



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Miroslaw Wróblewski

Warszawa,

DPNT.413.9.2025

**Pan
Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji**

Szanowny Panie Premierze,

w związku z zapadłym w **dniu 30 kwietnia 2024 r. wyrokiem Trybunału Sprawiedliwości UE w sprawie C-470/21 *La Quadrature du Net***, działając na podstawie art. 52 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych¹, zwracam się z uprzejmą prośbą **o rozważenie podjęcia prac legislacyjnych prowadzących do zmiany przepisów ustawy - Prawo komunikacji elektronicznej² w zakresie zasad dostępu organów ścigania do danych objętych tajemnicą komunikacji elektronicznej.**

Na wstępie uprzejmie informuję, że swoją opinię dotyczącą konieczności podjęcia działań legislacyjnych w związku z powyższym wyrokiem TSUE Prezes Urzędu Ochrony Danych Osobowych przedstawił wcześniej Ministrowi ds. Unii Europejskiej w piśmie z dnia 11 czerwca 2024 r. (sygn. akt DOL.0623.15.2024). Prezes UODO zwracał uwagę na najważniejsze tezy wyroku, a także na orzecznictwo Trybunału dotyczące pozyskiwania przez służby na potrzeby prowadzonego postępowania karnego dostępu do danych

¹ Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019, poz. 1781; dalej ustawa o ochronie danych osobowych). Zgodnie z art. 52 ust. 2 ustawy Prezes Urzędu może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych

² Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1221 ze zm.).

osobowych objętych tajemnicą telekomunikacyjną w myśl obowiązującej wówczas ustawy Prawo telekomunikacyjne³. Ponieważ organ nadzorczy nie otrzymał pozytywnej odpowiedzi na to wystąpienie, a sprawa dotyczy kwestii niezwykle istotnych z punktu widzenia prawa do prywatności, postulat wprowadzenia zmian w obowiązujących przepisach prawa pozostaje aktualny.

W opinii dotyczącej projektu ustawy Prawo komunikacji elektronicznej (druk sejmowy nr 423), która zastąpiła Prawo telekomunikacyjne, Prezes UODO zwrócił uwagę, że pomimo tego, że istniała okazja do przyjęcia standardów zgodnych z orzecnictwem sądów europejskich, projekt powiela niezgodny z nimi model m.in. retencji i udostępniania danych telekomunikacyjnych⁴. W konsekwencji obowiązujące przepisy Prawa komunikacji elektronicznej wymagają dostosowania do unijnych standardów ochrony prawa do prywatności.

W ww. wyroku z 30 kwietnia 2024 r. TSUE (w pełnym składzie) orzekł, że: „Artykuł 15 ust. 1 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 Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r., w świetle art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że:

- nie stoi on na przeszkodzie uregulowaniu krajowemu, które zezwala organowi publicznemu odpowiedzialnemu za ochronę praw autorskich i praw pokrewnych przed naruszeniami tych praw, do których dochodzi w Internecie, na dostęp do przechowywanych przez dostawców publicznie dostępnych usług łączności elektronicznej danych dotyczących tożsamości cywilnej odpowiadających adresom IP zbieranym wcześniej przez organizacje zrzeszające uprawnionych, aby ów organ mógł zidentyfikować posiadaczy tych adresów wykorzystywanych do aktywności mogącej stanowić takie naruszenia i aby mógł on w razie potrzeby zastosować wobec nich środki, pod warunkiem że na mocy tego uregulowania:
- dane te przechowywane są w warunkach i zgodnie z zasadami technicznymi, które gwarantują, że wykluczone jest, by ich przechowywanie mogło pozwalać na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego tych posiadaczy, na przykład poprzez ustalenie ich szczegółowego profilu, co można osiągnąć w szczególności poprzez

³ Ustawa z dnia 16 lipca 2024 r. – Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34 ze zm.).

⁴ Zob. opinia Prezesa UODO udostępniona na stronie UODO: <https://uodo.gov.pl/pl/138/3126>

nałożenie na dostawców usług łączności elektronicznej obowiązku przechowywania poszczególnych kategorii danych osobowych, takich jak dane dotyczące tożsamości cywilnej, adresy IP oraz dane o ruchu i dane dotyczące lokalizacji, gwarantującego rzeczywiście szczelne odseparowanie tych poszczególnych kategorii danych, które uniemożliwia na etapie przechowywania wszelkie powiązanie tych poszczególnych kategorii danych, przez okres nieprzekraczający tego, co ściśle niezbędne;

- dostęp tego organu publicznego do takich danych przechowywanych w sposób odseparowany i rzeczywiście szczelny służy wyłącznie zidentyfikowaniu osoby podejrzewanej o dopuszczenie się czynu zabronionego i towarzyszą mu gwarancje niezbędne do wykluczenia, by, poza sytuacjami nietypowymi, dostęp ten mógł pozwalać na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego posiadaczy adresów IP, na przykład poprzez ustalenie ich szczegółowego profilu, co wymaga w szczególności, by upoważnionych do posiadania takiego dostępu urzędników owego organu obowiązywał zakaz ujawniania w jakiegokolwiek formie informacji na temat zawartości plików przeglądanych przez tych posiadaczy, z jedynym wyjątkiem wiążącym się z ujawnieniem ich w celu zawiadomienia prokuratury, zakaz śledzenia historii treści przeglądanych przez owych posiadaczy oraz, ogólniej, zakaz wykorzystywania tych adresów IP do celów innych niż zidentyfikowanie ich posiadaczy, aby zastosować wobec nich ewentualne środki;

- możliwość powiązania przez osoby odpowiedzialne w ramach wspomnianego organu publicznego za analizę zdarzeń takich danych z plikami zawierającymi elementy umożliwiające poznanie tytułów utworów chronionych, których udostępnienie w Internecie uzasadniało zebranie adresów IP przez organizacje zrzeszające uprawnionych, jest uzależniona – w przypadkach kolejnego ponowienia aktywności naruszającej prawa autorskie lub prawa pokrewne przez tę samą osobę – od dokonania przez sąd lub niezależny organ administracyjny kontroli, która nie może być w pełni zautomatyzowana i powinna mieć miejsce przed dokonaniem takiego powiązania, ponieważ powiązanie to może w takich przypadkach pozwolić na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego wspomnianej osoby, której adres IP wykorzystano do aktywności mogącej naruszać prawa autorskie lub prawa pokrewne;

- system przetwarzania danych wykorzystywany przez organ publiczny podlega w regularnych odstępach czasu kontroli niezależnego organu mającego status strony trzeciej w stosunku do tego organu publicznego, mającej na celu weryfikację integralności systemu, w tym skutecznych gwarancji chroniących przed ryzykiem takiego

dostępu do tych danych lub takiego ich wykorzystywania, które nosiłyby znamiona nadużycia lub byłyby niezgodne z prawem, oraz jego skuteczności i niezawodności w wykrywaniu ewentualnych uchybień”.

Odnosząc się do ww. wyroku TSUE, należy zauważyć, że w prawie polskim nie ma odpowiednika francuskiego Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet [wysoki urząd ds. rozpowszechniania utworów i ochrony praw w Internecie (Hadopi)], o którym mowa w orzeczeniu jako organie publicznym odpowiedzialnym za ochronę praw autorskich i praw pokrewnych przed naruszeniami tych praw. Niemniej – jak to zostało opisane w wyroku – Hadopi posiada również kompetencję do ścigania przestępstw przeciwko prawom własności intelektualnej i jest organem publicznym w rozumieniu art. 3 dyrektywy 2016/680⁵. Ma to znaczenie z punktu widzenia oceny wpływu wyroku na prawo polskie ze względu na to, że świetle przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych organami publicznymi powołanymi do ścigania przestępstw stypizowanych w art. 115 i n. tej ustawy są organy ścigania. Do ich działania w tym zakresie zastosowanie znajdują wskazania płynące z tego wyroku. Organy prowadzące postępowania karne z tego zakresu nie są zatem objęte przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (dalej: RODO lub rozporządzenie 2016/679)⁶, a podlegają przepisom ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości⁷. Przesłanka legalności ich działania wynika z art. 13 ust. 1 tej ustawy, zgodnie z którym właściwe organy przetwarzają dane osobowe **wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa**. Jednocześnie uczestnikom postępowania przysługują prawa wynikające z ww. ustawy wdrażającej dyrektywę 2016/680⁸.

⁵ 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 uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE. L 119 z 4.5.2016, str. 89 ze zm.).

⁶ 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) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.).

⁷ Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206).

⁸ 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

Zgodnie z orzecznictwem Trybunału, jak też i utrwalonym stanowiskiem sądów polskich, adres IP uznawany jest za daną osobową w rozumieniu RODO, jak i daną o ruchu w rozumieniu dyrektywy 2002/58⁹ (podobnie np. wyrok z dnia 17 czerwca 2021 r. w sprawie C-597/19¹⁰, czy wyrok TSUE z dnia 7 marca 2024 r. w sprawie C-604/22¹¹). Jak wskazał TSUE w przytoczonym wyroku w sprawie C-604/22, powiązanie identyfikatora jakim jest np. adres IP urządzenia użytkownika z innymi informacjami o użytkowniku (np. dotyczącymi płatności przy użyciu karty kredytowej) pozwala na faktyczną identyfikację osoby (także przy dynamicznym adresie IP) oraz na stworzenie profilu użytkownika. Stworzenie takiego profilu skutkować może dostępem do informacji o różnego rodzaju aktywnościach użytkownika w Internecie, z których pośrednio wynikać mogą dane dotyczące tego użytkownika, w tym dane szczególnych kategorii.

W systemie prawa polskiego organ mający informację o uzasadnionym podejrzeniu popełnienia przestępstwa przeciwko prawom własności intelektualnej popełnionego przez użytkownika posługującego się określonym numerem IP może wystąpić do przedsiębiorcy telekomunikacyjnego o udostępnienie danych pozwalających ustalić jego tożsamość. Dane dotyczące podmiotu korzystającego z publicznie dostępnej sieci telekomunikacyjnej (użytkownika) objęte są tajemnicą komunikacji elektronicznej na podstawie w art. 386 oraz przepisów rozdziału 5, dział VII ustawy Prawo komunikacji elektronicznej. Tajemnica komunikacji elektronicznej stanowi jeden z elementów prawa do prywatności, które jest chronione zarówno na poziomie krajowym, jak i międzynarodowym. Prawo do prywatności obejmuje w szczególności odpowiednie reglamentowanie dostępu do danych, w szczególności objętych różnego rodzaju tajemnicami, w tym tajemnicą komunikowania się, zgodnie z zasadami niezbędności, proporcjonalności i minimalizacji danych¹². Zasady przetwarzania danych objętych tajemnicą komunikacji elektronicznej i dostępu do nich określone zostały w dziale I, rozdział V tej ustawy, która zasadniczo implementowała przepisy dyrektywy 2002/58. Zgodnie z art. 43 ust. 1 pkt 1 tej ustawy przedsiębiorca telekomunikacyjny, z wyjątkiem

zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW

⁹ 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. U. UE. L 201 z 31.7.2002, str. 37 ze zm.).

¹⁰ Wyrok TSUE z dnia 17 czerwca 2021 r. w sprawie C-597/19, Mircom International Content Management & Consulting (M.I.C.M.) Limited Przeciwko Telenet Bvba.

¹¹ Wyrok TSUE z dnia 7 marca 2024 r. w sprawie C-604/22, IAB EUROPE.

¹² Wyrok TSUE z dnia 8 kwietnia 2014 r., - połączone sprawy C-293/12 Digital Rights Ireland i C-594/12, Kärntner Landesregierung, wyrok ETPCz z 15 lutego 2024 r., Škoberne przeciwko Słowenii, nr 19920/20,

przypadków, o których mowa w przepisach wydanych na podstawie art. 46 ust. 1 pkt 2, jest obowiązany do zapewnienia warunków technicznych i organizacyjnych dostępu i utrwalania, umożliwiających jednocześnie i wzajemnie niezależne uzyskiwanie przez Policję, Biuro Nadzoru Wewnętrzny, Straż Graniczną, Inspektorat Wewnętrzny Służby Więziennej, Służbę Ochrony Państwa, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i Krajową Administrację Skarbową dostępu do informacji przesyłanych lub powstałych w ramach świadczonej publicznie dostępnej usługi telekomunikacyjnej. Przedsiębiorca telekomunikacyjny dodatkowo zapewnia warunki techniczne do utrwalania i udostępniania, na własny koszt, na rzecz sądu i prokuratora, przez podmiot wskazany w postanowieniu sądu lub prokuratora, komunikatów elektronicznych i danych, o których mowa w pkt 1 lit. a i b (art. 43 ust. 1 pkt. 2).

Analizując treść przepisów ustawy Prawo komunikacji elektronicznej przez pryzmat wyroku TSUE z 30 kwietnia 2024 r. stwierdzić należy, że nie odpowiadają one standardom wynikającym z art. 7, 8, 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, a ograniczenie tajemnicy komunikacji elektronicznej nie spełnia warunku wynikającego z art. 15 ust. 1 dyrektywy 2002/58 w postaci **niezbędności i proporcjonalności** w społeczeństwie demokratycznym.

Zgodnie z wyrokiem TSUE przepisy krajowe zezwalające organowi publicznemu na dostęp do przechowywanych przez operatora telekomunikacyjnego danych dotyczących tożsamości użytkownika posługującego się określonym numerem IP, co do którego organ posiada uzasadnione podejrzenie popełnienia przestępstwa przeciwko prawom własności intelektualnej, powinny określać, aby dane te przechowywane były w warunkach i zgodnie z zasadami technicznymi, które wykluczają możliwość uzyskania informacji pozwalających na wyciągnięcie na ich podstawie precyzyjnych wniosków na temat życia prywatnego tej osoby. Osiągnięcie tego celu jest możliwe w szczególności poprzez nałożenie na dostawców usług łączności elektronicznej obowiązku przechowywania **poszczególnych kategorii danych osobowych** w sposób gwarantujący **faktyczne odseparowanie poszczególnych kategorii danych** i uniemożliwienie powiązania ich przez okres uznany za niezbędny. Wyżej wskazane przepisy ustawy Prawo komunikacji elektronicznej nie zawierają gwarancji, na które wskazał Trybunał. Brak jest w nich gwarancji technicznych, które uniemożliwiłyby uzyskanie danych w zakresie szerszym niż tylko dla ustalenia tożsamości użytkownika, jak też operatorzy telekomunikacyjni nie mają obowiązku gromadzenia danych w sposób

zapewniający odseparowanie poszczególnych kategorii danych, tak aby nie było możliwe ich łączenie i tworzenie profilu aktywności użytkownika. Nawiązując do treści wyroku, stwierdzić należy, że brak jest przepisów gwarantujących, że dane przechowywane będą w „sposób odseparowany i rzeczywiście szczelny”, i że służyć będą wyłącznie zidentyfikowaniu osoby podejrzewanej o dopuszczenie się czynu zabronionego, a przetwarzaniu towarzyszyć będą gwarancje niezbędne do wykluczenia „by, poza sytuacjami nietypowymi, dostęp ten mógł pozwalać na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego posiadaczy adresów IP”.

Ponadto Trybunał wskazał w wyroku, że aby można było uznać dostęp do danych objętych tajemnicą telekomunikacyjną za niezbędny i adekwatny powinny istnieć w prawie krajowym gwarancje w postaci **kontroli niezależnego organu** mającego status osoby trzeciej w stosunku do organu ubiegającego się o dane osobowe.

Zgodnie z przytoczonym wyżej art. 43 ust. 1 pkt. 1 a ustawy Prawo komunikacji elektronicznej przedsiębiorcy telekomunikacyjni obligatoryjnie udostępniają dane uprawnionym podmiotom takim jak: Policja, Biuro Nadzoru Wewnętrzny, Straż Graniczna, Inspektorat Wewnętrzny Służby Więziennej, Służba Ochrony Państwa, Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, Centralne Biuro Antykorupcyjne i Krajowa Administracja Skarbowa oraz na rzecz sądu i prokuratora, przez podmiot wskazany w postanowieniu sądu lub prokuratora (art. 43 ust. 1 pkt. 2). **W demokratycznym państwie prawa zasadność pozyskania danych telekomunikacyjnych powinna być poddana kontroli sądu lub niezależnego organu administracyjnego.** Kontrola przeprowadzona przez te podmioty byłaby też zgodna z zasadą pogłębiania zaufania obywateli do państwa, gdyż eliminowałaby ryzyko nieproporcjonalnej ingerencji w prawa podstawowe, jak też gwarantowałaby pewność stosowania prawa, na co wskazał TSUE w wyroku z 8 kwietnia 2014 r. w sprawach połączonych Digital Rights Ireland Ltd (C-293/12) i Kärntner Landesregierung (C-594/12). Taki stan prawny czyni zasadnym postulat wprowadzenia zmian w przepisach prawa komunikacji elektronicznej w zakresie **zasad dostępu organów ścigania** do danych objętych tajemnicą telekomunikacyjną. Jednocześnie sama kontrola przeprowadzana przez sąd lub niezależny organ administracyjny powinna być konieczna i adekwatna w demokratycznym porządku prawa, a także przeprowadzona zgodnie z zasadą proporcjonalności (na co TSUE zwrócił uwagę w wyroku z dnia 2 marca 2021 r. w sprawie C-746/18 Prokuratuur) oraz dotyczyć powinna

wyłącznie przypadków wskazanych w art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej.

W kontekście kontroli sądowej należy wspomnieć także o wyroku Europejskiego Trybunału Praw Człowieka (dalej: ETPCz) z 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce (skargi nr 72038/17 i 25237/18). Sprawa dotyczyła ustawodawstwa polskiego, pozwalającego służbom na zbieranie informacji o obywatelach pod pretekstem walki z przestępczością i zagrożeniami dla bezpieczeństwa publicznego. ETPCz stwierdził, że w wyniku braku realnej kontroli nad prowadzeniem kontroli operacyjnej w ramach czynności operacyjno-rozpoznawczych oraz zbyt ogólnie sformułowanych przesłanek umożliwiających prowadzenie tej kontroli, doszło do trzech naruszeń art. 8 EKPC¹³ – prawa do poszanowania życia prywatnego, rodzinnego oraz korespondencji – w odniesieniu do skarg dotyczących m.in. zatrzymywania danych komunikacyjnych do potencjalnego wykorzystania przez właściwe organy lub władze krajowe.

Uzasadniając wniosek o zmianę przepisów w związku z omawianym wyrokiem TSUE podkreślenia wymaga, że w dotychczasowych orzeczeniach TSUE, w kontekście postanowień art. 7, 8, 11 oraz 52 ust. 1 Karty praw podstawowych Unii Europejskiej, a także m.in. dyrektywy 2002/58/WE, wypowiadał się na temat proporcjonalności przyjętych rozwiązań w tym obszarze i wskazywał na okoliczności w jakich dopuszczalne są określone ingerencje w prawo do prywatności. Najistotniejsze orzeczenia TSUE w tym zakresie to m.in.: wyrok z 13 czerwca 2024 r. w sprawie C-229/23 HYA i in. II, wyrok z 30 kwietnia 2024 r. w sprawie C-178/22 Procura della Repubblica presso il Tribunale di Bolzano, wyrok z 5 kwietnia 2022 r. w sprawie C-140/20, wyrok z 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-520/18, wyrok z 6 października 2020 r. Privacy International przeciwko Secretary of State for Foreign and Commonwealth Affairs i in. sprawa C-623/17, wyrok z 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 Tom Watson, Peter Brice, Geoffrey Lewis, wspomniany wyżej wyrok z 8 kwietnia 2014 r. w sprawach połączonych: C-293/12 i C-594/12, Digital Rights Ireland Ltd przeciwko Minister for Communications i in.

¹³ Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm.).

Mając powyższe na uwadze, po gruntownej analizie wyroku TSUE w sprawie C-470/21 *La Quadrature du Net* w ocenie Prezesa UODO konieczne jest podjęcie działań legislacyjnych, mających na celu zapewnienie skutecznej ochrony prawa do prywatności i prawa do ochrony danych osobowych w odniesieniu do przepisów dotyczących przetwarzania danych osobowych chronionych tajemnicą komunikacji elektronicznej.

W przypadku podjęcia prac legislacyjnych, w związku z przedstawionym powyżej wyrokiem, Prezes Urzędu Ochrony Danych Osobowych deklaruje swoje wsparcie eksperckie celem wypracowania rozwiązań uwzględniających przepisy o ochronie danych osobowych.

W świetle przedstawionej powyżej argumentacji, działając na podstawie art. 52 ust. 3 ustawy o ochronie danych osobowych, uprzejmie proszę Pana Premiera o odniesienie się do tego wystąpienia na **piśmie w terminie 30 dni** od daty jego otrzymania.

Łączę wyrazy szacunku

Mirosław Wróblewski

Prezes Urzędu

Ochrony Danych Osobowych