Warszawa, 18 grudnia 2020 r.

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Jan Nowak
DOL.401.612.2020.WL.MW.

Pani
Anna Chałupa
Podsekretarz Stanu
Ministerstwo Finansów,
Funduszy i Polityki Regionalnej
ul. Świętokrzyska 12
00-916 Warszawa
Elektroniczna Skrzynka Podawcza:
/bx1qpt265q/SkrytkaESP

Szanowna Pani Minister,

w odpowiedzi na pismo z dnia 3 grudnia 2020 r., udostępnione 4 grudnia br., uprzejmie informuję, że do **projektu *ustawy o Systemie Informacji Finansowej*** (dalej projekt ustawy) - Prezes Urzędu Ochrony Danych Osobowych z punktu widzenia przepisów *rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 04.05.2016, str. 1, z późn. zm.)*[1], zwanego dalej rozporządzeniem 2016/679 **- zgłasza następujące uwagi.**

[1] Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018 r., s. 2.

I. Ocena skutków dla ochrony danych osobowych.

Prezes Urzędu Ochrony Danych Osobowych poddaje pod rozwagę Projektodawcy art. 35 ust. 1 rozporządzenia 2016/679, który reguluje obowiązek dokonania – przed rozpoczęciem przetwarzania albo w związku z tworzeniem przepisów regulujących operację lub zestaw operacji przetwarzania – *oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych*. Taka ocena skutków ochrony danych powinna być dokonywana ze względu na rodzaj przetwarzania, w szczególności następujący 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. Przeprowadzenie takiej analizy powinno prowadzić do wykazania niezbędność przetwarzania określonych kategorii danych osobowych we wskazanym konkretnie celu i zakresie oraz oceny ryzyka projektowanych (przyjmowanych) rozwiązań w zakresie przetwarzania danych osobowych. Analiza przepisów projektu ze względu na zakładaną przez Projektodawcę skalę, zakres i sposoby przetwarzania danych osobowych zdaje się powodować ryzyko dla ochrony prywatności osób, których dane dotyczą oraz uzasadnia przeprowadzenie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Zgodnie z art. 35 ust. 7 rozporządzenia 2016/679 ocena skutków zawiera co najmniej: systematyczny opis planowanych operacji przetwarzania i celów przetwarzania; ocenę, czy operacje są niezbędne oraz proporcjonalne w stosunku do celów; ocenę ryzyka naruszenia praw lub wolności podmiotów danych; środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa, które mają zapewnić ochronę danych osobowych. Wsparciem dla Projektodawcy jest Inspektor Ochrony Danych (art. 37-39 rozporządzenia 2016/679) - osoba, która ze względu na posiadaną wiedzę z zakresu ochrony danych osobowych powinna wspomóc Projektodawcę w przeprowadzeniu stosownej analizy i oceny. *Uzasadnionym jest dokonanie oceny skutków dla ochrony danych – zgodnie z art. 35 ust. 10 rozporządzenia 2016/679 - już w ramach oceny skutków regulacji w związku z przyjmowaniem określonej podstawy prawnej przetwarzania danych, co przy dokonaniu prawidłowej oceny i wypracowaniu przepisów szczególnych uwzględniających stosowanie ogólnego rozporządzenia o ochronie danych może zastąpić dokonywanie takiej oceny przez podmioty stosujące / wykonujące następnie tak ustalone przepisy.* Poprawnie przeprowadzona ocena skutków powinna wskazywać związek pomiędzy pozyskiwanym lub przekazywanym przez podmiot określony w ustawie zakresem danych, z konkretnym celem ich przetwarzania, który to cel również powinien zostać wskazany w przepisach prawa powszechnie obowiązującego.

Z dokumentów przedstawionych do zaopiniowania nie wynika, by Projektodawca wykonał tego rodzaju analizę i ocenę, a w konsekwencji wyważył wpływ planowanego przetwarzania danych osobowych na prywatność osób, których te dane dotyczą i proponował rozwiązania odpowiadające poszanowaniu zasad przetwarzania danych osobowych. Tymczasem, wobec doniosłości i konsekwencji dla projektowanego przetwarzania danych osobowych w związku z przyjmowanymi w projekcie ustawy rozwiązaniami uznać to należy za wysoce pożądane.

II. **System teleinformatyczny.**

Wątpliwości Prezesa UODO budzą proponowane w niniejszym projekcie uregulowania dotyczące przekazywania informacji o rachunku SInF za pośrednictwem STIR **(art. 13 i następne projektu ustawy),** taki ich kształt należy uznać za niewystarczający**.** System teleinformatyczny regulowany mocą przedmiotowego projektu (SInF) jest częścią istniejącego już systemu informatycznego (STIR). Kwestie związane z funkcjonowaniem SInF oraz nakładaniem praw i obowiązków powinny być – w ocenie organu nadzorczego – uregulowane kompleksowo przez Projektodawcę w ustawie o Systemie Informacji Finansowej, a nie poprzez odwołanie do odpowiednich przepisów Ordynacji podatkowej, odnoszących się do STIR. Wątpliwości organu nadzorczego budzi brak regulacji w ww. zakresie oraz to, czy z użyciem STIR będzie dokonywana analiza przekazywanych za jego pośrednictwem informacji/danych także dla innych celów niż wynikające z projektu ustawy. Konieczne jest zatem precyzyjne określenie w projekcie ról i obowiązków – w odniesieniu do także precyzyjnie określonych celów przetwarzania, operacji (zestawów operacji) przetwarzania - podmiotów czerpiących dane osobowe z systemu teleinformatycznego oraz zasilających system danymi osobowymi. Przyjmowane rozwiązania dotyczące procesów przetwarzania danych powinny zostać przeanalizowane także pod względem ewentualnego przyjęcia przepisów regulujących współadministrowanie, tj. wspólne ustalanie celów i sposobów przetwarzania.

Z projektowanego **art. 18 projektu ustawy** nie wynika w jaki sposób przekazywane są Generalnemu Inspektorowi Informacji Finansowej informacje o rachunku zgromadzone w SInF - **art. 20 projektu ustawy** odnosi się bowiem tylko do udostępniania podmiotom uprawnionym wskazanym w **art. 19 projektu ustawy**. Kwestia ta wymaga uzupełnienia.

Pod rozwagę poddać należy **art. 19 projektu ustawy** – określający szeroki katalog podmiotów, którym planowane jest udostępnianie informacji. 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*[2] oraz wdrażającej ją *ustawy z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125),* bowiem dostęp do systemu teleinformatycznego mogą mieć tylko podmioty/organy wskazane w ww. aktach prawnych oraz dla realizacji celów nimi przewidzianych. Wskazana kwestia powinna podlegać szczególnej analizie Projektodawcy celem przyjęcia przepisów godzących zakładane cele projektu ustawy oraz obowiązujące przepisy regulujące ramy przetwarzania danych osobowych.

Wątpliwości budzi także **art. 20 projektu ustawy** dotyczący udostępniania informacji o rachunku podmiotom uprawnionym. Samo określenie „przy użyciu systemu teleinformatycznego" bez opisania przez Projektodawcę trybu, zasad i sposobu dostępu do tego systemu w ocenie organu nadzorczego jest niewystarczające i nie może być zaakceptowane.

Nie jest także precyzyjnie sformułowany **art. 23 projektu ustawy**, stanowiący o rejestrze osób upoważnionych do dostępu do SInF – z przepisu tego nie wynika bowiem czy rejestr ten jest odrębnym rejestrem publicznym czy funkcjonować ma on w ramach systemu SInF (ewentualnie w STIR). Poddać należy pod rozwagę Projektodawcy czy przekazywanie tak istotnych informacji jak unikalny identyfikator dostępu środkami komunikacji elektronicznej uznać należy za gwarantujący wystarczające ich bezpieczeństwo **(art. 23 ust. 2 projektu ustawy).** Organ nadzorczy zwraca również uwagę na okres przechowywania danych z rejestru wskazany w **art. 23 ust. 4 projektu –** jaki cel uzasadnia niezbędność przechowywania tych danych przez 5 lat.

Art. 24 projektu ustawy nie wskazuje natomiast kto/jaki podmiot udostępnia informacje o rachunku, na jakich zasadach weryfikowane są okoliczności przewidziane tym przepisem oraz jakie warunki uzasadniają odmowę udostepnienia, co wymaga uzupełnienia.

Art. 26 ust. 2 projektu ustawy stanowi o uprawnieniach kontrolnych wskazanych w tym przepisie organów, natomiast Projektodawca nie reguluje w tym przepisie w jaki sposób, na jakich zasadach kontrole miałyby być przeprowadzane. Te rozwiązania także należy uzupełnić.

Prezes UODO wskazuje pod rozwagę Projektodawcy na **art. 28 projektu ustawy** – czy poddano analizie, że przyjmowane rozwiązania regulowane w projekcie wyczerpują potrzeby

[2] 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.

bezpieczeństwa przetwarzania danych osobowych w systemie teleinformatycznym, o których stanowi art. 24 i 32 rozporządzenia 2016/679, czy rozwiązania te były weryfikowane na poziomie IOD wspomagającego Projektodawcę.

Projektowane jest również, w **art. 9 projektu ustawy**, że minister właściwy do spraw finansów publicznych może wyznaczyć w drodze rozporządzenia dyrektora izby administracji skarbowej do wykonywania zadań organu właściwego - w ocenie Prezesa UODO powinno być to uregulowane mocą przepisów przedmiotowej ustawy, skoro wyznaczane mają być zadania organu działającego w celu wykonania zadań organu właściwego.

III. Ochrona danych osobowych.

W **art. 30 projektowanej ustawy** Projektodawca przewiduje, że do przetwarzania danych osobowych zgromadzonych w SInF ma zastosowanie art. 6 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019r. poz.1789). Zgodnie z tym przepisem u.o.d.o., *ustawy oraz rozporządzenia 2016/679 nie stosuje się do: 1) przetwarzania danych osobowych przez jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 3, 5, 6 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019 r. poz. 869 i 1622), w zakresie, w jakim przetwarzanie to jest konieczne do realizacji zadań mających na celu zapewnienie bezpieczeństwa narodowego, jeżeli przepisy szczególne przewidują niezbędne środki ochrony praw i wolności osoby, której dane dotyczą; 2) działalności służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2018 r. poz. 2387, 2245 i 2399 oraz z 2019 r. poz. 53, 125 i 1091).* **Propozycja przyjęcia tak poważnego w skutkach rozwiązania – nawet w tak istotnych celach jak przewidywane art. 2 projektu ustawy - wymaga szczególnego odniesienia się przez organ nadzorczy.**

Wskazać zatem trzeba, że pojęcie „bezpieczeństwa narodowego" zostało wskazane w art. 4 ust. 2 Traktatu o Unii Europejskiej (Dz. U. z 2004 r. poz. 864/30, z późn. zm.)[3], natomiast w prawie krajowym brak jest definicji legalnej pojęcia „bezpieczeństwa narodowego". W literaturze

[3] Art. 4 ust. 2 TUE stanowi: „Unia szanuje równość Państw Członkowskich wobec Traktatów, jak również ich tożsamość narodową, nierozerwalnie związaną z ich podstawowymi strukturami politycznymi i konstytucyjnymi, w tym w odniesieniu do samorządu regionalnego i lokalnego. Szanuje podstawowe funkcje państwa, zwłaszcza funkcje mające na celu zapewnienie jego integralności terytorialnej, utrzymanie porządku publicznego oraz ochronę bezpieczeństwa narodowego. W szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego Państwa Członkowskiego". Konstytucja Rzeczypospolitej Polskiej nie posługuje się tym terminem, lecz pojęciem „bezpieczeństwa państwa", podczas gdy akty prawne Unii Europejskiej posługują się oboma ww. pojęciami.

eksperckiej i naukowej[4] podkreśla się że „bezpieczeństwo narodowe" jest pojęciem o najszerszym zakresie przedmiotowym, które obejmuje również inne rodzaje bezpieczeństwa, jak: bezpieczeństwo obywateli, bezpieczeństwo wewnętrzne oraz bezpieczeństwo zewnętrzne. Decyzja o tym, czy dane działanie uznane powinno być za objęte „bezpieczeństwem narodowym" powinna zostać przez Projektodawcę podjęta po wnikliwej ocenie każdego stanu faktycznego, przy czym nie powinno się stosować w tym przypadku wykładni zawężającej ochronę prawa podstawowego, jakim jest ochrona danych osobowych. Projektodawca powinien wykazać także cel takiego rozwiązania.

Organ nadzorczy wskazuje, że prawo do ochrony danych osobowych jest jednym z podstawowych praw każdego człowieka[5]. Sam fakt przetwarzania danych przez jednostkę z sektora finansów publicznych (czy Kolegium do Spraw Służb Specjalnych, o którym mowa w art. 11 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[6], do którego odnosi art. 6 pkt 2 ustawy o ochronie danych osobowych – w celach ochrony bezpieczeństwa państwa) **nie może powodować – niewynikającego z przepisów rozporządzenia 2016/679 wyłączenia w całości stosowania przepisów ogólnego rozporządzenia o ochronie danych oraz przepisów ustawy o ochronie danych osobowych**. Każde wyłączenie aby mogło być uznane za mające rację bytu musi bowiem wynikać z obowiązujących przepisów prawa, a jednocześnie – dla równowagi ograniczania pewnych elementów praw podstawowych - muszą być zapewnione odpowiednie instrumenty prawne dla poszanowania praw jednostki.

Wobec **proponowanej treści art. 30 projektowanej ustawy** należy zatem odnieść się do przewidzianych art. 23 rozporządzenia 2016/679 ograniczeń i w pierwszej kolejności wskazać, że nie mogą być one rozumiane jako wyłączenia spod regulacji rozporządzenia 2016/679 (wyłączenia przewidziane są bowiem jedynie w treści art. 13, 14 i 17 rozporządzenia 2016/679). Następnie wskazać należy, że ewentualne ograniczenia stosowania rozporządzenia 2016/679 mogą następować w dość szerokim, ale nie pełnym zakresie oraz tylko o ile spełnione zostaną warunki z art. 23, w szczególności dla zapewnienia poważnych celów, o których stanowi art. 23 ust. 1. *Zgodnie bowiem z art. 23 ust. 1 (prawo Unii lub) prawo państwa członkowskiego,*

[4] M. Brzeziński, Rodzaje bezpieczeństwa państwa, w: Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia, S. Sulowski, M. Brzeziński (red. nauk.), Warszawa 2009, Dom Wydawniczy Elipsa

[5] w Konstytucji RP ustawodawca zapewnia każdej osobie prawo do ochrony danych osobowych jej dotyczących - art. 51 ust. 1, takie samo prawo zapewnia także art. 16 Traktatu o funkcjonowaniu Unii Europejskiej.

[6] Art. 11. [Status Kolegium do Spraw Służb Specjalnych]
Przy Radzie Ministrów działa Kolegium do Spraw Służb Specjalnych, zwane dalej "Kolegium", jako organ opiniodawczo-doradczy w sprawach programowania, nadzorowania i koordynowania działalności ABW, AW, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego, zwanych dalej "służbami specjalnymi", oraz podejmowanych dla ochrony bezpieczeństwa państwa działań Policji, Straży Granicznej, Straży Marszałkowskiej, Żandarmerii Wojskowej, Służby Więziennej, Służby Ochrony Państwa, Krajowej Administracji Skarbowej, organów informacji finansowej oraz służb rozpoznania Sił Zbrojnych Rzeczypospolitej Polskiej.

któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12-22 i w art. 34, a także w art. 5 - o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12-22 - jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym np. bezpieczeństwu narodowemu.

Całkowite wyłączenie praw osób, których dane dotyczą nie jest zatem możliwe, choć jest możliwe ich ograniczenie, ale jedynie po spełnieniu następujących przesłanek: 1) odpowiednio skonstruowane przepisy aktu prawnego – a nie jedynie przepis wskazujący pełne wyłączenie stosowania całych aktów prawnych – może ograniczać ściśle określony wskazanymi przepisami rozporządzenia 2016/679 zakres praw i obowiązków, tj. tych, które przewidziane są w art. 12-22 i w art. 34 oraz art. 5 rozporządzenia 2016/679; 2) akt prawny ograniczający w ww. zakresie prawa i obowiązki musi zawierać przepisy odpowiadające prawom i obowiązkom przewidzianym w art. 12-22 rozporządzenia 2016/679; 3) wprowadzane w ww. sposób ograniczenie nie może naruszać istoty podstawowych praw i wolności (a za takie uznać należałoby aktualne brzmienie art. 30 projektu ustawy); 4) wprowadzane w ww. sposób ograniczenie musi być w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, 5) ograniczenie służyć może jednemu z celów przewidzianych w art. 23 ust. 2 lit a) – j) rozporządzenia 2016/679. Dodatkowo, niezbędne jest – dla wprowadzania zgodnego z przepisami rozporządzenia 2016/679 ograniczenia praw – aby akt prawny, o którym mowa w ust. 1, zawierał szczegółowe przepisy przynajmniej - w stosownym przypadku - o: a) celach przetwarzania lub kategorii przetwarzania; b) kategoriach danych osobowych; c) zakresie wprowadzonych ograniczeń; d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu; e) określeniu administratora lub kategorii administratorów; f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania; g) ryzykach naruszenia praw lub wolności osoby, której dane dotyczą; oraz h) prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

Bez wątpienia zatem proponowany art. 30 projektu ustawy, powinien być na nowo przeanalizowany pod kątem art. 23 rozporządzenia 2016/679, którego stosowanie w przypadku przetwarzania danych osobowych należy zapewnić wprowadzając do porządku krajowego zaproponowane rozwiązania ustawy o Systemie Informacji Finansowej.

Z tych względów niniejszy projekt ustawy o systemie Informacji Finansowej podlegać powinien ponownej analizie celem zapewnienia stosowania w projektowanych przepisach norm wynikających z rozporządzenia 2016/679 ale i *Dyrektywy 2016/680*[7] oraz *ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.*

Z poważaniem,

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

Monika Krasińska

/-podpisano elektronicznie/

[7] 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.