PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 24.02.2024 r.

DOL.401.512.2021.

Pan
Maciej Berek
Minister – Członek Rady Ministrów
Przewodniczący Stałego Komitetu
Rady Ministrów

Kancelaria Prezesa Rady Ministrów

Szanowny Panie Ministrze,

w związku ze wznowieniem rządowego procesu legislacyjnego nad **projektem ustawy o ochronie osób zgłaszających naruszenia prawa** sporządzonym w dniu 8 stycznia 2024 r. przez Ministra Rodziny, Pracy i Polityki Społecznej i przekazanym do rozpatrzenia przez Stały Komitet Rady Ministrów, Prezes Urzędu Ochrony Danych Osobowych (organ nadzorczy) – w kontekście przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietna 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., dalej jako „rozporządzenie 2016/679) – pragnie zwrócić uprzejmie uwagę na następujące zagadnienia.

W toku dotychczas prowadzonych prac nad projektem przedmiotowej ustawy organ nadzorczy przedstawił opinie legislacyjne do kolejnych wersji projektowanego aktu, w tym ostatnie uwagi zostały przekazane w lipcu 2022 r. Aktualnie procedowana wersja projektu pomimo, że została zmieniona merytorycznie, nie została przekazana do zaopiniowania organowi nadzorczemu, tymczasem szereg zaproponowanych rozwiązań budzi wątpliwości z punktu widzenia zgodności z przepisami o ochronie danych osobowych[1].

I. Projektodawca, sporządzając projekt przedmiotowej ustawy implementującej dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r.[2], co do zasady nie zdecydował się na przyjęcie rozwiązania umożliwiającego anonimowe dokonywanie zgłoszeń naruszenia prawa – korzystając z uprawnienia wynikającego z art. 6 ust. 2 tejże dyrektywy[3]. Rezygnację z anonimowego trybu zgłaszania naruszeń uzasadnił przesłankami o charakterze praktycznym, takimi jak: ryzyko nadmiernego wpływu informacji przypadkowych i o niskiej wartości z perspektywy rzeczywistego przeciwdziałania naruszeniom, czy trudności w uzyskaniu dodatkowych informacji od zgłaszającego, gdy już przekazane informacje są istotne, lecz niepełne, jak też trudności związane z późniejszym udowodnieniem, na potrzeby jakiegokolwiek postępowania, związku przekazanej informacji z osobą zgłaszającego. Jednocześnie projektodawca zapewnia ochronę osobom, które dokonały anonimowego zgłoszenia lub anonimowo ujawniły publicznie informacje, a następnie zostały zidentyfikowane i doświadczyły działań odwetowych, pod warunkiem że miały one uzasadnione podstawy sądzić, że będące przedmiotem zgłoszenia informacje są prawdziwe w momencie dokonywania zgłoszenia i że informacje takie stanowią informację o naruszeniu prawa (art. 7 projektu).

W projekcie ustawy przyjęto, że podstawą prawną umożliwiającą dokonywanie zgłoszeń oraz regulującą procedury dokonywania tych zgłoszeń przez zgłaszających, jak też podejmowanie działań następczych będzie wewnątrzorganizacyjny akt prawny, tzw. „procedura zgłoszeń wewnętrznych” w przypadku podmiotu prawnego (art. 24 ust. 1 projektu) oraz „procedura zgłoszeń zewnętrznych” w przypadku Rzecznika Praw Obywatelskich (art. 31 pkt 1 projektu) i organu publicznego (art. 33 projektu).

---

[1] Jednym z zadań organu nadzorczego jest opiniowanie projektów aktów prawnych, którego realizacja w toku procesu legislacyjnego następuje poprzez analizę projektowanych lub nowelizowanych przepisów pod kątem zapewnienia zgodności treści projektowanych regulacji z przepisami rozporządzenia 2016/679 na podstawie: art. 57 ust. 1 lit. c rozporządzenia 2016/679 oraz art. 51 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) jak i § 38 uchwały Nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów (M. P. z 2022 r. poz. 348).

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz. Urz. UE L 305 z 26.11.2019, str. 17, Dz. Urz. UE L 347 z 20.10.2020, str. 1, Dz. Urz. UE L 265 z 12.10.2022, str. 1 oraz Dz. Urz. UE L 150 z 09.06.2023, str. 40), dalej dyrektywa 2019/1937.

[3] Art. 6 ust. 2 dyrektywy 2019/1937: „Bez uszczerbku dla istniejących na mocy prawa Unii obowiązków w zakresie anonimowego zgłaszania, niniejsza dyrektywa nie wpływa na uprawnienia państw członkowskich do decydowania o tym, czy podmioty prawne w sektorze prywatnym lub publicznym oraz właściwe organy są zobowiązane do przyjmowania anonimowych zgłoszeń na temat naruszeń i podejmowania w związku z nimi działań następczych”.

Wprawdzie w projektowanej regulacji ustawowej zrezygnowano ze wskazania, iż w treści procedury zgłoszeń (zarówno wewnętrznych, jak i zewnętrznych) będzie określony m.in. zakres danych osobowych niezbędnych do skutecznego dokonania zgłoszenia, niemniej konieczność podania danych identyfikujących osobę dokonującą zgłoszenia oraz osobę, której dotyczy zgłoszenie, wynika z katalogu danych zawartych w rejestrze zgłoszeń wewnętrznych prowadzonym przez podmiot prawny[4] (**art. 29 ust. 4 pkt 3 projektu**), rejestrze zgłoszeń zewnętrznych prowadzonym przez Rzecznika Praw Obywatelskich (**art. 45 ust. 3 pkt 3 projektu)** oraz rejestrze zgłoszeń zewnętrznych prowadzonym przez organ publiczny (**art. 46 ust. 3 pkt 3 projektu**). Z kolei wskazanie adresu do kontaktu zgłaszającego, jakim jest adres korespondencyjny lub adres poczty elektronicznej zgłaszającego, zgodnie z art. 25 ust.1 pkt 2 projektu, stanowi element rejestru zgłoszeń wewnętrznych (**art. 29 ust. 4 pkt 4 projektu**).

Ponadto proponowaną treścią **art. 8 ust. 1** projektu[5] wprowadza się regulację dotyczącą ochrony danych osobowych pozwalających na ustalenie tożsamości zgłaszającego w celu zapewnienia obowiązku zachowania poufności wyrażonego w art. 16 ust. 1[6] dyrektywy wdrażanej mocą projektowanego aktu.

Przedstawione powyżej regulacje wskazują, że projektodawca za podstawę przyjmuje imienny tryb zgłaszania naruszeń prawa, z zachowaniem poufności zgłaszającego i nie reguluje wprost możliwości dokonania anonimowego zgłoszenia naruszenia, choć ochronę osób korzystających ze zgłoszenia w tym trybie przewiduje w art. 7 projektu[7]. Powstaje zatem niespójność projektowanych rozwiązań wymagająca konsekwentnego przyjęcia odpowiednich przepisów jednolicie kształtujących prawa i obowiązki osób, które zgłaszają informacje o naruszeniach prawa w zakresie trybu dokonania zgłoszenia[8].

---

[4] Zgodnie z art. 2 pkt 10 projektu podmiot prawny oznacza podmiot prywatny lub podmiot publiczny, przy czym podmiot prywatny oznacza osobę fizyczną prowadzącą działalność gospodarczą, osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, której ustawa przyznaje zdolność prawną, lub pracodawcę, jeżeli nie są podmiotami publicznymi (art. 2 pkt 11 projektu), a podmiotem publicznym jest podmiot wskazany w art. 3 ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. poz. 1641 oraz z 2022 r. poz. 1700) zgodnie z art. 2 pkt 12 projektu.

[5] Art. 8 ust. 1. projektu: „Dane osobowe zgłaszającego, pozwalające na ustalenie jego tożsamości nie podlegają ujawnieniu nieupoważnionym osobom, chyba że za wyraźną zgodą zgłaszającego".

[6] Art. 16 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz. Urz. UE L 305 z 26.11.2019, str. 17, Dz. Urz. UE L 347 z 20.10.2020, str. 1, Dz. Urz. UE L 265 z 12.10.2022, str. 1 oraz Dz. Urz. UE L 150 z 09.06.2023, str. 40): „Państwa członkowskie zapewniają, by tożsamość osoby dokonującej zgłoszenia nie została ujawniona – bez wyraźnej zgody tej osoby – żadnej osobie, która nie jest upoważnionym członkiem personelu właściwym do przyjmowania zgłoszeń i podejmowania w związku z nimi działań następczych. Ma to również zastosowanie do wszelkich innych informacji, na podstawie których można bezpośrednio lub pośrednio zidentyfikować tożsamość osoby dokonującej zgłoszenia".

[7] Art. 7 projektu: Jeżeli informacja o naruszeniu prawa została anonimowo zgłoszona podmiotowi prawnemu, Rzecznikowi Praw Obywatelskich albo organowi publicznemu lub ujawniona publicznie, a następnie doszło do ujawnienia tożsamości zgłaszającego i doświadczył on działań odwetowych, przepisy rozdziału 2 stosuje się, jeżeli zostały spełnione warunki określone w art. 6.

[8] Zgodnie z art. 2 pkt 15 projektu poprzez zgłoszenie należy rozumieć ustne lub pisemne zgłoszenie wewnętrzne lub zgłoszenie zewnętrzne, przekazane zgodnie z wymogami określonymi w projektowanej ustawie.

II. Dodatkowo, skoro projektodawca przewiduje konieczność dokonania identyfikacji osoby zgłaszającego naruszenie oraz osoby, której zgłoszenie dotyczy, należałoby rozważyć wskazanie w projektowanym akcie poprzez jakie dane osobowe możliwa będzie identyfikacja tożsamości ww. osób, zwłaszcza, że zgodnie z przedstawioną w uzasadnieniu projektu intencją projektodawcy „przewiduje się, iż przedmiotem przetwarzania będą dane obejmujące: imię i nazwisko zgłaszającego (…)". 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[9]). Zapewniłoby to zgodność projektowanego rozwiązania z art. 17 implementowanej dyrektywy 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 (…)".

III. Zasadą przyjmowanych rozwiązań powinno być określenie w treści przepisów projektowanej ustawy, a nie w treści aktów wewnątrzorganizacyjnych (procedur) odpowiednio (wyczerpująco) skonstruowanej **podstawy prawnej dla określania obowiązku przetwarzania danych osobowych**, w szczególności celu przetwarzania i zakresu danych osobowych niezbędnych dla wykonania tego celu, sposobu przetwarzania danych adekwatnego do celów przetwarzania oraz innych elementów niezbędnych dla kompleksowego uregulowania przetwarzania danych dla osiągnięcia celów prawodawcy.

IV. Projektowanym aktem wprowadza się ograniczenie określonego zakresu praw i obowiązków spoczywających na administratorze w zakresie przetwarzania danych osobowych przewidzianych w rozporządzeniu 2016/679 poprzez wyłączenie obowiązku przekazania osobie, której dane dotyczą (określonego w art. 14 ust. 2 lit. f rozporządzenia 2016/679) informacji o źródle pochodzenia danych osobowych (**art. 8 ust. 5 projektu**) oraz wyłączenie obowiązku realizacji wniosku osoby, której dane dotyczą (określonego w art. 15 ust. 1 lit. g rozporządzenia 2016/679) w zakresie udzielenia wszelkich dostępnych informacji o ich źródle zgodnie z (**art. 8 ust. 6 projektu**). Niewątpliwie celem projektowanych ograniczeń, będących w istocie wyłączeniem bezpośredniej stosowalności wskazanych przepisów rozporządzenia 2016/679, jest obowiązek zapewnienia poufności tożsamości zgłaszającego naruszenie prawa, jako kluczowego elementu koncepcji ochrony danych sygnalisty. W konsekwencji ustawodawca uznał za niezbędne ograniczenie prawa osoby, której dane dotyczą, a mianowicie prawa dostępu do informacji o źródle pochodzenia danych (czyli danych dotyczących zgłaszającego). Niemniej zauważyć należy, że skorzystanie przez ustawodawcę z prawa do wprowadzenia ograniczeń na podstawie art. 23 rozporządzenia 2016/679 zostało obwarowane wymaganiami dotyczącymi treści ustawy

[9] Art. 5 ust. 1 lit. c rozporządzenia 2016/679: Dane osobowe muszą być: adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych").

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 projektowanej ustawy. Niezwykle istotną kwestią jest także prawidłowe zrozumienie i zdefiniowanie pojęcia „kategorii danych osobowych”[10] 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. Organ nadzorczy zwraca uwagę projektodawcy 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 dotyczą mogą wykonywać swoje prawa po zniesieniu ograniczeń oraz skutków naruszeń art. 23 rozporządzenia 2016/679.

V. Ponadto, należy stwierdzić, że wprowadzana regulacja zasadniczo tworzy ramy prawne dla ochrony poufności tożsamości zgłaszającego naruszenie prawa, zgodnie z którymi jego dane osobowe będą podlegały ujawnieniu tylko, gdy zgłaszający wyrazi na to wyraźną zgodę (**art. 8 ust. 1 projektu, art. 8 ust. 5 i 6 projektu**). Skoro podstawą legalizującą udostępnienie danych zgłaszającego 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. 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

[10] 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).

zgłoszenie dotyczy, czy osób trzecich, powinna być zagwarantowana przepisami projektowanej ustawy, a nie treścią procedur zgłoszeń wewnętrznych na co wskazuje **art. 27 ust. 1 projektu** czy zewnętrznych zgodnie **z art. 43 projektu.** 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** i „osoba powiązana ze zgłaszającym", zdefiniowana w **art. 2 pkt 9 projektu**, 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.

VII. 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 zewnętrznego oraz dokumenty związane z tym zgłoszeniem są przechowywane przez Rzecznika Praw Obywatelskich (**art. 8 ust. 7 projektu**) oraz
- **3 lata** po zakończeniu roku kalendarzowego, w którym przekazano zgłoszenie zewnętrzne do organu publicznego właściwego do podjęcia działań następczych lub zakończono działania następcze lub po zakończeniu postępowań zainicjowanych tymi działaniami - gdy dane osobowe przetwarzane w związku z przyjęciem zgłoszenia lub podjęciem działań następczych oraz dokumenty związane z tym zgłoszeniem są przechowywane przez podmiot prawny oraz organ publiczny (**art. 8 ust. 8 projektu**).

Proponowane rozwiązanie zawarte w **art. 8 ust. 7 projektu** 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 następczych zgodnie art. 31 pkt 2 projektu. 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 następczych oraz spójnego z terminem przedawnienia roszczeń ze stosunku pracy (art. 291 Kodeku 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, przez co celowym wydaje się uzupełnienie tej materii.

VIII. Ponownej analizy pod kątem zgodności projektowanego aktu z przepisami implementowanej dyrektywy wymaga **art. 28 ust.1 i 2 projektu, art. 29 ust. 2** w związku z upoważnieniem podmiotu zewnętrznego, o którym mowa **w art. 25 ust.1 pkt 1** projektu do przyjmowania zgłoszeń wewnętrznych.

Art. 16 ust. 1 dyrektywy[11] jednoznacznie formułuje wymóg zapewnienia przez państwa członkowskie, by tożsamość osoby dokonującej zgłoszenia nie została ujawniona – bez wyraźnej zgody tej osoby – żadnej osobie, która nie jest upoważnionym członkiem personelu właściwym do przyjmowania zgłoszeń i podejmowania w związku z nimi działań następczych. 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 następczych, 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.

IX. Ponadto w **art. 28 ust. 2 projektu** 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 przeredagowanie 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

[11] Art. 16 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz. Urz. UE L 305 z 26.11.2019, str. 17, Dz. Urz. UE L 347 z 20.10.2020, str. 1, Dz. Urz. UE L 265 z 12.10.2022, str. 1 oraz Dz. Urz. UE L 150 z 09.06.2023, str. 40): „Państwa członkowskie zapewniają, by tożsamość osoby dokonującej zgłoszenia nie została ujawniona – bez wyraźnej zgody tej osoby – żadnej osobie, która nie jest upoważnionym członkiem personelu właściwym do przyjmowania zgłoszeń i podejmowania w związku z nimi działań następczych. Ma to również zastosowanie do wszelkich innych informacji, na podstawie których można bezpośrednio lub pośrednio zidentyfikować tożsamość osoby dokonującej zgłoszenia".

osoby, której dane dotyczą (zgodnie z art. 28 ust. 3 oraz motywem 81 rozporządzenia 2016/679).

Uwagi organu nadzorczego – co należy podkreślić – mają charakter wskazówek eksperckich, a za ostateczną zgodność projektowanych przepisów z ogólnym rozporządzeniem o ochronie danych odpowiada oczywiście ostatecznie projektodawca. Należy jednak wskazać, że celem projektodawcy powinno być tworzenie przepisów, które będą spełniały standardy rozporządzenia 2016/679, co w praktyce oznacza zapewnienie rzetelności i przejrzystości procesom przetwarzania w ich oparciu i nienarażanie administratorów danych osobowych na ryzyka związane z niewłaściwym stosowaniem przepisów. Przyjęcie – już na etapie tworzenia przepisów prawa – rozwiązań zapewniających stosowanie przepisów ogólnego rozporządzenia o ochronie danych pozwoli wypracować rozwiązania optymalne dla realizacji ratio legis regulacji, tj. celów tworzonego aktu i zapewnienia stosowania przepisów rozporządzenia 2016/679. Wyrażam nadzieję, że niniejsze uwagi będą pomocne w realizacji tego celu.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

Do wiadomości:
Pan Marcin Wiącek
Rzecznik Praw Obywatelskich