



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Miroslaw Wróblewski

Warszawa, 6.05.2024 r.

DOL.401.512.2021.WL.JR

Pan
Dariusz Salamończyk
Zastępca Szefa Kancelarii Sejmu RP
Kancelaria Sejmu RP

ul. Wiejska 4/6/7
00-902 Warszawa
Skrytka ESP: /KSRP/SkrytkaESP

Wniosek nr 12-DY-SZEP-133
Data DS. 18.04.188.2021
Data wpływu 10.05.2024

Szanowny Panie Ministrze,

odpowiadając na pismo z 23 kwietnia br. (data wpływu do Urzędu Ochrony Danych Osobowych 26 kwietnia br.) o sygn.: SPS-WP.020.120.5.2024 przedstawiające rządowy projekt ustawy o ochronie sygnalistów (druk sejmowy nr 317, dalej jako „projekt ustawy”), działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹ oraz art. 51 ustawy o ochronie danych osobowych² uprzejmie informuję, że w toku wznowionego rządowego procesu

¹ 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, dalej jako: rozporządzenie 2016/679), Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.

² Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, tj. Dz. U. z 2019 r. poz. 1781, dalej jako: ustawa o ochronie danych osobowych.

legislacyjnego nad projektem przedmiotowej ustawy Prezes UODO brał udział w procesie konsultacyjnym z własnej inicjatywy. Pomimo obowiązku wynikającego z art. 51 ustawy o ochronie danych osobowych projektodawca na etapie rządowym, po rozpoczęciu na nowo prac nad zmienionym projektem, nie zwrócił się o opinię do organu nadzorczego, chociaż organ nadzorczy uczestniczył w pracach w latach poprzednich. Ponieważ jednak projekt budzi szereg wątpliwości z punktu widzenia zgodności z przepisami o ochronie danych osobowych, Prezes UODO przedstawił swoje uwagi w dniach 24 lutego i 4 kwietnia br. (pisma o tożsamej sygnaturze). Uwagi Prezesa UODO nie zostały uwzględnione w aktualnie procedowanej wersji projektu ustawy.

Wobec powyższego pragnę podtrzymać **dotychczasowe stanowisko i w uzupełnieniu do poprzednio przedstawionych uwag - w związku z kolejnymi wprowadzonymi zmianami w projekcie ustawie – zwrócić uwagę na istotne zagadnienia z punktu widzenia stosowania rozporządzenia 2016/679.**

I. Ustawodawca mocą art. 7 ust. 1 projektu ustawy wprowadza **możliwość** przyjmowania przez podmioty prawne, Rzecznika Praw Obywatelskich i organy publiczne **zgłoszeń dokonywanych anonimowo** i korzystając z przysługującego mu uprawnienia wynikającego z art. 6 ust. 2 dyrektywy 2019/1937³ nie decyduje się na wprowadzenie obligatoryjnego wdrożenia anonimowego trybu dokonywania zgłoszeń wewnętrznych, jak i zgłoszeń zewnętrznych. Z kolei zgodnie z intencją projektodawcy **„tryb postępowania z informacjami o naruszeniach prawa zgłoszonymi anonimowo”** będzie stanowił element procedury zgłoszeń wewnętrznych podmiotu prawnego (art. 25 ust.1 pkt 4 projektu ustawy) lub procedury zgłoszeń zewnętrznych (art. 31 ust. 1 pkt 1 projektu ustawy- w przypadku jej ustalania przez Rzecznika Praw Obywatelskich, art. 33 projektu ustawy - w przypadku jej ustalania przez organ publiczny). Jednocześnie **„dane osobowe sygnalisty oraz osoby, której dotyczy zgłoszenie, niezbędne do identyfikacji tych osób”** stanowią obligatoryjny element rejestru zgłoszeń wewnętrznych prowadzonego przez podmiot prawny (art. 29 ust. 4 pkt 3 projektu ustawy), rejestru zgłoszeń zewnętrznych prowadzonego przez Rzecznika Praw Obywatelskich (art. 45 ust. 3 pkt 3 projektu ustawy) oraz rejestru zgłoszeń zewnętrznych prowadzonego przez organ publiczny (art. 46 ust. 3 pkt 3 projektu ustawy). Dodatkowo, w przypadku zgłoszenia wewnętrznego adres do kontaktu sygnalisty stanowi element rejestru zgłoszeń wewnętrznych zgodnie z art. 29 ust. 4 pkt 4 projektu ustawy.

W konsekwencji tak zaprojektowanej konstrukcji przepisów powstaje niespójność proponowanych rozwiązań w odniesieniu **do katalogów danych zawartych w rejestrach zgłoszeń**, których zakres nie został dostosowany do możliwości anonimowego dokonania zgłoszenia naruszenia. Wyjaśnienia tej kwestii nie dostarcza uzasadnienie projektu, zgodnie z którym: „Projektodawca nie zdecydował się na wprowadzenie obligatoryjnego wdrożenia anonimowego trybu dokonywania zgłoszeń wewnętrznych, jak i zgłoszeń zewnętrznych. Oznacza to, że dla skutecznego dokonania

³ Art. 6 ust. 2 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r., Dz. Urz. L 305 z 26.11.2019, s. 17, dalej jako: dyrektywa 2019/1937.

zgłoszenia osoba zgłaszająca będzie musiała podać dane identyfikujące taką osobę i umożliwiające kontakt z taką osobą.”. W związku z tym w opinii organu nadzorczego w projekcie ustawie należy w sposób **przejrzysty i konsekwentny uregulować prawa i obowiązki sygnalistów**, chcących dokonać zgłoszenia zarówno w trybie imiennym, jak i anonimowym.

II. Dodatkowo należałoby rozważyć określenie w projekcie ustawie zakresu danych osobowych umożliwiających identyfikację tożsamości sygnalistów. Takie rozwiązanie zapewniłoby przyjęcie spójnego katalogu przetwarzanych danych osobowych w poszczególnych rejestrach w kontekście identyfikacji. Dobór zakresu danych powinien nastąpić z uwzględnieniem celu tego elementu regulacji, czyli identyfikacji tożsamości zgłaszającego oraz osoby, której dotyczy zgłoszenie oraz z poszanowaniem zasady „minimalizacji danych” (art. 5 ust.1 lit. c rozporządzenia 2016/679). Zapewniłoby to zgodność projektowanego rozwiązania z art. 17 dyrektywy 2019/1937 stanowiącym, że „Przetwarzania danych osobowych zgodnie z niniejszą dyrektywą, w tym wymiany lub przekazywania danych osobowych przez właściwe organy, dokonuje się zgodnie z rozporządzeniem (UE) 2016/679 (...)”. Zasadą przyjmowanych rozwiązań powinno być określenie w treści przepisów projektu ustawy, a nie w treści aktów wewnątrzorganizacyjnych (procedur), odpowiednio (wyczerpująco) skonstruowanej podstawy prawnej dla określania obowiązku przetwarzania danych osobowych, celem zapewnienia stosowania zasad dotyczących przetwarzania danych osobowych, w tym zasady legalizmu (art. 5 ust. 1 lit. a rozporządzenia 2016/679), ograniczenia celu (art. 5 ust. 1 lit. b rozporządzenia 2016/679) oraz zasady minimalizacji danych (art. 5 ust. 1 lit. c rozporządzenia 2016/679).

III. Rozważenia wymaga także przyjęcie spójnego standardu ochrony praw pozostałych osób, których dane będą przetwarzane w związku ze zgłoszeniem naruszenia prawa. Ochrona poufności tożsamości tych osób, tj. osób, których zgłoszenie dotyczy, czy osób trzecich wskazanych w zgłoszeniu powinna być zagwarantowana przepisami projektu ustawy, a nie treścią procedur zgłoszeń wewnętrznych na co wskazuje art. 27 ust. 1 projektu ustawy czy zewnętrznych zgodnie z art. 43 projektu ustawy. Ponadto uzasadnionym byłoby dostosowanie redakcyjne i przyjęcie stosownej definicji pojęcia „osoby trzeciej wskazanej w zgłoszeniu” w związku z przewidzianą w art. 27 ust.1 projektu ochroną jej tożsamości, jak również wyraźne wskazanie czy „osoba pomagająca w dokonaniu zgłoszenia” zgodnie z definicją przyjętą w art. 2 pkt 8 projektu ustawy i „osoba powiązana z sygnalistą” zdefiniowana w art. 2 pkt 9 projektu ustawy- są „osobami trzecimi wskazanymi w zgłoszeniu” zgodnie z intencją projektodawcy, czy też ich definicje zostały utworzone jedynie na potrzeby zachowania terminologii przyjętej w przepisach implementowanej dyrektywy.

IV. Kluczowym elementem ochrony sygnalisty jest obowiązek zapewnienia poufności jego tożsamości wynikający z art. 16 ust.1 dyrektywy 2019/1937. Z uwagi na ww. ochronę ustawodawca wprowadza zawieszenie prawa osoby, której dane dotyczą dostępu do informacji o źródle danych osobowych (czyli danych

dotyczących sygnalisty). W konsekwencji w art. 8 ust. 5 projektu ustawy wyłączony został spoczywający na administratorze obowiązek (określony w art. 14 ust. 2 lit. f rozporządzenia 2016/679) przekazania osobie, której dane dotyczą informacji o źródle pochodzenia danych osobowych oraz obowiązek realizacji wniosku osoby, której dane dotyczą (określonego w art. 15 ust. 1 lit. g rozporządzenia 2016/679) w zakresie przekazania informacji o źródle pozyskania danych zgodnie z art. 8 ust. 6 projektu ustawy .

Niemniej zauważyć należy, że skorzystanie przez ustawodawcę z prawa do wprowadzenia ww. ograniczeń (na podstawie art. 23 rozporządzenia 2016/679) zostało obwarowane wymaganiami dotyczącymi treści ustawy zawierającej ograniczenia. Zgodnie z art. 23 ust. 2 rozporządzenia 2016/679 wydawany akt prawny powinien zawierać szczegółowe przepisy o: celach przetwarzania lub kategorii przetwarzania, kategoriach danych osobowych, zakresie wprowadzonych ograniczeń, zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu, określeniu administratora lub kategorii administratorów, okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania, ryzyka naruszenia praw lub wolności osoby, której dane dotyczą oraz prawie osób, której dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia. Podkreślić należy, że spełnienie wszystkich ww. wymogów legislacyjnych powinno nastąpić w treści tworzonych przepisów, a nie w ich wyjaśnieniu w uzasadnieniu projektu ustawy. Niezwykle istotną kwestią jest także prawidłowe zrozumienie i zdefiniowanie pojęcia „kategorii danych osobowych”⁴ dla celów ich przetwarzania na podstawie projektowanych przepisów, gdyż nie są nimi - jak to zostało wskazane w uzasadnieniu projektu - „dane o źródle pozyskania danych”, ale poszczególne kategorie danych identyfikujących tożsamość zgłaszającego i pozostałych osób wskazanych w zgłoszeniu.

Prezes UODO zwraca uwagę na prace Europejskiej Rady Ochrony Danych (EROD) dotyczące Wytycznych 10/2020 w sprawie ograniczeń na podstawie art. 23 rozporządzenia 2016/679, które zawierają dogłębną analizę kryteriów stosowania ograniczeń, ocen, które należy uwzględniać, sposobu w jaki osoby, których dane

⁴ Dane osobowe podzielić można na trzy kategorie:

- a) dane tzw. zwykłe, takie jak np.: imię, nazwisko, numer PESEL, adres zamieszkania, data i miejsce urodzenia, numer telefonu, wykonywany zawód, wizerunek, adres e-mail itp. (przetwarzane na podstawie art. 6 ust. 1 rozporządzenia 2016/679),
- b) szczególne kategorie danych osobowych, ujawniające informacje takie jak np. stan zdrowia i poglądy polityczne (art. 9 rozporządzenia 2016/679),
- c) dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa (art. 10 rozporządzenia 2016/679).

dotyczą mogą wykonywać swoje prawa po zniesieniu ograniczeń oraz skutków naruszeń art. 23 rozporządzenia 2016/679⁵.

Dostrzec należy ponadto, że wskazane w art. 8 ust. 5 i 6 projektu ustawy wyłączenia będą uwarunkowane obowiązkiem spełnienia przez sygnalistę warunków zawartych w art. 6 projektu ustawy albo wyrażeniem przez niego wyraźnej zgody na ujawnienie swojej tożsamości bądź przekazanie informacji o źródle pozyskania danych. Zgodnie natomiast z treścią art. 6 projektu ustawy warunkiem objęcia sygnalisty ochroną przewidzianą w przepisach projektu ustawy jest posiadanie przez niego uzasadnionych podstaw, by sądzić, że informacja będąca przedmiotem zgłoszenia lub ujawnienia publicznego jest prawdziwa w momencie dokonywania zgłoszenia lub ujawnienia publicznego i że stanowi informację o naruszeniu prawa. Wobec powyższych założeń ustawodawcy powstaje pytanie – do kogo należeć będzie ocena przesłanki „uzasadnionych podstaw” utwierdzających sygnalistę w przekonaniu o prawdziwości informacji objętej zgłoszeniem.

Organ nadzorczy zwraca uwagę na obiektywną trudność w dokonaniu takiej oceny, bez uszczerbku dla stosowania pewnych uproszczeń w dokonywaniu kwalifikacji uzasadnionego przekonania sygnalisty o wystąpieniu naruszenia. Z kolei mając na względzie **zasadę przejrzystości** wyrażoną w art. 5 ust. 1 lit. a rozporządzenia 2016/679 oczekuje się, aby tworzone przepisów sposób jasny, precyzyjny oraz wyczerpujący, w sposób nie budzący wątpliwości interpretacyjnych regulowały kwestie dotyczące przetwarzania danych.

V. Wprowadzana regulacja zasadniczo tworzy ramy prawne dla ochrony poufności tożsamości sygnalisty, zgodnie z którymi jego dane osobowe będą podlegały ujawnieniu tylko, gdy zgłaszający wyrazi na to wyraźną zgodę (art. 8 ust. 1 oraz art. 8 ust. 5 i 6 projektu ustawy). Skoro podstawą legalizującą udostępnienie danych sygnalisty będzie wyrażenie przez niego wyraźnej zgody, to uzasadnione byłoby odesłanie w ustawie do treści przepisów rozporządzenia 2016/679, że „zgoda osoby, której dane dotyczą oznacza pojęcie zdefiniowane w art. 4 pkt 11 rozporządzenia 2016/679”, a jej wyrażenie następuje zgodnie z warunkami wskazanymi w art. 7 rozporządzenia 2016/679.

VI. W projektowanym art. 8 wskazano dwa okresy retencji danych osobowych, odpowiednio:

- **12 miesięcy** po zakończeniu roku kalendarzowego, w którym przekazano zgłoszenie zewnętrzne do organu publicznego właściwego do podjęcia działań następczych - gdy dane osobowe przetwarzane w związku z przyjęciem zgłoszenia

⁵ Przykład zastosowania ograniczenia mającego na celu ochronę praw i wolności innych osób na podstawie art. 23 ust. 1 lit. i rozporządzenia 2016/679 został przywołany w pkt 34 Wytycznych 10/2020 EDOD: „Ograniczenie mające na celu ochronę praw i wolności innych osób można zilustrować przykładem dochodzenia administracyjnego lub postępowania dyscyplinarnego, lub postępowania przygotowawczego w sprawie zarzutów molestowania w miejscu pracy. W takim przypadku **akt prawny może przewidywać**, że osoba, wobec której prowadzone jest dochodzenie lub postępowanie dyscyplinarne, może podlegać ograniczeniu przysługującego jej prawa dostępu, jeżeli nie można ujawnić tożsamości domniemanej ofiary lub świadka lub **sygnalisty** w celu ochrony tych osób przed działaniami odwetowymi (...).”

zewnętrznego oraz dokumenty związane z tym zgłoszeniem są przechowywane przez Rzecznika Praw Obywatelskich (art. 8 ust. 7 projektu ustawy) oraz

- 3 lata po zakończeniu roku kalendarzowego, w którym przekazano zgłoszenie zewnętrzne do organu publicznego właściwego do podjęcia działań następnych lub zakończono działania następne lub po zakończeniu postępowań zainicjowanych tymi działaniami - gdy dane osobowe przetwarzane w związku z przyjęciem zgłoszenia lub podjęciem działań następnych oraz dokumenty związane z tym zgłoszeniem są przechowywane przez podmiot prawny oraz organ publiczny (art. 8 ust. 8 projektu ustawy).

Proponowane rozwiązanie zawarte w art. 8 ust. 7 projektu ustawy budzi wątpliwości interpretacyjne, gdyż taka redakcja przepisu sugeruje przypadek przekazania zgłoszenia bezpośrednio do organu publicznego - jako jednego z umocowanych podmiotów (oprócz Rzecznika Praw Obywatelskich) do przyjmowania zgłoszeń zewnętrznych zgodnie z art. 30 ust. 2 projektu. Tymczasem najbardziej prawdopodobną intencją prawodawcy wydaje się być wskazanie 12 miesięcznego okresu po zakończeniu roku kalendarzowego, w którym Rzecznik Praw Obywatelskich przekazał zgłoszenie zewnętrzne do organu publicznego właściwego do podjęcia działań następnych, zgodnie art. 31 pkt 2 projektu ustawy. Istotne jest zatem zredagowanie brzmienia przedmiotowego przepisu w sposób nie budzący wskazanych wątpliwości.

Uzasadnienie projektu zawiera wyjaśnienie 3 letniego okresu przechowywania danych przez podmiot prawny oraz organ publiczny jako niezbędnego dla celów ewentualnych postępowań po zakończeniu działań następnych oraz spójnego z terminem przedawnienia roszczeń ze stosunku pracy (art. 291 Kodeksu pracy), jak też roszczeń o świadczenia okresowe i roszczeń związanych z prowadzeniem działalności gospodarczej (art. 118 Kodeksu cywilnego). Projektodawca natomiast nie uzasadnił proponowanego 12 miesięcznego okresu retencji danych przechowywanych przez Rzecznika Praw Obywatelskich.

VII. Ponownej analizy pod kątem zgodności projektu ustawy z przepisami dyrektywy 2019/1937 wymaga art. 25 ust.1 pkt 1 projektu ustawy (jak też pozostający w związku z nim art. 28 ust.1 i 2 oraz art. 29 ust. 2 projektu ustawy), który upoważnia podmiot zewnętrzny do przyjmowania zgłoszeń wewnętrznych.

Art. 16 ust. 1 dyrektywy 2019/1937 jednoznacznie formułuje wymóg zapewnienia przez państwa członkowskie, by tożsamość osoby dokonującej zgłoszenia nie została ujawniona – bez wyrażnej zgody tej osoby – żadnej osobie, która nie jest upoważnionym członkiem personelu właściwym do przyjmowania zgłoszeń i podejmowania w związku z nimi działań następnych. Skoro prawodawca unijny dookreślił i wyraźnie wskazał upoważnionych członków personelu jako osoby właściwe do przetwarzania danych w związku z przyjmowaniem zgłoszeń i podejmowania w związku z nimi działań następnych - to regulacje krajowe powinny również uwzględniać takie rozwiązanie, co zostało zasygnalizowane w uzasadnieniu projektu stwierdzeniem, że: „podmiotami uprawnionymi do przetwarzania danych osobowych na mocy projektowanej ustawy będą wyłącznie zdefiniowane w niej podmioty prawne oraz

organy publiczne, a także pracownicy upoważnieni przez te podmioty i organy”. Dlatego też ponownej analizie należałoby poddać prawidłowość umocowania podmiotu zewnętrznego do przyjmowania zgłoszeń wewnętrznych zgodnie z art. 25 ust.1 pkt 1 projektu.

VIII. Ponadto w art. 28 ust. 2 projektu ustawy prawodawca wskazuje, że umowa zawarta z podmiotem zewnętrznym w celu powierzenia obsługi przyjmowania zgłoszeń, potwierdzania przyjęcia zgłoszenia, przekazania informacji zwrotnej oraz zapewnienia informacji na temat procedury zgłoszeń wewnętrznych z zastosowaniem rozwiązań technicznych i organizacyjnych zapewniających zgodność tych czynności z ustawą - określa szczegółowe prawa i obowiązki podmiotu zewnętrznego związane z przetwarzaniem danych osobowych, o których mowa, w szczególności w art. 28 ust. 3 rozporządzenia 2016/679. Uzasadnionym byłoby prerogatywowanie tej normy celem zapewnienia podmiotowi zewnętrznemu, w oparciu o projektowane przepisy działania, w imieniu i na rzecz administratora. Zgodnie z przepisami rozporządzenia 2016/679 prawa i obowiązki związane z przetwarzaniem danych osobowych wynikają bowiem z rozporządzenia 2016/679, natomiast treść umowy wiążącej podmiot przetwarzający z administratorem powinna określać m.in.: przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą (zgodnie z art. 28 ust. 3 oraz motywem 81 rozporządzenia 2016/679).

Uprzejmie dziękuję za przedstawienie do zaopiniowania projektu ustawy.
Uwagi organu właściwego w sprawie ochrony danych osobowych przedstawiane w toku prac legislacyjnych mają charakter eksperckich wskazówek dla ustawodawcy, który podejmuje decyzję co do ostatecznego kształtu przyjmowanych przepisów i odpowiada za zapewnienie ich zgodności z przepisami o ochronie danych osobowych.

Z wyrazami szacunku,
z up. Prezesa Urzędu
Ochrony Danych Osobowych
Zastępczyni Prezesa
dr hab. Agnieszka Grzelak

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym/

