanowi, że: „Podmiot, który uzyskał pozwolenie na dostęp do PRS, prowadzi rejestr sprzętu na potrzeby PRS lub technologii PRS będących w posiadaniu tego podmiotu oraz imienny rejestr osób mających dostęp do sprzętu na potrzeby PRS lub technologii PRS będących w posiadaniu tego podmiotu”. Przepisy ustawy powinny określać jaki jest zakres danych wpisywanych do tego **imiennego rejestru osób**, co odpowiadałoby zasadzie zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu oraz minimalizacji danych określonych w rozporządzeniu 2016/679.

Art. 350 ust. 1 pkt 3 PKE stanowi, że „Dostawca usług komunikacji elektronicznej zapewnia dla każdego fakultatywnego obciążania rachunku autoryzację usługi przy pomocy co najmniej jednego z elementów uwierzytelniania należącego do kategorii: (...) cechy charakterystyczne abonenta – chyba że przepisy odrębne przewidują wyższy poziom autoryzacji”. Pojęcie cech charakterystycznych abonenta może obejmować również dane osobowe abonenta, które będą służyć potwierdzeniu jego tożsamości, dlatego też projektowany przepis powinien wprost odsyłać do kategorii danych osobowych i źródła tych danych. We wcześniejszej wersji projektowanego przepisu (art. 350 ust. 1 pkt 2 wersji projektu ustawy z dnia 11 kwietnia 2024 r. skierowanej na posiedzenie Stałego Komitetu Rady Ministrów) projektodawca posłużył się w tej materii dużo bardziej precyzyjnym odesłaniem do „danych potwierdzających tożsamość abonenta wyrażającego zgodę na fakultatywne obciążanie rachunku lub informacji o nim pochodzących z wiarygodnego i niezależnego źródła, w tym, o ile są dostępne, ze środków identyfikacji elektronicznej lub z odpowiednich usług zaufania określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73)”. Takie sformułowanie w sposób pełniejszy odpowiada zasadzie zgodności z prawem, rzetelności i przejrzystości.

Jednocześnie organ nadzorczy informuje, że nie zgłasza uwag do projektu ustawy Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych