Warszawa, 16.06.2025 r.

**PREZES**
**URZĘDU OCHRONY**
**DANYCH OSOBOWYCH**
**Mirosław Wróblewski**

DPNT.0623.12.2025.

**Pan**
**Ignacy Niemczycki**
**Sekretarz Stanu**

**Kancelaria**
**Prezesa Rady Ministrów**

Szanowny Panie Ministrze,

w odpowiedzi na pismo z dnia 22 maja 2025 r., znak: DPUE.7313.191.2025.JH(1)(JS), ***w sprawie C-222/25 Rahapesu Andmebüroo***, w odniesieniu do pytań prejudycjalnych sądu estońskiego w zakresie stosowania przepisów 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.), (dalej: rozporządzenie 2016/679) oraz przepisów dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 4.5.2016, str. 89 ), (dalej: dyrektywa 2016/680), uprzejmie informuję, że Prezes UODO jako organ nadzorczy do spraw ochrony danych osobowych **dostrzega zasadność udziału w postępowaniu**.

**Uzasadnienie**

Sąd estoński przekazał do Trybunału Sprawiedliwości Unii Europejskiej (dalej: TSUE, Trybunał) sprawę, która zainicjowana została skargą X, w której skarżący wniósł o uchylenie decyzji i zarządzenia *Rahapesu Andmebüroo* (jednostki analityki finansowej w Estonii; dalej: RAB), na mocy których odmówiono przekazania dotyczących go danych.

X (skarżący) zażądał bowiem od RAB udzielenia informacji na temat tego, czy estońskim lub zagranicznym instytucjom kredytowym czy też zagranicznym organom przekazano o nim informacje dotyczące podejrzenia prania pieniędzy. Na zadane pytanie RAB odpowiedziała, że zgodnie z przepisami estońskimi nie może przekazywać żadnych danych zbieranych w ramach wykonywania swoich zadań ani też informacji o istnieniu lub ewentualnej wymianie takich danych, po czym następnie X (skarżący) zażądał od RAB udzielenia informacji o tym, czy do jednostki tej wpłynęły dotyczące go zarządzenia lub zapytania estońskich lub zagranicznych instytucji kredytowych czy też zagranicznych organów w odniesieniu do podejrzenia prania pieniędzy. X (skarżący) zwrócił się do RAB z pytaniem o to, na jakiej podstawie opiera się ograniczenie dostępu do żądanych informacji, na co otrzymał od RAB informację, że ograniczenie dostępu wynika z przepisów estońskich[1], gdyż nie są spełnione przesłanki odstępstwa w odniesieniu do ujawnienia informacji.

X (skarżący) wniósł skargę do sądu administracyjnego, aby zobowiązać RAB do ponownego zbadania jego wniosku o udzielenie informacji. Sąd administracyjny w Tallinnie[2] oraz sąd apelacyjny w Tallinnie[3] oddaliły skargę, ale Sąd Najwyższy w Estonii[4] uchylił orzeczenia obu wskazanych powyżej sądów, uwzględnił skargę i zobowiązał RAB do wydania nowej decyzji w przedmiocie przekazania X żądanych danych.

Niezależnie od powyższego X złożył w RAB wniosek o udzielenie informacji, w którym pytał, czy RAB w latach 2012–2015 utworzyła dotyczącą go dokumentację kontrolną i czy zwracała się z zapytaniami do Stanów Zjednoczonych. Po tym jak także w tej sprawie RAB oddaliła wniosek, X (skarżący) złożył skargę administracyjną do estońskiego organu nadzorczego[5] (dalej jako: AKI). AKI uwzględnił skargę administracyjną i zobowiązał RAB do ponownego zbadania wniosku o udzielenie informacji, zaś RAB ponownie oddalił wniosek o udzielenie informacji, po czym X (skarżący) ponownie wniósł skargę administracyjną do AKI.

AKI wydał decyzję w przedmiocie skargi administracyjnej i zastosował środek tymczasowy, na mocy którego zobowiązał podmiot posiadający żądane informacje do ich przekazania. AKI uzasadnił swoją decyzję tym, że prawa osoby, której dane dotyczą, nie mogą być ograniczane na podstawie § 60 ust. 1 RahaPTS[6], a

---

[1] *Z Rahapesu ja terrorismi rahastamise tõkestamise seadus* (**ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu**, zwanej dalej „RahaPTS"), dokładnie z § 60 ust. 1 RahaPTS, gdyż nie są spełnione określone w § 60 ust. 2–7 RahaPTS przesłanki odstępstwa w odniesieniu do ujawnienia informacji.

[2] Est. *Tallinna Halduskohus*.

[3] Est. *Tallinna Ringkonnakohus*.

[4] Est. *Riigikohus.*

[5] Est. *Andmekaitse Inspektsioon.*

[6] Brak przywołanego brzmienia przepisów w całej sprawie, wobec czego niniejsza analiza oparta jest na opisowym ich przywoływaniu w przedłożonej do zaopiniowania dokumentacji.

ograniczenie praw osoby, której dane dotyczą, bezpośrednio na podstawie art. 23 rozporządzenia 2016/679 nie jest możliwe, chyba że dokonałby go ustawodawca państwa członkowskiego.

RAB wydała także decyzję, w której odmówiła X (skarżącemu) udzielenia informacji co do tego, czy RAB posiada o nim informacje i ewentualnie jakie. W decyzji tej RAB wyjaśniła, że jest zobowiązana do poufnego traktowania informacji znajdujących się w jej bazie danych, aby zapewnić integralność otoczenia biznesowego oraz chronić estoński system finansowy i estoński obszar gospodarczy jako całość. Celem § 60 ust. 1 RahaPTS w ocenie RAB jest natomiast ograniczenie dostępu do informacji zawartych w bazie danych RAB wszystkim osobom i podmiotom niewymienionym w ustawie, aby przeciwdziałać praniu pieniędzy i finansowaniu terroryzmu. W ramach walki z tymi niebezpiecznymi formami przestępczości kluczowe jest utrzymywanie w tajemnicy wszystkich danych przekazywanych RAB i zbieranych przez RAB.

Z okoliczności przedmiotowej sprawy wynika także, że RAB wydała zarządzenie, w którym dostęp do danych ujętych w jej bazie danych został ograniczony również z mocą wsteczną, a dane określone w statucie bazy danych RAB uznano za informacje przeznaczone do wyłącznego użytku wewnętrznego organów.

Sąd estoński zadał następujące pytania prejudycjalne we wskazanych powyżej okolicznościach faktycznych i prawnych:

1. Czy wykładni art. 2 ust. 2 lit. d) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych; zwanego dalej „RODO”) i art. 2 ust. 1 w związku z art. 1 dyrektywy 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 uchylającej decyzję ramową Rady 2008/977/WSiSW należy dokonywać w ten sposób, że ewentualne przetwarzanie danych osobowych przez jednostkę analityki finansowej może stanowić przetwarzanie danych osobowych przez właściwy organ do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, nawet jeżeli jednostka analityki finansowej nie jest organem dochodzeniowo-śledczym
w rozumieniu kodeksu postępowania karnego?

2. Czy wykładni art. 23 ust. 2 lit. h) RODO i art. 15 ust. 3 dyrektywy 2016/680 należy dokonywać w ten sposób, że osobie, której dane dotyczą, w postępowaniu administracyjnym lub w postępowaniu sądowym można odmówić ujawnienia również aktu prawnego, na podstawie którego odmówiono jej informacji o dotyczących jej danych osobowych, aby zapobiec zarówno potwierdzeniu przetwarzania dotyczących jej danych osobowych, jak i zaprzeczeniu temu faktowi, jeżeli osoba, której dane dotyczą, nie wie, czy takie przetwarzanie miało miejsce, oraz czy można w takim wypadku nie udzielić takiej osobie, której dane dotyczą, również informacji o tym, czy może skorzystać z prawa przewidzianego w art. 17 ust. 1 dyrektywy 2016/680?

3. Czy wykładni art. 15 dyrektywy 2016/680 czy też art. 23 RODO należy dokonywać w ten sposób, że jest z nimi zgodny przepis krajowy, który upoważnia dyrektora jednostki analityki finansowej do ograniczenia praw osoby, której dane dotyczą, i w wypadku którego cel, przesłanki, a także czasowy i przestrzenny zakres ograniczenia praw osoby, której dane dotyczą, są wyrażone w związku z innymi przepisami, w tym przepisami niższego rzędu?

4. Czy wykładni art. 15 dyrektywy 2016/680 czy też art. 23 RODO należy dokonywać w ten sposób, że jest z nimi zgodny przepis krajowy, który ogranicza wykonywanie prawa przewidzianego w art. 14 dyrektywy 2016/680 czy też art. 15 RODO aż do momentu zniszczenia danych w pełnym zakresie, w związku z czym osoba, której dane dotyczą, nie ma możliwości, aby kiedykolwiek uzyskać informację o tych danych?

**Ad 1**

Na wstępie należy zaznaczyć, że zgodnie z art. 2 ust. 2 lit. d rozporządzenia 2016/679 rozporządzenie to nie ma zastosowania do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Przepisy zaś o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom ustanowione zostały w dyrektywie 2016/680, która zastosowanie ma do właściwych organów do realizacji wskazanych powyżej celów tej dyrektywy. Właściwymi organami są natomiast – w myśl art. 3 pkt 7 dyrektywy 2016/680:

1) organ publiczny właściwy do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom;

2) inny organ lub podmiot, któremu prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony

przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom;

Administratorem zaś – zgodnie z art. 3 pkt 8 dyrektywy 2016/680 – może być jedynie organ właściwy, o którym mowa była wcześniej.

Zgodnie natomiast z art. 8 ust. 1 dyrektywy 2016/680 państwa członkowskie zapewniają, by przetwarzanie było zgodne z prawem wyłącznie wówczas i w zakresie, w jakim jest ono niezbędne do wykonania zadania realizowanego przez właściwy organ w celach określonych w art. 1 ust. 1 tej dyrektywy oraz ma podstawę w prawie Unii lub prawie państwa członkowskiego, a więc wyraźnie odnosi się do działań właściwych organów i wyłącznie do celu, o którym mowa w art. 1 ust. 1 dyrektywy. Ustawodawstwo zaś krajowe, które stanowi implementację dyrektywy 2016/680, musi określać co najmniej powody przetwarzania, dane osobowe mające podlegać przetwarzaniu oraz cele przetwarzania, zaś z okoliczności przedstawionych w niniejszej sprawie wynika, że ustawodawstwo estońskie nie czyni temu zadość.

Mając jednak powyższe na uwadze, należy zaznaczyć, że w przypadku rozpatrywanej przez Trybunał jednej ze spraw[7] wskazano, że przetwarzanie danych osobowych przez organ publiczny, takie jak to, którego dokonuje wysoki urząd ds. rozpowszechniania utworów i ochrony praw w Internecie[8] w ramach stosowanej procedury, musi być zgodne z dotyczącymi ochrony tych danych przepisami szczególnymi przewidzianymi w dyrektywie 2016/680, której celem jest, stosownie do jej art. 1, ustanowienie przepisów o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. W okolicznościach powołanej sprawy Trybunał uznał, że przywołany powyżej francuski urząd – nawet jeżeli na podstawie właściwego prawa krajowego nie posiada własnych uprawnień decyzyjnych – w sytuacji, gdy w ramach stosowanej procedury przetwarza dane osobowe i stosuje środki takie jak kierowanie zaleceń czy informowanie osoby, której dane dotyczą, że odnośne czyny mogą być przedmiotem ścigania, jest „organem publicznym” w rozumieniu art. 3 dyrektywy 2016/680, zaangażowanym w zapobieganie czynom zabronionym i wykrywanie takich czynów, a mianowicie wykroczeń w postaci rażącego niedbalstwa czy występków w postaci naruszenia praw własności intelektualnej, w związku z czym jest objęty zakresem stosowania tej dyrektywy zgodnie z jej art. 1.

Wobec powyższego należy wskazać, że mając na uwadze dotychczasowe orzecznictwo TSUE można dopuścić, iż organy niemające stricte dochodzeniowo-

---

[7] Wyrok TSUE z 30 kwietnia 2024 r., *La Quadrature du Net*, C-470/21, ECLI:EU:C:2024:370, pkt 158.

[8] *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet*. Jest to niezależny organ publiczny, który realizuje następujące zadania: 1) zadania w zakresie wspierania rozwoju zgodnej z prawem oferty i w zakresie nadzorowania zgodnego i niezgodnego z prawem korzystania z utworów i przedmiotów, z którymi związane jest prawo autorskie lub prawo pokrewne, w sieciach łączności elektronicznej wykorzystywanych do świadczenia usług internetowej komunikacji publicznej; 2) zadania w zakresie ochrony tych utworów i przedmiotów przed naruszeniami tych praw w sieciach łączności elektronicznej wykorzystywanych do świadczenia usług internetowej komunikacji publicznej;

śledczych uprawnień mogą także w rozumieniu art. 3 dyrektywy 2016/680 być uznawane za właściwe organy realizujące działania związane z zapobieganiem przestępczości. W okolicznościach powołanej dla przykładu sprawy francuskiej na pytanie Trybunału rząd francuski wskazał, że ze względu na to, iż środki stosowane przez wskazywany w tej sprawie urząd w ramach jego działania „poprzedzają postępowanie karne, mając bezpośredni związek z postępowaniem sądowym", wdrażany przez ten urząd system zarządzania środkami ochrony utworów w Internecie podlega przepisom prawa krajowego mającym na celu transpozycję dyrektywy 2016/680, **jednak** – co należy podkreślić – **tylko w tym zakresie**.

Odpowiadając na pytanie sądu krajowego, **należy** – w ocenie Prezesa Urzędu Ochrony Danych Osobowych – **przyjąć, mając na uwadze zakres danych przetwarzanych przez podmiot analityki finansowej, a także różne cele w jakich te dane mogą być przez ten organ przetwarzane, że działania realizowane przez ten podmiot nie mogą być wszystkie uznane jako te, które realizują cele dyrektywy 2016/680. Możliwe zatem jest również podleganie pod przepisy rozporządzenia 2016/679.** Zgodnie bowiem z motywem 38 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/843 z 30 maja 2018 r. zmieniającej dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniającej dyrektywy 2009/138/WE i 2013/36/UE (Dz. Urz. UE L 156 z 19.6.2018 s. 43) do przetwarzania danych osobowych w ramach powołanej dyrektywy stosuje się przepisy rozporządzenia 2016/679.

Ponadto należy dodać, że sprawa C-470/21 rozpatrywana przez Trybunał była także przedmiotem analizy, a także oceny skutków wyroku polskiego organu nadzorczego[9]. Mimo, ż francuski urząd, którego dotyczyło postępowanie w powołanej wyżej sprawie, nie ma swojego odpowiednika w polskim porządku prawnym, to ważną kwestią poruszoną przez organ nadzorczy było posiadanie przez ów organ także kompetencji do ścigania przestępstw przeciwko prawom własności intelektualnej i bycie organem publicznym w rozumieniu art. 3 dyrektywy 2016/680. W świetle bowiem przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2025 r. poz. 24) organami publicznymi powołanymi do ścigania przestępstw stypizowanych w art. 115 i kolejnych tej ustawy są organy ścigania. W konsekwencji zaś do ich działania w tym zakresie zastosowanie znajdują wskazania płynące z powołanego wyroku TSUE. Organy prowadzące postępowania karne z tego zakresu nie są zatem objęte przepisami rozporządzenia 2016/679, lecz podlegają przepisom ustawy 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), stanowiącej implementację[10] dyrektywy 2016/680. Przesłanka legalności ich działania wynika z art. 13 ust. 1 powołanej ustawy, zgodnie z którym

[9] Pismo Departamentu Orzecznictwa i Legislacji UODO z 27 października 2021 roku, znak: DOL.0623.15.2021.PD, a także pismo Prezesa Urzędu Ochrony Danych Osobowych z 11 czerwca 2024 roku, znak: DOL.0623.15.2021.WL.RB.

[10] Krytykowaną przez organ nadzorczy, zob. pismo Prezesa Urzędu Ochrony Danych Osobowych z 7 lutego 2022 roku (znak: DOL.413.4.2022.WL.AG).

właściwe organy przetwarzają dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Odpowiadając na pytanie zadane Trybunałowi, w ocenie Prezesa UODO instytucja analityki finansowej, taka jak wskazana w okolicznościach faktycznych postępowania głównego, nie działała na zasadach dotyczących organu ścigania karnego i w trybie przepisów procedury karnej. Z powyższego wynika zatem, że zasadny jest wniosek zmierzający do oceny działania tej instytucji na podstawie przepisów rozporządzenia 2016/679 i nie korzysta ona z wyłączenia wskazanego w art. 2 ust. 2 lit. d tego aktu. Wniosek taki wypływa również z treści motywu 11 dyrektywy 2016/680.

**Ad 2.**

W myśl art. 15 rozporządzenia 2016/679 osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania do nich dostępu. Podobne prawo gwarantuje się osobie, której dane dotyczą, w art. 8 ust. 2 Karty Praw Podstawowych UE (dalej: „KPP"). Artykuł 23 rozporządzenia 2016/679 umożliwia ograniczenie aktem prawnym prawa osoby, której dane dotyczą, przewidzianego w art. 15 rozporządzenia 2016/679, jeżeli służy to określonym interesom publicznym. Takim interesem publicznym jest ważny interes gospodarczy lub finansowy Unii lub państwa członkowskiego [art. 23 ust. 1 lit. e rozporządzenia 2016/679]. Jakkolwiek w myśl motywu 41 rozporządzenia 2016/679 możliwe jest takie podejście do interpretacji przepisów rozporządzenia, że użyte w nim wyrazy „podstawa prawna" lub „akt prawny" niekoniecznie oznaczać muszą przyjęcie aktu prawnego przez parlament[11]. W takim wypadku wdrożenie aktu prawnego muszą regulować odpowiednie przepisy, w których należy określić, kto, w jaki sposób i w jakim okresie może przetwarzać jakie dane, nie udzielając osobie, której one dotyczą, informacji na ten temat.

Powyższa kwestia była także przedmiotem orzeczenia TSUE w innej sprawie[12]. Trybunał wyjaśnił w tej sprawie, że jeżeli prawo podstawowe może być ograniczone jedynie ustawą, oznacza to, że podstawa prawna, która pozwala na ingerencję w te prawa, musi sama określać zakres ograniczenia wykonywania danego prawa. Jednocześnie ograniczenie to może być sformułowane w sposób wystarczająco otwarty, tak, aby można je było dostosować do różnych przypadków, jak i do zmieniających się sytuacji. Zbieranie, posiadanie i udostępnianie informacji na podstawie dyrektywy w sprawie przeciwdziałania praniu pieniędzy muszą czynić w pełni zadość wymogom wynikającym z rozporządzenia 2016/679. Ponadto, by zadośćuczynić wymogowi proporcjonalności, dane uregulowanie zawierające ingerencję musi również zawierać jasne i precyzyjne reguły dotyczące zakresu i sposobu stosowania rozpatrywanych środków, a także ustanawiać minimalne wymogi służące temu, aby osoby, których dane zostały przekazane, miały

---

[11] Z zastrzeżeniem wymogów wynikających z porządku konstytucyjnego danego państwa członkowskiego.

[12] Wyrok TSUE z 22 listopada 2022 r., *Luxembourg Business Registers*, C-37/20 i C-601/20, EU:C:2022:912.

wystarczające gwarancje rzeczywistej ochrony swoich danych osobowych przed ryzykiem niewłaściwego wykorzystania. Zgodnie bowiem z art. 52 ust. 1 KPP wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w KPP muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

Przepisy te muszą także – zgodnie z art. 23 ust. 2 lit. h[13] rozporządzenia 2016/679 – regulować kwestie dotyczące prawa osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia. Natomiast dyrektywa 2016/680 w art. 15 ust. 1 przewiduje, że państwa członkowskie mogą przyjmować akty prawne pozwalające ograniczyć w całości lub w części prawo dostępu osoby, której dane dotyczą, w takim stopniu i przez taki okres, w jakim takie częściowe lub całkowite ograniczenie jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej. Cele uzasadniające przyjęcia takich zasad przez ustawodawcę są następujące:

1) uniemożliwienie utrudnienia czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;
2) uniemożliwienie zakłócania zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar;
3) ochrona bezpieczeństwa publicznego;
4) ochrona bezpieczeństwa narodowego;
5) ochrona prawa i wolności innych osób.

Powyższe przesłanki uzasadniają jednak, jak wskazano powyżej, jedynie ograniczenie w odpowiednim zakresie prawa dostępu do danych i to w takim stopniu, a także przez taki okres, w jakim tego typu działanie ze strony państwa jest proporcjonalne oraz nie narusza istoty praw i wolności oraz uzasadnionych interesów podmiotu danych. W okolicznościach badanej sprawy niedopuszczalne jest zatem całkowite pozbawienie podmiotu danych prawa dostępu do danych.

W okolicznościach, o których mowa powyżej, konieczne jest zapewnienie przez państwo członkowskie, aby administrator bez zbędnej zwłoki poinformował pisemnie osobę, której dane dotyczą, o każdej odmowie lub o każdym ograniczeniu dostępu i o przyczynach tej odmowy lub tego ograniczenia (art. 15 ust. 3 dyrektywy 2016/680). Informacje takie można pominąć, jeżeli ich udzielenie godziłoby w którykolwiek z celów, o których mowa powyżej (1-5). Państwa członkowskie

[13] Z dokumentacji przedstawionej w przedmiotowej sprawie zawarto jedynie informacje o tym, że statut bazy danych RAB zawiera listę kategorii danych osobowych, które mają być ujęte w bazie danych (§§ 8–17), wyznacza administratora odpowiedzialnego za przetwarzanie (§ 6 ust. 1) i określa środki ochrony danych osobowych poprzez klasyfikację danych w zakresie bezpieczeństwa (§ 5 ust. 2). Są to jednak elementy aktu prawnego wymagane w art. 23 ust. 2 lit. b, d i e rozporządzenia 2016/679.

zapewniają wówczas, by administrator informował osobę, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu.

Ponadto należy wskazać, że przepisy krajowe w kontekście brzmienia motywu 45 oraz art. 15 ust. 3 dyrektywy 2016/680 wskazują na możliwość odmowy i ograniczenia dostępu do danych, jednakże jest to związane z jednoczesnym zobowiązaniem administratora danych do powiadomienia na piśmie osoby, której dane dotyczą o tym fakcie, a także o podstawie faktycznej i prawnej takiej decyzji.

W takiej sytuacji **możliwość zastosowania przez osobę, której dane dotyczą, możliwości zwrócenia się do organu nadzorczego w trybie art. 17 ust. 1 dyrektywy 2016/680 wydaje się wręcz zasadna**, by zapewnić w takiej sytuacji realizację przesłanki należytego uwzględnienia praw podstawowych i uzasadnionych interesów osoby fizycznej. **O uprawnieniu wynikającym z powołanego powyżej przepisu podmiot danych musi być bezwzględnie poinformowany, w tym także o kwestiach wynikających z motywu 45 i art. 15 ust. 3 dyrektywy 2016/680, o których mowa powyżej.**

**Ad 3.**

Odnosząc się do tej części odesłania prejudycjalnego należy wskazać, że w części dotyczącej pytania 2 organ nadzorczy wypowiedział się w zakresie możliwości ograniczenia praw osób, których dane dotyczą, gdyż taka możliwość wynika wprost z art. 23 RODO oraz dyrektywy 2016/680. Taka była właśnie intencja prawodawcy unijnego, niemniej dla przeciwwagi muszą być określone odpowiednie gwarancje, a także prawo realizacji swoich uprawnień podmiotu danych za pośrednictwem organu nadzorczego, który jest gwarantem realizacji praw i wolności w obszarze przetwarzania danych takiej osoby.

Ponadto należy zaznaczyć, że w ocenie Trybunału osoba, której dane dotyczą, powinna być w stanie określić okoliczności i warunki, w jakich istnieje prawo do ograniczenia prawa do informacji o własnych danych[14]. Przepisy estońskie zaś – jak wynika z okoliczności sprawy – weszły w życie przed rozpoczęciem stosowania przepisów rozporządzenia 2016/679. Ustawodawca nie określił, w ramach jakich czynności RAB przetwarza dane osobowe, z jakich powodów uzyskanie informacji o przetwarzaniu danych osobowych jest wykluczone oraz jak długo trwa ograniczenie.

Dodatkowo należy podkreślić, że zgodnie z motywem 7 zd. 3 dyrektywy 2016/680 ustawodawca unijny założył, że w celu zapewnienia skuteczności ochrony danych osobowych w Unii celowe jest wzmocnienie praw osób, których dane dotyczą, oraz obowiązków podmiotów, które przetwarzają dane osobowe, jak i odpowiadających im uprawnień w zakresie monitorowania i egzekwowania przepisów o ochronie danych osobowych w państwach członkowskich, a co za tym idzie ustawodawca unijny dostrzega potrzebę zabezpieczenia praw osób, których dane dotyczą nawet w sytuacji gdy dane te przetwarzane są do realizacji celów, o których mowa w art. 1 ust. 1 dyrektywy 2016/680.

[14] Wyrok TSUE z 24 lutego 2022 r., *Valsts ieņēmumu dienests*, C-175/20, EU:C:2022:124, pkt 56.

Kompetencja organu nadzorczego, o której mowa na wstępie analizy dotyczącej pytania 3, jest kluczowa jeśli chodzi o zadania i cele dyrektywy 2016/680, ale także wymaga utworzenia przez państwa członkowskie takich organów, które mają możliwość wykonywania swych funkcji w sposób całkowicie niezależny, gdyż zgodnie z motywem 75 powołanej dyrektywy jest to zasadniczy element ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

**Ad 4.**

Jak wynika z wcześniejszej analizy, ograniczenie praw osób, których dane dotyczą jest możliwe w określonych i omówionych we wcześniejszej części niniejszego stanowiska okolicznościach. Zniszczenie (usunięcie) jednak danych bez poinformowania o tym podmiotu danych stanowi naruszenie praw i wolności tego podmiotu.

Jak wynika z przedłożonej dokumentacji w sprawie ustawodawca estoński[15] miał na celu ograniczenie dostępu, które umożliwia również ograniczenie praw osoby, której dane dotyczą. W przepisie tym nie określono jednak wyraźnie ani przesłanek, przy spełnieniu których dyrektor RAB może podjąć taką decyzję, ani czasowego i przedmiotowego zakresu ograniczenia dostępu, wobec czego przepis ten uznać należy za niepełny, o czym już była mowa we wcześniejszej części stanowiska.

Ograniczenie praw osoby, której dane dotyczą, może faktycznie trwać aż do upływu terminów przechowywania danych, określonych w § 26 statutu bazy danych RAB, które co do zasady wynosi 15 lat. Brak jakiejkolwiek możliwości wniesienia przez osobę, której dane są przetwarzane w oparciu o przepisy regulujące zapobieganie przestępczości, zażalenia do sądu w ocenie organu nadzorczego stanowi zaniechanie prawodawcze. Wyeliminowanie tego zaniechania jest obowiązkiem ustawodawcy związanym z koniecznością zapewnienia zgodności przepisów prawa ze standardami ochrony prywatności jednostki. W świetle tych standardów nie może być tak, że osoba, której dane były przetwarzane, w związku z działaniami mającymi na celu zapobieganie przestępczości, jest całkowicie pozbawiona prawa do wniesienia środka, który otworzy drogę do sądowej kontroli takich działań. Poza tym w sprawach podobnych, niejednokrotnie podejmowanych już przez Trybunał, bardzo ważną kwestią jest także obowiązek następczego informowania o działaniach podejmowanych wobec konkretnej osoby**.**

W ocenie Prezesa UODO należy uznać, że udział Polski w postępowaniu w ***sprawie C-222/25 Rahapesu Andmebüroo*** może być rozważany w kontekście niezmienionego brzmienia przepisów ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2025 r., poz. 644), z której nie wynika jasno, czy osoba, której dane osobowe były przetwarzane (w tym udostępnione) przez instytucję finansową, ma prawo do skorzystania z prawa do uzyskania informacji na temat okoliczności takiego przetwarzania na podstawie rozporządzenia 2016/679, czy ustawy wdrażającej

[15] W§ 60 ust. 1 zdanie drugie RahaPTS.

dyrektywę 2016/680. W przypadku bowiem polskich przepisów należy wskazać, że w ustawie z 1 marca 2018 r. znajduje się wyłącznie jeden przepis zawierający wyłączenie stosowania przepisów o ochronie danych osobowych. Jest nim art. 66 tej ustawy, zgodnie z którym do przetwarzania danych osobowych zgromadzonych w Centralnym Rejestrze Beneficjentów Rzeczywistych nie stosuje się przepisów art. 15 ust. 1 lit. c rozporządzenia 2016/679[16]. Pośrednio jedynie ustawodawca nawiązuje do uprawnień informacyjnych przysługujących podmiotowi danych, niemniej nie rozstrzyga to zasadniczych wątpliwości interpretacyjnych, który z ww. aktów prawa unijnego znajduje zastosowanie w pozostałym zakresie. Należy także wskazać, że wyłączenie, o którym mowa powyżej, a mianowicie wyłączenie stosowania art. 15 ust. 1 lit. c rozporządzenia 2016/679 w polskich przepisach o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu budzi także wątpliwości w zakresie zgodności tego wyłączenia z art. 23 rozporządzenia 2016/679, gdyż w obrębie tego wyłączenia znaleźć się mogą osoby, wobec których nie jest prowadzone żadne postępowanie, a prawa tych osób muszą być realizowane zgodnie z zasadami wynikającymi z przywołanego rozporządzenia.

Ponadto także należy zaznaczyć, że 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) w sposób nieprawidłowy implementowała dyrektywę 2016/680, co niewątpliwie wymaga uwagi i zaangażowania polskiego ustawodawcy[17], zwłaszcza w kontekście przyjętego brzmienia art. 3 tej ustawy wyłączającego jej stosowanie we wskazanym zakresie i w konsekwencji ograniczającego także kompetencje organu właściwego ds. ochrony danych osobowych.

Łączę wyrazy szacunku,

Mirosław Wróblewski

Prezes

Urzędu Ochrony Danych Osobowych

[16] „15.1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji: c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;”.

[17] Sygnalizowane przez Prezesa Urzędu Ochrony Danych Osobowych przy okazji prac nad projektem ustawy o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (UD 153), https://uodo.gov.pl/pl/138/3494 (dostęp 12.06.2025).