Warszawa,

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

DOL.413.5.2024

Pan
Marcin Łoboda
Sekretarz Stanu
Szef Krajowej Administracji
Skarbowej

Ministerstwo Finansów
ul. Świętokrzyska 12
00-916 Warszawa

Szanowny Panie Ministrze,

w odpowiedzi na pismo Pana Ministra dotyczące wystąpienia Prezesa Urzędu Ochrony Danych Osobowych z 1 lipca br. w przedmiocie **podjęcia przez Ministerstwo Finansów prac legislacyjnych prowadzących do nowelizacji art. 46a oraz art. 48 ustawy o KAS**[1] **celem dostosowania tych przepisów do wymogów ochrony danych osobowych oraz ochrony prywatności wynikających z Konstytucji RP oraz rozporządzenia 2016/679**[2]**, z uwzględnieniem orzecznictwa Trybunału Konstytucyjnego, Trybunału Sprawiedliwości Unii Europejskiej i Europejskiego Trybunału Praw Człowieka,** uprzejmie dziękuję za wyjaśnienia dotyczące zagadnień poruszonych w tym wystąpieniu. Jednocześnie przedstawiam uprzejmie następujące uwagi.

Odnosząc się do otrzymanych wyjaśnień pragnę poinformować, że w opinii organu nadzorczego (Prezesa UODO) nie można zgodzić się ze stwierdzeniem, że

[1] Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2023 r. poz. 615 ze zm.), dalej: „ustawa o KAS".
[2] 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.), dalej: „rozporządzenie 2016/679".

obecne brzmienie **art. 46a ustawy o KAS dotyczące wymiany informacji pomiędzy ministrem właściwym ds. zdrowia a organami KAS** wyklucza przyjmowanie jako podstawy prawnej przez Szefa Krajowej Administracji Skarbowej tego przepisu do pozyskiwania danych osobowych, o których mowa w art. 9 rozporządzenia 2016/679, tj. danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Brzmienie tego przepisu jest na tyle ogólne, że można z niego wywieść również przetwarzanie ww. danych osobowych („dokonują wymiany informacji (…) w zakresie niezbędnym do realizacji ich ustawowych zadań"). Literalna wykładnia art. 46a ustawy o KAS wskazuje na możliwość pozyskiwania na jego podstawie danych osobowych wymienionych w art. 9 rozporządzenia 2016/679. Należy mieć też na uwadze, że celem omawianej regulacji jest zapewnienie KAS dostępu do informacji i danych koniecznych do realizacji jej zadań, natomiast ustawa o KAS uprawnia ministra właściwego ds. finansów i Szefa KAS do prowadzenia m.in. działalności analitycznej, prognostycznej i badawczej (art. 14 ust. 1 pkt 20 i art. 12a ustawy o KAS).

W ocenie organu nadzorczego, jeżeli art. 46a ustawy o KAS rzeczywiście nie stanowi podstawy do przetwarzania danych osobowych w wyżej opisany sposób, powinno to wynikać wprost z jego treści – **przepisy ustawy o KAS powinny jasno wyłączać przetwarzanie danych osobowych określonych w art. 9 ust. 1 rozporządzenia 2016/679 na podstawie ww. art. 46a**. Ponownie podkreślić należy, że postulowane rozwiązanie jest istotne z punktu widzenia zasad przetwarzania danych osobowych wyrażonych w art. 5 rozporządzenia 2016/679, w szczególności zasad zgodności z prawem, rzetelności i przejrzystości oraz zasady minimalizacji[3]. Jako przykład właściwej regulacji można tu wskazać art. 29 ust. 1 pkt 2 ustawy o NIK[4], który stanowi, że w celu dokonania czynności kontrolnych upoważnieni przedstawiciele Najwyższej Izby Kontroli mają prawo do m. in. przetwarzania danych osobowych, z wyjątkiem danych ujawniających poglądy polityczne, przekonania religijne lub światopoglądowe, jak również danych genetycznych, o nałogach, o seksualności lub o orientacji seksualnej.

Ustawodawca uwzględnił więc potrzebę ochrony danych osobowych szczególnej kategorii w przypadku realizacji zadań ustawowych przez Najwyższą Izbę Kontroli. **Powyższe przemawia za przyjęciem analogicznego rozwiązania w ustawie o KAS.**

[3] Zgodnie z art. 5 ust. 1 rozporządzenia 2016/679, dane osobowe muszą być m. in. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość") i adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych").
[4] Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2022 r. poz. 623).

Podkreślenia ponadto wymaga, że przetwarzanie danych osobowych przez organy KAS w celach analitycznych – w ocenie organu do spraw ochrony danych osobowych – powinno być dokonywane **wyłącznie na danych zanonimizowanych,** co również winno znaleźć odzwierciedlenie w przepisach prawa. Z kolei, gdyby przetwarzanie w ww. celach miało odbywać się na danych nieanonimowych, konieczne byłoby uwzględnienie w przepisach ustawy następujących elementów: 1) konkretnych zadań KAS, jakie są w ten sposób realizowane, 2) sposobów (procedur) przetwarzania danych dla realizacji takich zadań, 3) kategorii danych osobowych, przetwarzanych dla realizacji tych celów.

Przykładami prawidłowych regulacji w tym zakresie są art. 105a ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2023 r. poz. 2488 ze zm.) oraz art. 41 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2024 r. poz. 838). Powyższe przepisy regulują przetwarzanie danych osobowych w sposób zautomatyzowany, w tym poprzez profilowanie, i szczegółowo określają one m. in. cele przetwarzania danych oraz ich zakres. Choć wskazane przepisy dotyczą przetwarzania danych przez podmioty prywatne (tj. banki i zakłady ubezpieczeń), to ze względu na skalę wykonywanych na podstawie ustawy o KAS operacji przetwarzania i ich cele, stanowią one wzór właściwego, tj. dostosowanego do rozporządzenia 2016/679, uregulowania kwestii zautomatyzowanego przetwarzania danych, który powinien być uwzględniony przez ustawodawcę także przy ważeniu interesu państwa (realizowanego przez KAS) i prawa osób fizycznych do ochrony ich prywatności.

Wskazane wyżej **elementy powinny zostać zatem wyraźnie wyodrębnione w przepisach ustawy,** w szczególności z uwagi na fakt, że przetwarzania dokonuje podmiot publiczny, którego wszelkie władcze działania powinny znajdować podstawę w przepisach prawa o treści, która nie budzi wątpliwości. Podnoszona kwestia zyskuje tym większe znaczenie w perspektywie rozwoju technologii sztucznej inteligencji i jej ewentualnego wykorzystania do przetwarzania danych w celach analitycznych, a także szczególnych zasad przetwarzania danych osobowych wynikających z unijnego aktu o sztucznej inteligencji[5]. Raz jeszcze podkreślenia wymaga, że uwzględnienie powyższych elementów jest istotne z punktu widzenia norm konstytucyjnych, w szczególności art. 51, ustanawiającego prawo do ochrony danych osobowych, oraz art. 31 ust. 3 Konstytucji RP, regulującym warunki ograniczania przez ustawodawcę konstytucyjnych wolności i praw. Należy także wskazać na art. 7 Konstytucji RP, z którego wynika zasada działania organów władzy publicznej na podstawie w przepisach prawa. Z powołanych przepisów rangi konstytucyjnej wynika konieczność regulowania kompetencji podmiotu publicznego w sposób przejrzysty i wyczerpujący.

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. U. UE L z 2024 r. poz. 1689).

Odnosząc się zaś do wyjaśnień dotyczących **art. 48 ustawy o KAS i wynikającego z tego przepisu uprawnienia organów KAS do pozyskiwania informacji o rachunkach bankowych**, organ do spraw ochrony danych osobowych pragnie w pierwszej kolejności zauważyć, że wyjaśnienie, zgodnie z którym „celem znowelizowanego przepisu art. 48 ustawy o KAS jest ujednolicenie oraz doprecyzowanie uprawnień KAS w zakresie dostępu do informacji bankowych w przypadku, gdy organy KAS prowadzą postępowanie przygotowawcze dotyczące osoby fizycznej, osoby prawnej lub jednostki organizacyjnej niemającej osobowości prawnej w zakresie tej osoby fizycznej, osoby prawnej i jednostki niemającej osobowości prawnej, niezależnie albo zanim zostaną wszczęte procedury podatkowe (kontrola celno-skarbowa, kontrola podatkowa, postępowanie podatkowe)", nie może być uznane za wystarczające dla uzasadnienia obecnego brzmienia tego przepisu i tak głębokiej ingerencji w prywatność osób fizycznych. Przedmiotowa regulacja ma bowiem w gruncie rzeczy charakter blankietowy, stanowiąc w ust. 1 o związku z czynami popełnionymi w zakresie działalności m.in. osób fizycznych. Fakt, że dane dotyczące rachunków bankowych pozyskiwane są na podstawie art. 48 ustawy o KAS tylko w razie uzasadnionego podejrzenia popełnienia przestępstwa nie zmienia tego, że w ocenie organu do spraw ochrony danych osobowych **zakres podmiotowy tych danych tak ukształtowany jest zbyt ogólny i pozwala na gromadzenie informacji o osobach, które nie posiadają statusu osoby podejrzanej w prowadzonym przez organ KAS postępowaniu karnym**. Poszerzenie w 2022 r. przetwarzania danych osobowych pozyskiwanych na podstawie art. 48 ustawy o KAS, zarówno w aspekcie podmiotowym jak i przedmiotowym, nie wiązało się z uzasadnieniem przez projektodawcę niezbędności takiego rozwiązania, na co zwracał również uwagę Rzecznik Praw Obywatelskich.

Nie można się również zgodzić ze stwierdzeniem, że dane o rachunkach bankowych pozyskiwane na podstawie art. 48 ustawy o KAS nie mogą, choćby potencjalnie, ujawniać szczególnych kategorii danych osobowych. Jak wyjaśniono w wystąpieniu, dane te mogą ujawniać np. informacji o wpłatach na konkretne stowarzyszenia, partie polityczne, czy wydatkach związanych ze stanem zdrowia (dokonywanych np. w placówkach medycznych). Informacje te są wystarczające, aby uznać je za dane szczególnej kategorii w rozumieniu art. 9 rozporządzenia 2016/679. Analiza danych pochodzących z konta bankowego pozwala również KAS zidentyfikować informacje dotyczące wyroków skazujących oraz czynów zabronionych (np. dotyczące mandatów, nawiązek, grzywien i świadczeń pieniężnych płaconych przez osobę fizyczną), które stanowią dane chronione i powinny być przetwarzane na podstawie i na warunkach określonych w art. 10 rozporządzenia 2016/679[6], odzwierciedlonych w przepisach prawa krajowego.

[6] Zgodnie z art. 10 rozporządzenia 2016/679, przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą.

Podsumowując powyższe rozważania należy ogólnie stwierdzić, że przepisy ustawy o KAS powinny też być skonstruowane w sposób przejrzysty, aby wynikały z nich **kategorie przetwarzanych danych osobowych przyporządkowane do konkretnych zadań KAS.** Określenie w przepisach praw i obowiązków związanych z przetwarzaniem danych osobowych przyczyni się do realizacji zasad ich przetwarzania określonych w art. 5 rozporządzenia 2016/679, w szczególności wspomnianej już zasady przejrzystości zgodności z prawem, rzetelność i przejrzystości oraz zasady rozliczalności[7]. Przepisy kompetencyjne ustanawiające zadania organu władzy publicznej powinny w szczególności uwzględniać elementy wymienione w art. 6 ust. 3 rozporządzenia 2016/679[8], jako że właściwą przesłankę przetwarzania danych osobowych stanowi w takim przypadku jego art. 6 ust. 1 lit. c, tj. realizacja obowiązku prawnego ciążącego na administratorze. W szczególności przepisy ustawy o KAS powinny odzwierciedlać, poprzez regulacje szczegółowe, zapewnienie odpowiedniego stosowania rozporządzenia 2016/679, a także – w zakresie przetwarzania danych osobowych w związku z rozpoznawaniem i ściąganiem czynów zabronionych – odrębnie zapewnienie zgodności z przepisami 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), implementującej dyrektywę 2016/680[9]. Jednocześnie należy mieć na względzie problem odpowiedniego wdrożenia przez ustawodawcę dyrektywy 2016/680 oraz zgodności jej przepisów z powołaną wyżej ustawą.

Wyrażam nadzieję, że uwagi przedstawione w niniejszym piśmie okażą się pomocne i przyczynią się one do zmiany analizowanych przepisów, a przez to zmiany modelu przetwarzania danych osobowych na podstawie ustawy o KAS, zgodnie z postulatami wyrażonymi w moim wystąpieniu z 1 lipca br.

---

[7] Zgodnie z art. 5 ust. 2 rozporządzenia 2016/679 administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

[8] „Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona: a) w prawie Unii; lub b) w prawie państwa członkowskiego, któremu podlega administrator.
Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) - musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.”

[9] 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 uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE L 119 4.5.2016, str. 89 ze zm.).

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/

Urząd Ochrony
Danych Osobowych
ul. Stawki 2
00-193 Warszawa

tel. 22 531-03-88
fax 22 531-03-99

www.uodo.gov.pl