Warszawa, 20 lipca 2022 r.

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Jan Nowak

DOL.401.612.2020.WL.MW.

Pan
Rafał Gumowski
Dyrektor
Departamentu Prawa Gospodarczego
w Rządowym Centrum Legislacji
ul. Krucza 36 / Wspólna 6
00-522 Warszawa

Szanowny Panie Dyrektorze,

w związku z pismem z dnia 18 lipca 2022 r. (znak sprawy: RCL.DPG.550.80/2020), będącym zaproszeniem na komisję prawniczą dotyczącą projektu ustawy ***o Systemie Informacji Finansowej (***UC66), która zostanie przeprowadzona w formie telekonferencji (w systemie zoom) i rozpocznie się w dniu 21 lipca 2022 r. o godz. 10.00, uprzejmie informuję, że udział w niej weźmie - jako przedstawiciel Urzędu Ochrony Danych Osobowych - Pani Monika Witak-Gryciuk – Główny Specjalista w Wydziale Legislacji Departamentu Orzecznictwa i Legislacji. Organ nadzorczy dziękując za zaproszenie, jednocześnie wskazuje, że pomimo prawnego obowiązku konsultacji projektu ustawy, nie był on przez resort finansów przekazany do zaopiniowania na wcześniejszym etapie. Jest to o tyle istotne, gdyż niniejszy projekt wprowadza rozwiązania w sposób rażąco godzący w autonomię realizacji zadań Prezesa Urzędu Ochrony Danych Osobowych, wprowadzając przepisy niekonsultowane z organem, pomimo że dotyczą także nakładania określonych obowiązków związanych z realizacją zdań i współpracy z organem nadzorczym.

Projekt ustawy ***o Systemie informacji Finansowej*** z dnia 13 lipca 2022 r. budzi szereg wątpliwości organu nadzorczego, gdyż znacząco różni się od wersji projektu ww. ustawy procedowanej na wcześniejszych etapach prac legislacyjnych (dodano wiele nowych przepisów, także z zakresu ochrony danych osobowych). W związku z powyższym Prezes UODO podtrzymuje dotychczas wniesione uwagi do projektu z dnia 27 listopada 2020 r.[1], które nie zostały przez projektodawcę uwzględnione w obecnej wersji projektu ustawy *o Systemie Informacji Finansowej* (SInF). Jednocześnie organ nadzorczy zwraca uwagę na zagadnienia, które zawiera nowa wersja projektu ustawy, i które są niezgodne z zasadami ochrony danych osobowych wynikającymi z przepisów rozporządzenia 2016/679[2]. Należy podkreślić, że procesy przetwarzania danych dla realizacji ww. zadań muszą być także zgodne zarówno z przepisami rozporządzenia 2016/679, jak również *dyrektywy 2016/680*[3], implementowanej *ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości* (Dz. U. z 2019 r. poz. 125).

Ponownego podkreślenia wymaga, że przetwarzanie danych osobowych w ramach SiNF – mimo, że wprowadza do porządku krajowego przepisy unijne - będzie nową regulacją w krajowym porządku prawnym (a co za tym idzie będzie miało do niej zastosowanie rozporządzenie 2016/679). W związku z powyższym, aktualność zachowuje uwaga organu nadzorczego zgłaszana wcześniej dotycząca konieczności przeprowadzenia oceny skutków dla ochrony danych ze względu na rodzaj przetwarzania, w szczególności następującego przy użyciu nowych technologii, ale także gdy charakter, zakres, kontekst i cele przetwarzania z dużym 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 bowiem do wniosku, że projektowane rozwiązania powodują takie ryzyko oraz uzasadnia przeprowadzenie oceny skutków planowanych tymi przepisami operacji przetwarzania dla ochrony danych osobowych. Wprowadzeniu do porządku krajowego postanowień dyrektywy powinna towarzyszyć także analiza zgodności z normami

[1] Uwagi z dnia 18 grudnia 2020 r., 14 lipca 2021 r., 14 września 2021 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.).

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 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. Akt ten reguluje sferę wyłączoną spod stosowania ogólnego rozporządzenia o ochronie danych (RODO), tj. w zakresie 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.

rozporządzenia 2016/679. Przeprowadzenie takiej analizy powinno prowadzić do wykazania niezbędności przetwarzania określonych kategorii danych osobowych we wskazanym konkretnie celu i zakresie oraz oceny ryzyka projektowanych (przyjmowanych) rozwiązań w zakresie przetwarzania danych osobowych.

Odnosząc się do poszczególnych przepisów projektu ustawy z dnia 13 lipca 2022 r. zwrócić kierunkowo uwagę na następujące kwestie.

Art. 12 ust. 2 lit. j projektu ustawy wskazuje na dane identyfikacyjne osoby fizycznej w postaci numeru telefonu i adresu poczty elektronicznej - dane w postaci numeru telefonu oraz adresu poczty elektronicznej. Zauważyć należy, że w polskim porządku prawnym nie ma obowiązku posiadania numeru telefonu oraz adresu e-mail. Dlatego zasadnym jest doprecyzowanie w projektowanych przepisach, że zamieszczanie numeru telefonu i adres poczty elektronicznej powinno odbywać się w sposób fakultatywny oraz wyłącznie wtedy, gdy osoba przedmiotowe dane posiada. Pamiętać należy, że zgodnie z zasadą minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c rozporządzenia 2016/679 dane osobowe muszą być stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Wątpliwości budzi **art. 19 ust. 3** projektu ustawy – jest to nowy przepis, który dotyczy udostępnienia informacji o rachunku kolejnym (nowym) podmiotom *w zakresie niezbędnym* do wykonywanych przez nich zadań. Określając szeroki katalog podmiotów, którym planowane jest udostępnianie informacji projektodawca nie wyjaśnił tego rozwiązania w uzasadnieniu do projektu ustawy. Dane osobowe mogą być udostępniane jedynie, o ile jest to niezbędne i w zakresie minimalnym dla wypełnienia celów projektowanej regulacji. Z uwagi na dostęp wielu podmiotów do informacji/danych znajdujących się w systemie teleinformatycznym, regulowanym w niniejszym projekcie ustawy, wskazać trzeba na konieczność dostosowania projektowanych rozwiązań do zakresu podmiotowego i przedmiotowego regulacji wynikającego z przepisów Dyrektywy 2016/680 oraz wdrażającej ją ustawy z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, bowiem dostęp do systemu teleinformatycznego mogą mieć tylko podmioty/organy wskazane w ww. aktach prawnych oraz dla realizacji celów nimi przewidzianych. Przepis w projektowanym kształcie jest blankietowy - wskazana kwestia powinna podlegać szczególnej analizie projektodawcy celem przyjęcia przepisów godzących zakładane cele projektu ustawy oraz obowiązujące przepisy regulujące ramy przetwarzania danych osobowych.

Kolejne zastrzeżenia budzi projektowany **art. 21**, który dotyczy upoważnienia podmiotu uprawnionego do dostępu do SInF. W **ust. 3** ww. przepisu projektodawca wprowadza upoważnienie do udzielania dalszych upoważnień do dostępu do SInF. Administratorem danych

zgromadzonych w SInF, zgodnie z projektowanym art. 6 ustawy jest Szef Krajowej Administracji Skarbowej. Zgodnie z art. 29 rozporządzenia 2016/679 upoważnienia są wydawane wyłącznie na polecenie administratora - nawet jeśli mają być przetwarzający i dalsi przetwarzający to administrator musi wyrazić zgodę, a w sposób skonstruowany w projektowanym **art. 21 ust. 3** w istocie naruszona została zasada rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679) po stronie administratora danych przetwarzanych w tym systemie.

Ponadto **art. 21 ust. 5** wskazuje, że *Do dostępu do SInF upoważniona może zostać wyłącznie osoba o nieskazitelnym charakterze, przestrzegającą zasad etyki zawodowej, która posiada niezbędną wiedzę w zakresie przepisów mających zastosowanie do SInF, w szczególności dotyczących ochrony danych, w tym danych osobowych, kwalifikacje zapewniające zachowanie bezpieczeństwa systemów teleinformatycznych oraz daje rękojmię ochrony informacji o rachunku zgromadzonych w SInF.* Wyjaśnienia oraz doprecyzowania wymaga kto i na jakich zasadach będzie weryfikował i dokonywał oceny wyżej wymienionych kwalifikacji/kompetencji. Projektodawca nie wskazuje jak będą badane te kryteria, jakie dane osobowe, z jakich źródeł będą pozyskiwane celem zbadana nieskazitelnego charakteru, przestrzegania etyki, w jaki sposób będzie badana niezbędna wiedza z zakresu ochrony danych, a także jak będzie dokumentowane spełnienie tych kryteriów. Projektowany przepis nie zawiera informacji czy będą w związku z tym i przez jaki okres i w jakiej formie utrwalane dane osobowe, w tym dane z art. 10 rozporządzenia 2016/679 (dotyczące wyroków skazujących i naruszeń prawa).

Wątpliwości budzi **art. 25** projektu dotyczący *rejestru działań osób, o których mowa w art. 21 ust. 1* – czy jest to nowy rejestr czy stanowi on cześć SInF. Nie wskazano czy rejestr ten jest prowadzony w systemie teleinformatycznym oraz nie określono ról podmiotów w tym rejestrze. Precyzyjne określenie ról poszczególnych podmiotów, odpowiadających procesom przetwarzania danych osobowych - rzeczywistym celom i potrzebom związanym z przetwarzaniem danych osobowych, jest niezbędne dla zapewnienia rozwiązań zgodnych z przepisami o ochronie danych osobowych. Zastrzeżenia budzi ust. 4 ww. przepisu który wskazuje na kontrolę Prezesa UODO w zakresie prawidłowości prowadzenia rejestru. W tym miejscu wskazać należy, że uprawnienia i obowiązki organu nadzorczego wynikają bezpośrednio z rozporządzenia 2016/679 i są realizowane niezależnie od tego jakie rozwiązania będą kształtowane w niniejszych przepisach. Uprawnienia kontrolne są jednym z obowiązków Prezesa UODO, który realizować także będzie także inne, m.in. rozpatrywać w postępowaniach administracyjnych skargi na związane z przetwarzaniem danych w przedmiotowym systemie.

W uzasadnieniu do projektu ustawy projektodawca wyjaśnia, że przepis ten *„(...) stanowi implementację art. 6 ust. 2 dyrektywy 2019/1153. W przypadku stwierdzenia nieprawidłowości w zakresie prowadzenia rejestru o którym mowa w ust. 1, Prezes Urzędu Ochrony Danych Osobowych informuje o tym fakcie organ właściwy. Organ właściwy w sprawach SInF w ramach sprawowanej przez siebie kontroli nad rejestrem logowań wykonywanej przy pomocy wyznaczonego inspektora ochrony danych osobowych, będzie miał możliwość zapewnienia, iż w rejestrze gromadzone są wszystkie wymagane przez ustawę, a co za tym idzie również przez dyrektywę 2019/1153 informacje. Prezes Urzędu Ochrony Danych Osobowych będzie uprawniony do przeprowadzania kontroli prawidłowości przetwarzania danych osobowych w SInF, w tym w zakresie rejestru logowań. W ustawie o SInF nie przewidziano specjalnej procedury kontrolnej, tym samym Prezes Urzędu Ochrony Danych Osobowych będzie sprawował kontrolę na podstawie przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781)*". Wyżej wskazane uzasadnienie stanowi błędną interpretację art. 6 ust. 2 ww. dyrektywy, który brzmi: *Inspektorzy ochrony danych dotyczących scentralizowanych rejestrów rachunków bankowych regularnie sprawdzają logi. Logi są również udostępniane właściwym organom nadzorczym ustanowionym zgodnie z art. 41 dyrektywy (UE) 2016/680, na żądanie.* Zdanie drugie stanowi jedynie o udostępnianiu organowi nadzorczemu na jego żądanie przedmiotowych logów. Taka interpretacja i tak brzmiący projektowany przepis rażąco godzi w niezależność i autonomię organu nadzorczego (art. 52 rozporządzenia 2016/679). Ww. przepis dyrektywy stanowi o uprawnieniach administratorów i wspierających ich inspektorów ochrony danych, natomiast nie wskazuje na uprawnienia kontrolne organu nadzorczego. Podobne zastrzeżenia budzi **art. 25 ust. 6** projektu ustawy: *Podmiot uprawniony, o którym mowa w art. 19 ust. 2 pkt 3 i 9–15, na żądanie Prezesa Urzędu Ochrony Danych Osobowych lub inspektora ochrony danych organu właściwego udostępnia do wglądu informacje z rejestru, o którym mowa w ust. 1, w terminie wskazanym w żądaniu, nie krótszym niż 7 dni.* W sposób określony w ww. przepisie uprawnienia kontrolne organu nadzorczego zostały ograniczone, ponieważ zgodnie z art. 58 ust. 1 rozporządzenia 2016/679 organ nadzorczy możemy nie tylko do żądać wglądu dostępu do informacji, ale i żądać innych dowodów (m.in. uzyskać od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych do realizacji swoich zadań oraz dostępu do wszystkich pomieszczeń, w tym sprzętu czy środków służących do przetwarzania danych). Taki przepis zatem w sposób nieuprawniony wyłącza rozporządzenie 2016/679 w obszarze realizacji innych kompetencji. Jednocześnie podkreślenia wymaga, że przepisy te nie były przez

projektodawcę przedkładane organowi nadzorczemu do zaopiniowania – dopiero projekt ustawy z dnia 13 lipca br. zawiera te regulacje.

Art. 27 projektu ustawy zawiera sformułowanie „co najmniej", które wskazuje na otwarty katalog stosowanych zabezpieczeń. Należy szczegółowo określić w przepisach prawa przedmiotowy katalog, nie używając ww. zwrotu, lecz zamkniętego katalogu informacji, tak, aby wyeliminować wątpliwości w przedmiotowym zakresie.

Niezrozumiały jest **art. 30 ust. 2** projektu ustawy, który wskazuje: *Na uzasadniony wniosek podmiotów wskazanych w ust. 1, organ właściwy przekazuje informacje o rachunkach z SInF oraz informacje dotyczące wypełniania przez instytucje zobowiązane obowiązku przekazywania informacji o rachunku, w zakresie w jakim informacje te są niezbędne do sprawowania kontroli, o której mowa w ust. 1,* nie precyzując trybu, czy wniosek ma być w formie pisemnej. W celu wyeliminowania wątpliwości należy przepis ten dookreślić uwzględniając powyższe kwestie.

Zwrócić uwagę należy na projektowany **art. 41,** który wprowadza zmiany 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). Art. 41 pkt 2 stanowi, że po art. 2 dodaje się art. 2a, który w ust. 2 wskazuje: *W ramach wymiany informacji, o której mowa w ust. 1, podmioty, o których mowa w art. 1 ust. 2, mogą przekazywać wyznaczonym właściwym organom informacje finansowe, o których mowa w art. 2 ust. 2 pkt 10a ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, oraz analizy finansowe, o których mowa w art. 2 ust. 2 pkt 1a tej ustawy, a także występować do wyznaczonych właściwych organów o przekazanie informacji pochodzących od jednostki analityki finansowej z państwa pochodzenia tego organu-* wątpliwości budzi brak określonego zakresu informacji oraz czy informacje te zawierają dane o charakterze osobowym.

Wątpliwości budzi **art. 41 pkt 5** projektu ustawy, który po art. 25 dodaje art. 25a, dotyczący rejestru realizowanych wniosków o informacje. Przepis ten określa, jakie wnioski muszą być rejestrowane (ust. 1), zakres rejestrowanych danych (ust. 2), okres przechowywania danych (ust. 3) oraz wskazuje na możliwość udostępniania rejestrowanych danych do wglądu Prezesowi Urzędu Ochrony Danych Osobowych (ust. 4). Projektodawca nie wskazał czy ww. rejestr będzie odrębnym rejestrem czy będzie stanowił element już istniejącego rejestru. Nie jest określone czy i jakie dane osobowe będą przetwarzane (chociażby w postaci metadanych) w ww. rejestrze oraz cel ich przetwarzania. Istotną kwestią jest zagadnienie związane z zabezpieczeniem dokumentacji, wdrożeniem odpowiednich środków technicznych i

organizacyjnych. Projektodawca powinien uzupełnić ww. przepis w taki sposób, aby zachować zgodność z przepisami rozporządzenia 2016/679 w zakresie zasad wynikających z art. 5 ust. 1. Ponadto dodawany tym przepisem **art. 25c** zawiera poprzez użycie zwrotu **„w szczególności"** otwarty katalog informacji o „wnioskach o informacje". Konieczne jest doprecyzowanie przedmiotowego katalogu, nie używając ww. zwrotu, lecz zamkniętego katalogu informacji.

Wskazać należy na **art. 43** projektu ustawy wprowadzający zmiany w *ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Dz. U. z 2022 r. poz. 593, 655 i 835). Wątpliwości budzi pkt 2 ww. przepisu, który wprowadza zmiany w art. 105 ustawy, uprawniając *Generalnego Inspektora do udostępniania posiadanych informacji w tym informacji finansowych oraz analiz finansowych, na pisemny i uzasadniony wniosek Szefa Krajowej Administracji Skarbowej, dyrektora izby administracji skarbowej lub naczelnika urzędu celno-skarbowego w zakresie ich ustawowych zadań*. Wskazać należy na brak określonego zakresu informacji oraz czy informacje te zawierają dane o charakterze osobowym (jeśli tak, konieczne jest uwzględnienie zasad wynikających z przepisów o ochronie danych osobowych). Zastrzeżenia budzi także pkt 3 ww. przepisu, który po art. 105 ustawy dodaje **art. 105b**: *Podmioty, o których mowa w art. 104 oraz 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 794/2016, ich wykrywaniem oraz prowadzeniem postępowań w ich sprawie, innych niż cele, dla których dane zostały pierwotnie zebrane.* W opinii organu nadzorczego rozwiązanie to powinno zostać szczegółowo uzasadnione. Wskazać bowiem należy, że jedną z naczelnych zasad jest zasada ograniczenia celu, według której dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (art. 5 ust. 1 lit. b rozporządzenia 2016/679). Projektodawca mając na względzie art. 6 ust. 3 rozporządzenia 2016/679 powinien wyraźnie wskazać w przepisach projektowanej ustawy podstawę prawną i cel przetwarzanych danych.

Wątpliwości budzi także pkt 7 ww. przepisu, który po art. 116a dodaje **art. 116b**, który wskazuje na rejestr wniosków - Projektodawca nie wskazał czy ww. rejestr będzie odrębnym rejestrem i nie określił formy jego prowadzenia (elektronicznie/papierowo). Istotną kwestią jest zagadnienie związane z zabezpieczeniem dokumentacji, wdrożeniem odpowiednich środków technicznych i organizacyjnych. Projektodawca powinien uzupełnić ww. przepis w taki sposób, aby zachować zgodność z przepisami rozporządzenia 2016/679 w zakresie zasad wynikających z art. 5 ust. 1.

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

Z poważaniem,

Z up. Prezesa Urzędu
Ochrony Danych Osobowych
Dyrektor Departamentu
Orzecznictwa i Legislacji

Monika Krasińska

/- dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym/