Warszawa, 29 listopada 2022 r.

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Jan Nowak

DOL.401.612.2020.WL.MW

Pan
Andrzej Kosztowniak
Przewodniczący
Komisji Finansów Publicznych
Kancelaria Sejmu RP
ul. Wiejskiej 4/6/8
00-902 Warszawa

Szanowny Panie Przewodniczący,

w związku z pismem z dnia 23 listopada 2022 r. (znak: FPB.016.371.2022) informującym o posiedzeniu Komisji w dniu 29 listopada br. dotyczącym rozpatrzenia rządowego projektu ustawy ***o Systemie Informacji Finansowej*** (druk nr 2771), uprzejmie dziękując za przedstawienie przedmiotowego projektu wskazać należy na aktualność stanowisk organu nadzorczego, przedstawionych w toku procesu legislacyjnego[1] (w załączeniu).

Przetwarzanie danych osobowych w Systemie Informacji Finansowej (zwanym dalej: SInF), mimo że wprowadza do porządku krajowego przepisy unijne - będzie nową regulacją w krajowym porządku prawnym (a co z tym jest związane - będzie miało do niej zastosowanie rozporządzenie 2016/679[2]). W związku z powyższym, aktualność zachowuje uwaga organu nadzorczego zgłaszana na wcześniejszym etapie procesu legislacyjnego dotycząca konieczności przeprowadzenia tzw. testu prywatności, tj. oceny skutków dla ochrony danych istotnej ze względu na rodzaj przetwarzania, w szczególności następującego przy użyciu nowych technologii, ale także gdy charakter, zakres, kontekst i cele przetwarzania z dużym

[1] Uwagi z dnia 18 grudnia 2020 r., 14 lipca 2021 r., 14 września 2021 r., 20 lipca 2022 r. (znak: DOL.401.612.2020).

[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 (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.).

prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób. Analiza przepisów projektu ze względu na zakładaną przez Projektodawcę skalę i sposoby przetwarzania danych i informacji prowadzi do wniosku, że projektowane rozwiązania powodują takie ryzyko oraz uzasadnia przeprowadzenie oceny skutków planowanych tymi przepisami operacji przetwarzania dla ochrony danych osobowych. Poprawnie przeprowadzona ocena skutków powinna wskazywać związek pomiędzy operacjami wykonywanymi na danych osobowych, m.in. pozyskiwanym lub przekazywanym przez podmiot określony w ustawie zakresem danych, a konkretnym celem ich przetwarzania. Cel przetwarzania musi być określony w przepisach prawa powszechnie obowiązującego (art. 6 ust. 3 rozporządzenia 2016/679). Tymczasem, w związku z przyjmowanymi w projekcie ustawy rozwiązaniami, powinny one zawsze być poprzedzone analizą ryzyka i oceną skutków dla ochrony danych towarzyszących proponowanym rozwiązaniom, oceną ich wpływu na obowiązujące rozwiązania i kompleksowym odzwierciedleniem projektowanych zmian w obowiązującym porządku prawnym.

Procesy przetwarzania danych dla realizacji zadań określonych ww. ustawą muszą być zgodne zarówno z przepisami rozporządzenia 2016/679, jak również dyrektywy 2016/680, implementowanej ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

Projekt wprowadza rozwiązania w sposób rażąco godzący w autonomię realizacji zadań Prezesa Urzędu Ochrony Danych Osobowych, wprowadzając przepisy dotyczące nakładania określonych obowiązków związanych z realizacją zdań i współpracy (**art. 25a ust. 4, 6, 14 pkt 1, art. 42 zmiana 5 dodająca art. 25a ust. 4** w ustawie z dnia 16 września 2011 r. *o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi* (Dz. U. z 2020 r. poz. 158 oraz z 2022 r. poz. 350 i 1933) oraz **art. 44 zmiana 8 dotycząca dodawanego art. 116a** w ustawie z dnia 1 marca 2018 r. *o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Dz. U. z 2022 r. poz. 593, 655, 835, 2180 i 2185). Dotąd wskazywane stanowisko organu nadzorczego w tym zakresie nie uległo zmianie.

Odnosząc się do nowych rozwiązań, które zostały zaproponowane w aktualnie opiniowanej wersji projektu ustawy ***o Systemie Informacji Finansowej*** wskazać należy na **art. 20 pkt 3** określający nową podstawę prawną przetwarzania danych w SInF: *Organ właściwy może przetwarzać dane zgromadzone w SInF w celu wymiany informacji podatkowych, o której mowa w ustawie z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami (Dz. U. z 2021 r. poz. 626 i 2105 oraz z 2022 r. poz. 1301) oraz rozporządzeniu Rady (UE) nr*

904/2010 z dnia 7 października 2010 r. w sprawie współpracy administracyjnej oraz zwalczania oszustw w dziedzinie podatku od wartości dodanej (Dz. Urz. UE L 268 z 12.10.2010, str. 1, z późn. zm.)). Przedmiotowy przepis w sposób ogólny, wręcz blankietowy wskazuje na „wymianę informacji podatkowych" bez określenia trybu, zakresu tych informacji, zwłaszcza, że będą to także dane o charakterze osobowym. Dane osobowe mogą być udostępniane jedynie, o ile jest to niezbędne i w zakresie minimalnym dla wypełnienia celów projektowanej regulacji, przy czym cel (cele) przetwarzania danych także powinny być określone przejrzyście. Projektodawca powinien uzupełnić ww. przepis w taki sposób, aby zapewnić stosowanie przepisów rozporządzenia 2016/679 w zakresie zasad wynikających z art. 5 ust. 1, jak również zasady rozliczalności (art. 5 ust. 2)[3].

Zwrócić uwagę należy na **art. 39 pkt 3** wprowadzający zmiany *w ustawie z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym* (Dz. U. z 2022 r. poz. 660, 872, 1488, 1692 i 2185) – w dodawanym **art. 17g** Projektodawca wskazuje, że *W celu określenia zasad współpracy oraz wymiany dokumentów i informacji z Komisją Europejską, Europejskim Bankiem Centralnym, Europejskim Urzędem Nadzoru Bankowego, Europejskim Urzędem Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych, Europejskim Urzędem Nadzoru Giełd i Papierów Wartościowych, Europejską Radą ds. Ryzyka Systemowego oraz Europejskim Systemem Banków Centralnych oraz z właściwymi organami nadzoru nad rynkiem finansowym oraz z jednostkami analityki finansowej, Komisja może zawierać odpowiednie porozumienia.* Regulacje nakładające prawa i obowiązki w zakresie przetwarzania danych osobowych powinny zostać uregulowane mocą przepisów powszechnie obowiązujących ustawy, a nie w porozumieniu. Wszelkie kluczowe decyzje związane z przetwarzaniem danych osobowych dla realizacji zadań publicznych powinny być określone w przepisach prawa, a nie w aktach pozaustawowych czy

[3] „1. Dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość"); b) 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 ("ograniczenie celu"); c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych"); d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość"); e) 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 ("ograniczenie przechowywania"); f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność"). 2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność")" .

uzgodnieniach/porozumieniach. Pamiętać należy, że szczególny reżim przetwarzania[4] wymaga uwzględnienia w przepisach nakładających obowiązek przetwarzania danych i zapewnienia nie tylko rzetelności i przejrzystości, ograniczenia celu, niezbędności, minimalizacji (art. 5), ale i uwzględnienia warunków wynikających z art. 6 ust. 3, warunków odpowiednich zabezpieczeń praw podstawowych i interesów osoby, której dane dotyczą, konkretnych środków ochrony praw i wolności osób (art. 9) oraz warunków dokonywania operacji na danych z art. 10 wyłącznie pod nadzorem władz publicznych z zabezpieczeniem praw i wolności osób, których dane dotyczą (art. 10 rozporządzenia 2016/679).

Wątpliwości budzi **art. 43**, który w zmianie 2 dodaje **art. 48a ust. 1** do ustawy z dnia 16 listopada 2016 r. *o Krajowej Administracji Skarbowej* (Dz. U. z 2022 r. poz. 813, z późn. zm.): *Na sporządzone na piśmie żądanie Szefa Krajowej Administracji Skarbowej wydane w związku z wnioskiem o informacje złożonym na podstawie art. 7 ust. 3a rozporządzenia (UE) nr 883/2013, bank jest obowiązany do sporządzania i przekazywania informacji dotyczących obrotów i stanów wskazanych w żądaniu rachunków bankowych, z podaniem wpływów, obciążeń rachunków i ich tytułów oraz odpowiednio ich nadawców i odbiorców.* Wskazać należy na rozszerzenie zakresu pozyskiwanych danych przez Szefa KAS dla celów udzielenia odpowiedzi na wniosek o informacje złożony przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) na podstawie art. 7 ust. 3a rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 bez przeprowadzonej oceny skutków – analizy ryzyk dla projektowanego przetwarzania danych i wpływu udostępniania danych na prywatność osób, których dane dotyczą. Organ nadzorczy krytycznie odnosi się do zmian poszerzających zakres udostępnianych danych bez wnikliwej oceny i analizy ryzyk. Projektowany przepis, jako zbyt ogólny jest blankietowy a zatem niewystarczający dla przejrzystego i wyczerpującego określenia ww. trybu procedowania opisanych czynności bankowych.

Nowym przepisem jest również dodawany **art. 70a ust. 1** do ustawy z dnia 1 marca 2018 r. *o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Dz. U. z 2022 r. poz. 593, 655, 835, 2180 i 2185) wprowadzany **art. 44 zmianą 2** projektu ustawy: *W celu realizacji ustawowych zadań informacje, o których mowa w art. 59, udostępnia się: 1) Generalnemu Inspektorowi, 2) Komendantowi Głównemu Policji, 3) Komendantowi Centralnego Biura Śledczego Policji, 4) Komendantowi Centralnego Biura Zwalczania Cyberprzestępczości, 5) komendantom wojewódzkim Policji i Komendantowi Stołecznemu Policji, 6) Komendantowi*

[4] Realizacja tak istotnego projektu, dla którego mają być przetwarzane na masową skalę dane osobowe, w tym dane szczególnych kategorii i dane z art. 10 rozporządzenia 2016/679, w ocenie organu nadzorczego wymaga rozważenia, wybrania i zastosowania najlepszych rozwiązań organizacyjno–prawnych, zwłaszcza zastosowania szeregu instrumentów prawnych przewidzianych w rozporządzeniu 2016/679.

Głównemu Żandarmerii Wojskowej, 7) Komendantowi Głównemu Straży Granicznej, 8) Szefowi Agencji Bezpieczeństwa Wewnętrznego, 9) Szefowi Agencji Wywiadu, 10) Szefowi Krajowej Administracji Skarbowej, 11) Szefowi Służby Kontrwywiadu Wojskowego, 12) Szefowi Służby Wywiadu Wojskowego, 13)Szefowi Centralnego Biura Antykorupcyjnego, 14)Inspektorowi Nadzoru Wewnętrznego, 15)Komendantowi Biura Spraw Wewnętrznych Policji, 16) Komendantowi Biura Spraw Wewnętrznych Straży Granicznej, 17) Przewodniczącemu KNF, 18)Prezesowi NIK, 19)Prezesowi NBP, 20)sądom, 21) prokuraturze – za pomocą urządzeń teletransmisji danych.

Przepis ten wymaga uszczegółowienia, tak aby normy kompleksowo regulowały planowany mechanizm oraz prawa i obowiązki związane z przetwarzaniem danych osobowych[5]. Nie jest jasne czy realizacja projektowanych rozwiązań wiązać się będzie również z automatycznym przetwarzaniem danych osobowych w systemie, w tym profilowaniem. Na zagrożenia związane z wykorzystaniem automatycznego przetwarzania danych zwraca uwagę Grupa Robocza Art. 29 - organ, którego następcą prawnym jest funkcjonująca na podstawie przepisów rozporządzenia 2016/679 Europejska Rada Ochrony Danych - w Wytycznych w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679 przyjętych w dniu 3 października 2017 r. (ostatnio zmienionych i przyjętych w dniu 6 lutego 2018 r.). Stosowne normy powinny gwarantować właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Z motywu 31 rozporządzenia 2016/679 wynika, że ujawnianie danych podmiotom publicznym powinno mieć co do zasady charakter wnioskowy (odbywać się w formie pisemnej, być uzasadnione i mieć charakter wyjątkowy), nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

[5] Wskazać w tym miejscu należy zasadę rozliczalności wynikającą z art. 5 ust. 2 rozporządzenia 2016/679 oraz na wyrok WSA z dnia 24 stycznia 2022 r. sygn. akt II SA/Wa 2168/17, w którym Sąd wskazuje, że „(…) obowiązek wdrożenia dokumentacji ciąży na administratorze danych. Przez wdrożenie rozumieć można opracowanie, zatwierdzenie i opublikowanie w odpowiedniej formie (np. zarządzenia) oraz zaznajomienie z ich treścią osób upoważnionych do przetwarzania danych. Dokumentacja powinna być sprawdzana pod kątem zgodności ze stanem faktycznym (zabezpieczenia, ilość zbiorów, kategorie danych, itp.), zgodności ze stanem prawnym (wymogi z ustawy i rozporządzenia) oraz poprawności funkcjonowania. Zmiany w tym zakresie powinny być na bieżąco uwzględniane w dokumentacji. Weryfikacji powinien dokonywać administrator danych, na nim także spoczywa obowiązek monitorowania zabezpieczeń systemu informatycznego - w praktyce zazwyczaj czynności te wykonują administrator bezpieczeństwa informacji lub podmioty zewnętrzne (audytorzy).(…) Sąd wskazuje, iż art. 48 pkt 2 ustawy o ewidencji ludności nakłada na podmioty realizujące dostęp do rejestru PESEL za pomocą urządzeń teletransmisji danych obowiązek posiadania zabezpieczeń technicznych i organizacyjnych właściwych dla przetwarzania danych osobowych, uniemożliwiających w szczególności wykorzystanie danych niezgodnie z celem ich uzyskania. W związku z powyższym, należy wskazać, że słuszne jest stanowisko Generalnego Inspektora Ochrona Danych Osobowych, który uznał, że środkiem, który uniemożliwi (lub co najmniej utrudni) wykorzystanie danych niezgodnie z celem ich uzyskania, jest wyposażenie aplikacji „Źródło" w funkcjonalność pozwalającą na odnotowanie uzasadnienia dla dokonywanego sprawdzenia danych w rejestrze PESEL".

Wątpliwości budzi także projektowany **art. 105 ust. 1** ww. ustawy (wprowadzany **art. 44 zmianą 3** projektu ustawy), w którym wprowadzenie do wyliczenia otrzymuje brzmienie: *Generalny Inspektor udostępnia posiadane informacje, w tym informacje finansowe oraz analizy finansowe, na pisemny i uzasadniony wniosek* oraz **ust. 4:** *Generalny Inspektor udostępnia posiadane informacje, w tym informacje finansowe oraz analizy finansowe, na pisemny i uzasadniony wniosek Szefa Krajowej Administracji Skarbowej, dyrektora izby administracji skarbowej lub naczelnika urzędu celno-skarbowego w zakresie ich ustawowych zadań.* Projektowane zmiany są ogólne, nie wskazują zakresu danych osobowych oraz trybu przekazywania przedmiotowych informacji.

Podobnie, wprowadzany **art. 44 zmianą 4** projektu ustawy **art. 105b** *ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* wskazuje, że *Podmioty, o których mowa w art. 104 i art. 105 ust. 1 i 4, mogą przetwarzać dane osobowe, otrzymane w dokumentach i informacjach przekazanych przez Generalnego Inspektora, do celów związanych z zapobieganiem przestępstwom obejmującym co najmniej jeden z rodzajów działalności, o której mowa w załączniku I do rozporządzenia 2016/794, ich wykrywaniem oraz prowadzeniem postępowań w ich sprawie, innych niż cele, dla których dane zostały pierwotnie zebrane* budzi wątpliwości organu nadzorczego. Wskazać należy na problem zmiany celu przetwarzania. Propozycja przetwarzania zindywidualizowanych danych osobowych pozbawiona jest ważnego elementu, jakim jest wskazanie kategorii tych danych oraz bez wykazania niezbędności przetwarzania danych. Dodatkowo, w przypadku danych szczególnej kategorii należy dokładnie uzasadnić niezbędność wykorzystania takich właśnie danych. Ponownej analizy wymaga zatem propozycja tego przepisu pod kątem przetwarzania w tak określonych celach danych osobowych. Weryfikacji wymaga, czy w istocie dane osobowe, zindywidualizowane informacje o osobach są niezbędne do przeprowadzenia ogólnych, wskazanych celów. Z punktu widzenia dbałości o komfort wykonawców tych przepisów, tj. poszanowania zasady zgodności z prawem, rzetelności oraz przejrzystości oraz ze względu na prywatność osób, których dane dotyczą oraz poszanowania zasad przetwarzania danych osobowych, przepis ten wymaga ponownej analizy.

Wątpliwości budzi **art. 47 ust. 2 projektu ustawy:** *Przekazywanie informacji, o których mowa w art. 12 ust. 1 pkt 4, 11 i 12, ust. 2, ust. 3 pkt 1 lit. h–j, pkt 2 lit. e oraz f, zawierających dane uzyskane przed dniem wejścia w życie niniejszej ustawy, które znajdują się w formie uniemożliwiającej automatyczne przetwarzanie tych danych w systemach teleinformatycznych instytucji zobowiązanych, rozpoczyna się nie później niż ostatniego dnia 6 miesiąca od dnia upływu terminów, o których mowa w art. 46.* Projektowane rozwiązanie wiąże się

z automatycznym przetwarzaniem danych osobowych w systemie. Konstrukcja ta jest obarczona szeregiem ryzyk, na które powinien zwrócić uwagę Projektodawca, a które były już wskazywane na wcześniejszych etapach procesu legislacyjnego.

Uwzględnienie powyższych kwestii wskazanych jako eksperckie wsparcie z zakresu przetwarzania danych osobowych niewątpliwie przyczyni się do właściwego wdrożenia zasad ochrony danych wynikających z przepisów rozporządzenia 2016/679 w procedowanym akcie normatywnym.

Z wyrazami szacunku,

Prezes Urzędu
Ochrony Danych Osobowych
Jan Nowak

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/

Załączniki:

- pisma z dnia 18 grudnia 2020 r., 14 lipca 2021 r., 14 września 2021 r., 20 lipca 2022 r. (znak: DOL.401.612.2020).