



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Miroslaw Wróblewski

Warszawa, 12.08.2025 r.

DPNT.413.12.2025

**Pan
Marcin Kierwiński
Minister Spraw Wewnętrznych i
Administracji**

**Ministerstwo Spraw
Wewnętrznych i Administracji**

Szanowny Panie Ministrze,

w związku z zapadłym w **dniu 4 października 2024 r. wyrokiem Trybunału Sprawiedliwości UE w sprawie C-548/21**, CG v Bezirkshauptmannschaft Landeck, działając na podstawie art. 52 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych¹, uprzejmie informuję, że w ocenie Prezesa Urzędu Ochrony Danych Osobowych **wyrok ten determinuje konieczność dokonania zmian legislacyjnych w przepisach krajowych.**

W związku z powyższym, zwracam się z uprzejmą prośbą o rozważenie podjęcia właściwych działań legislacyjnych zmierzających do zapewnienia skutecznej ochrony danych osobowych osób fizycznych.

Na wstępie pragnę zaznaczyć, że swoją opinię na temat skutków ww. wyroku dla prawa polskiego, zawierając wniosek o konieczności podjęcia działań legislacyjnych Prezes Urzędu Ochrony Danych Osobowych przedstawił uprzednio Ministrowi ds. Unii Europejskiej w piśmie z dnia 15 listopada 2024 r. (sygn. akt

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

DOL.0623.29.2021), jednakże nie uzyskał odpowiedzi. Ponieważ wyrok dotyczy materii szczególnie istotnej z punktu widzenia prawa do prywatności, dotyczącej działalności Policji, w ocenie organu, uzasadnione jest niniejsze wystąpienie.

Odnosząc się do przytoczonego wyroku TSUE w sprawie C-548/21, należy wskazać, że dotyczy on zajęcia przez Policję telefonu komórkowego i próby jego odblokowania, w ramach prowadzonego dochodzenia w sprawie handlu narkotykami, w celu uzyskania dostępu do zawartych w nim danych. Jak uznał Trybunał, w przypadku, gdy Policja zatrzymuje telefon i posługuje się nim w celu pozyskania zawartych w nim informacji, w tym danych osobowych, rozpoczyna się proces przetwarzania danych osobowych w rozumieniu art. 3 ust. 2 dyrektywy 2016/680², nawet jeśli ze względów technicznych w danej sytuacji Policja nie uzyska dostępu do tych danych. Trybunał podkreślił, że uzyskanie dostępu do wszystkich danych zawartych w telefonie komórkowym może stanowić poważną ingerencję w prawa podstawowe osoby, której dane dotyczą. Pozyskane w ten sposób dane mogą obejmować wiadomości, zdjęcia i historię przeglądania Internetu, co w konkretnym przypadku stwarza możliwość wyciągnięcia bardzo precyzyjnych wniosków na temat życia prywatnego tej osoby. Przetwarzane dane osobowe mogą przy tym należeć do szczególnych kategorii, jak dane o stanie zdrowia, orientacji seksualnej, czy poglądach politycznych.

Rozstrzygając sprawę, Trybunał uznał, że art. 4 ust. 1 lit. c) dyrektywy 2016/680 w związku z art. 7, 8 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej **nie stoi na przeszkodzie** uregulowaniu krajowemu, które przyznaje właściwym organom możliwość uzyskania wglądu do danych zapisanych w telefonie komórkowym w celu zapobiegania przestępstwom, wykrywania ich i ścigania, **pod warunkiem** jednak, że proces ten jest odpowiednio uregulowany w przepisach prawa, które: wystarczająco **precyzyjnie określają charakter lub kategorie przestępstw**, których to dotyczy, **zawierają gwarancje** poszanowania zasady proporcjonalności oraz uzależniają skorzystanie z tej możliwości, z wyjątkiem należycie uzasadnionych pilnych przypadków, od **uprzedniej kontroli sądu** lub niezależnego organu administracyjnego.

Ponadto Trybunał stwierdził, że art. 13 i 54 dyrektywy 2016/680 w związku z art. 47 i art. 52 ust. 1 Karty praw podstawowych **stoją na przeszkodzie** uregulowaniu krajowemu, które zezwala właściwym organom na podjęcie próby uzyskania wglądu do danych zapisanych w telefonie komórkowym **bez poinformowania osoby**, której dane dotyczą w ramach mających zastosowanie procedur krajowych **o powodach**, na których opiera się zgoda na wgląd do takich danych wydana przez sąd lub niezależny organ administracyjny, z chwilą gdy

² 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 uchyłającej decyzję ramową Rady 2008/977/WSiSW, Dz.Urz. L 119 z 4.5.2016, s. 89.

przekazanie tych informacji przestało zagrażać prawidłowemu wykonywaniu zadań spoczywających na tych organach na gruncie przepisów tej dyrektywy.

Uzasadniając wniosek o zmianę przepisów prawa polskiego w związku ze wskazanym wyrokiem TSUE, Prezes UODO chciałby zwrócić na wstępie uwagę, że już we wcześniejszych orzeczeniach TSUE - mając na uwadze postanowienia art. 7, 8 oraz 52 ust. 1 KPP, a przy tym także m.in. dyrektywy 2002/58/WE, wypowiadał się na temat konieczności zapewnienia proporcjonalności przyjętych rozwiązań prawnych w obszarze dostępu służb ochrony państwa do danych objętych tajemnicą telekomunikacyjną i wskazywał na przesłanki legalizujące taki dostęp. Najistotniejsze orzeczenia TSUE w tym zakresie to: wyrok z 13 czerwca 2024 r. w sprawie C-229/23 HYA i in. II, wyrok z 30 kwietnia 2024 r. w sprawie C-470/21 La Quadrature du Net i in. przeciwko Premier Ministre i Ministere de la Culture, 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, 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.

Mając na uwadze ww. orzecznictwo TSUE, organ nadzorczy sygnalizował już w minionym czasie konieczność dokonania zmiany przepisów krajowych uprawniających Policję do dostępu do danych³, w tym danych telekomunikacyjnych, to jest regulacji: ustawy o Policji (art. 19 ustawy o Policji⁴, 20c ustawy o Policji), Prawa telekomunikacyjnego (180c, art. 180d prawa telekomunikacyjnego⁵), czy Kodeksu postępowania karnego (art. 218 § 1 k.p.k., 236a k.p.k.).

W związku z powyższym, zważywszy na wyrok TSUE w sprawie C-548/21, a także dotychczasowe orzecznictwo TSUE oraz prezentowane stanowiska organu nadzorczego, należy wskazać, że przepisy postępowania karnego przewidują, że we wszczętym postępowaniu przygotowawczym Policja może uzyskać dostęp do urządzeń i danych telekomunikacyjnych za pośrednictwem prokuratora (art. 217 § 1 Kodeksu postępowania karnego⁶, art. 218 § 1 w zw. z 236a Kodeksu postępowania karnego). Jednocześnie, na podstawie art. 19 ustawy o Policji Policja może uzyskać dostęp do informacji i danych (w tym danych telekomunikacyjnych) w toku przeprowadzania czynności operacyjno-rozpoznawczych, a zatem także w postępowaniu sprawdzającym (art. 307 Kodeksu postępowania karnego).

³ Zob. opinie Prezesa UODO w podobnych sprawach: <https://uodo.gov.pl/pl/138/3524>, <https://uodo.gov.pl/pl/138/3252>, <https://uodo.gov.pl/pl/138/3219>, <https://uodo.gov.pl/pl/138/3126>

⁴ Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2024 r. poz. 145 ze zm.).

⁵ Ustawa z dnia 16 lipca 2024 r. – Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34 ze zm.).

⁶ Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 2024 r. poz. 37 ze zm.).

W myśl art. 19 ust. 6 ustawy o Policji, kontrola operacyjna ma na celu zapobieżenie, wykrycie, ustalenie sprawców, a także uzyskanie i utrwalenie dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw wskazanych w tym przepisie, jest prowadzona niejawnie i polega np. na: 1) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych; 2) uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne; 3) uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; 4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych; 5) uzyskiwaniu dostępu i kontroli zawartości przesyłek. Kontrolę działań Policji sprawuje sąd okręgowy.

Należy podkreślić, że **przyjęty w art. 19 ustawy o Policji model stosowania kontroli operacyjnej nie spełnia standardów ochrony: prawa do prywatności i prawa do ochrony danych osobowych wynikających z orzecznictwa TSUE.**

Regulacje te nie przewidują bowiem właściwych gwarancji ochrony prawa do prywatności. Mając na uwadze omawiany wyrok TSUE, należy wskazać, że przepisy te nie zapewniają właściwej kontroli sądowej, gdyż aktualnie nie ma konieczności uzasadnienia przez sąd postanowienia o zarządzeniu kontroli, co w konsekwencji powoduje, że **kontrola sądowa ma charakter iluzoryczny z punktu widzenia podmiotu danych.** Ponadto przepisy nie przewidują możliwości poinformowania osoby, wobec której była przeprowadzona kontrola operacyjna, a także nie zapewniają możliwości złożenia środka odwoławczego. Dodatkowe zastrzeżenia budzi również katalog przestępstw, których podejrzenie popełnienia może stanowić podstawę do przeprowadzenia kontroli operacyjnej.

Wymaga przy tym podkreślenia, że przepisy ustawy o Policji były przedmiotem oceny **Europejskiego Trybunału Praw Człowieka, który wyrokiem z 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce** (skargi nr 72038/17 i 25237/18) orzekł naruszenie art. 8 EKPC, tj. prawa do poszanowania życia prywatnego, rodzinnego oraz korespondencji⁷. Trybunał stwierdził, że prawo krajowe nie zapewniało wystarczających zabezpieczeń przed nadmierną ingerencją w życie prywatne jednostek, a także w odniesieniu do komunikacji objętej tajemnicą adwokacką. Brak takich gwarancji nie został dostatecznie zrównoważony przez istniejący mechanizm kontroli sądowej. Trybunał zauważył, że obowiązujące przepisy nie wymagały od sądu rozpatrującego wniosek o zezwolenie na inwigilację potwierdzenia, czy istnieje „uzasadnione podejrzenie” w odniesieniu do osoby, której dotyczy wniosek, a w szczególności zbadania, czy istnieją jakiegokolwiek dowody na to, że osoba ta planuje, dokonuje lub dokonała czynów przestępczych lub jakiegokolwiek innego przestępstwa pozwalającego na zastosowanie środków tajnej inwigilacji, takich jak czyny zagrażające bezpieczeństwu narodowemu. Ponadto

⁷ Zob. też inne np. wyrok ETPC z 12.01.2023 w sprawie Potoczka i Adamčo przeciwko Słowacji, skarga nr 7286/16.

Trybunał uznał, że istniejąca procedura wydawania zgód powinna zostać uzupełniona o inne mechanizmy kontroli proceduralnej *post factum*. Zauważył jednocześnie, że w obecnym stanie prawnym, nie przewidziano obowiązku informowania osoby objętej środkiem kontroli, nawet po upływie określonego czasu i nawet w przypadku, gdy nie zagrażałoby to celowi, dla którego zastosowano ww. środek. ETPC wskazał przy tym, że prawo nie przewidywało skutecznego środka odwoławczego dla osób, które uważały, że zostały poddane tajnej inwigilacji.

Mając powyższe na uwadze, po analizie wyroku TSUE w sprawie C-548/21, w ocenie Prezesa UODO, konieczne jest podjęcie możliwie pilnie działań legislacyjnych mających na celu zapewnienie skutecznej ochrony prawa do prywatności i prawa do ochrony danych osobowych w odniesieniu do przepisów dotyczących stosowania przez organy Policji kontroli operacyjnej.

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 Ministra o odniesienie się do tego wystąpienia na **piśmie w terminie 30 dni** od daty jego otrzymania.

Z wyrazami szacunku
z up. Prezesa Urzędu
Ochrony Danych Osobowych
Zastępczyni Prezesa
dr hab. Agnieszka Grzelak

Załącznik:

1. Opinia Prezesa UODO z dnia 15 listopada 2025., sygn. akt DOL.0623.29.2021

Do wiadomości:

Pan Ignacy Niemczycki

Sekretarz Stanu

Kancelaria Prezesa Rady Ministrów