Ustawa o ochronie sygnalistów z perspektywy RODO – relacja z seminarium

Posted on 2024-08-30

7 sierpnia w Urzędzie Ochrony Danych Osobowych odbyło się seminarium, podczas którego prezes UODO Mirosław Wróblewski wspólnie z przedstawicielami Społecznego Zespołu Ekspertów przy PUODO oraz zewnętrznymi ekspertami zastanawiali się nad interpretacją przepisów tej ustawy.

Wątpliwości Urzędu

Ustawa o ochronie sygnalistów została przyjęta przez Sejm RP w dniu 14.06.2024. Prezes UODO przewidując, że stosowanie ustawy może zrodzić poważne wątpliwości w praktyce, wraz ze Społecznym Zespołem Ekspertów przy PUODO oraz ekspertami Urzędu podjęli inicjatywę konsultacji społecznych. W ramach konsultacji można było zgłaszać pytania i obiekcje, dotyczące stosowania tych przepisów w zakresie ochrony danych osobowych.

Na podstawie przesłanych uwag UODO przygotował wyjaśnienia, które zostały przedstawione w ramach otwartego spotkania w formie seminarium. Jego celem było zidentyfikowanie i omówienie obszarów, które mogą generować największe wątpliwości

interpretacyjne.

Uwagi UODO do ustawy

Mirosław Wróblewski na początku spotkania, przypomniał o kilku uwagach, które Urząd zgłaszał w toku prac legislacyjnych. Chodziło o wątpliwości dotyczące przepisów w odniesieniu do katalogów danych zawartych w rejestrach zgłoszeń. Ich zakres nie został dostosowany do możliwości anonimowego dokonania zgłoszenia naruszenia. Jak podkreślił: „Ustawa wymaga przejrzystego i konsekwentnego przyjęcia pewnych przepisów kształtujących prawa i obowiązki sygnalistów, chcących dokonać zgłoszenia zarówno w trybie imiennym, jak i w trybie anonimowym, jeśli organizacja dopuści takie anonimowe zgłoszenia".

Prezes UODO zaznaczył, że organ nadzorczy postulował o wyraźne określenie w ustawie poprzez jakie dane osobowe możliwa będzie identyfikacja tożsamości sygnalisty:

– „Dobór zakresu danych powinien następować z uwzględnieniem celu regulacji, czyli identyfikacji tożsamości zgłaszającego oraz osoby, której dotyczy zgłoszenie z uszanowaniem jednoczesnym zasady minimalizacji danych". Mamy bowiem w art. 17 dyrektywy 2019/1937 założenie zgodności i poszanowania przepisów RODO.

MirosławWróblewski zaakcentował, że „kluczowym elementem ochrony sygnalisty jest obowiązek zapewnienia poufności jego tożsamości, wynikający z art. 16 ust. 1 dyrektywy. Tutaj warto odnieść się do art. 8 ust. 5 i ust. 6 ustawy o sygnalistach, gdzie ograniczane są prawa wynikające z RODO". Natomiast w opinii UODO spełnienie tych wymogów zgodnie z art. 23 RODO powinno nastąpić
w treści przepisów ustawowych.

Prezes UODO wspomniał również o wątpliwościach odnoszących się do art. 6 ustawy – do kogo należeć będzie ocena przesłanki uzasadnionych podstaw utwierdzających sygnalistę w przekonaniu o prawdziwości informacji ujętej w zgłoszeniu. Podkreślił również, że siatka

pojęciowa ustawy przysparza trudności w interpretacji przepisów.

Dr Mirosław Gumularz, przewodniczący Społecznego Zespołu Ekspertów przy PUODO podziękował za przesłanie licznych uwag i aktywny udział w konsultacjach społecznych. Zapewnił jednocześnie, że każda uwaga została wnikliwie przeanalizowana przez Społeczny Zespół Ekspertów w dialogu z Urzędem oraz zaprezentował najbardziej problematyczne kwestie, jakie pojawiły się w ramach konsultacji społecznych. Omawiano je w kolejnych panelach.

Obowiązki informacyjne oraz retencja danych

W panelu poświęconym obowiązkom informacyjnych i retencji danych podkreślono, że w kontekście realizacji obowiązku informacyjnego wskazanego w art. 13 RODO (tj. gdy dane są pozyskiwane bezpośrednio od podmiotu danych) należy:

- uwzględnić, że w procesie przyjmowania zgłoszeń sygnalistów będzie dochodziło do przetwarzania danych osobowych różnych kategorii podmiotów danych, tj. m.in. sygnalistów, osób których dotyczy zgłoszenie, świadków, etc.;

- stosować warstwowe podejście do wykonania obowiązku informacyjnego, odsyłając np. do procedury zgłoszeń wewnętrznych (klauzula informacyjna może się pojawić jednocześnie także na stronie www w miejscu, gdzie będzie informacja o kanałach przyjmowania zgłoszeń);

- obowiązek informacyjny można spełnić także np. przy pierwszym kontakcie z osobą, która potencjalnie może być sygnalistą, np. na etapie rekrutacji, zatrudniania, ofertowania, zawierania umów cywilnych czy innych stosunków z osobami, które będą wykonywały pracę na rzecz podmiotu prawnego.

Paneliści rozważali scenariusze problemów ze spełnieniem obowiązku informacyjnego.

Zastanawiali się też, od kiedy należy liczyć okres retencji. Ustalono, że okres retencji należy

liczyć od momentu wpłynięcia zgłoszenia.

Zwrócono uwagę, że (co podkreślał m.in. dr Paweł Litwiński) art. 8 ust. 3 ustawy o ochronie sygnalistów nie jest do końca jasny, gdy uświadomimy sobie, że jedno zgłoszenie może zawierać informacje o kilku naruszeniach prawa – wtedy okresy retencji danych liczone oddzielnie dla każdej z informacji o naruszeniu prawa mogą być różne. Mimo tego wydaje się, że 3-letni okres retencji danych powinien być zawsze liczony od daty przyjęcia zgłoszenia. Dotyczy to także danych zawartych w rejestrze zgłoszeń (art. 29 ust. 5 ustawy o ochronie sygnalistów) – rejestr zgłoszeń jest bowiem konstruowany w oparciu o zgłoszenie (w rejestrze odnotowujemy numer zgłoszenia itd.,
a więc informacje związane ze zgłoszeniem), a w konsekwencji, to data dokonania zgłoszenia będzie miała podstawowe znaczenia dla obliczania okresu retencji danych.

Zakaz ujawniania tożsamości sygnalisty (który pojawia się m.in. w art. 8 ust. 1 ustawy) należy rozumieć szeroko, w świetle art. 16 ust. 1 dyrektywy o ochronie sygnalistów (dyrektywa 2019/1937 z dnia 23 października 2019 r.). Prowadzący panel mocno zaakcentowali, że nie wolno informować o tożsamości sygnalisty ponieważ zgodnie z art. 16 ust. 1 dyrektywy (implementowany do art. 27 ustawy krajowej) „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” . Przypomnieli słuchaczom, że tożsamość sygnalisty to nie tylko imię i nazwisko, ale też np. jego miejsce i stanowisko pracy.

W kontekście art. 8 ust. 1 ustawy dyskutanci wskazali argumenty przemawiające za tym, że zgoda, o której mowa w tym przepisie jest zgodą w rozumieniu RODO, niemniej dotyczy jednej specyficznej operacji na danych (tj. ujawnienia danych sygnalisty). Zgoda musi

spełniać wymagania RODO, a więc być dobrowolnym, konkretnym, świadomym i jednoznacznym okazaniem woli, jak również kryteria wskazane w art. 8 ust. 1 ustawy o ochronie sygnalistów, tj. musi być wyraźna.

Przypomniano, że zgodnie z art. 7 ust. 3 RODO wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem, o czym sygnalistę należy poinformować.

Prelegenci podkreślili, że sygnalista musi też zostać poinformowany co się wydarzy, gdy jego tożsamość zostanie ujawniona.

Jeśli chodzi o osoby, których dotyczą dane podawane w zgłoszeniu sygnalisty (np. sprawcy, tj. osoby, której dotyczy zgłoszenie) i obowiązków informacyjnych z art. 14 RODO, należy pamiętać o wyłączeniu z art. 14 ust. 5 lit. b) RODO, a nie tylko o wyłączeniu wynikającym bezpośrednio
z ustawy z 14 czerwca 2024 o ochronie sygnalistów.

Przepisy ustawy nie uwzględniły jak wyłączyć obowiązek w przypadku przekazania kopii danych,
by nie przekazywać informacji o sygnaliście, świadku i wszystkich, których prawa mogłyby na tym ucierpieć. W związku z tym zasadne wydaje się być zastosowanie art. 15 ust. 4 RODO, by w efekcie nie uwzględniać w kopii takich danych, których ujawnienie mogłoby niekorzystnie wpłynąć na prawa i wolności innych (tu: głównie sygnalisty).

Przetwarzać dane osobowe sygnalisty (oraz innych osób wskazanych w art. 27 ustawy) wewnątrz organizacji (podmiotu prawnego) mogą wyłącznie osoby wskazane w art. 27 ust. 1 ustawy, tj. zajmujące się przyjmowaniem zgłoszeń i prowadzeniem działań następczych. Nie wyklucza to outsourcingu, ale wyłącznie w zakresie wskazanym w art. 28 ust. 1 ustawy.

Jak zostało wskazane w ustawie: upoważnienie podmiotu zewnętrznego (o którym mowa w art. 25 ust. 1 pkt 1), wymaga zawarcia umowy w celu powierzenia obsługi przyjmowania

zgłoszeń wewnętrznych, potwierdzania przyjęcia zgłoszenia, przekazywania informacji zwrotnej oraz dostarczania informacji na temat procedury zgłoszeń wewnętrznych z zastosowaniem rozwiązań technicznych i organizacyjnych zapewniających zgodność tych czynności z ustawą.

Jednocześnie należy zwrócić uwagę, że art. 27 ust. 2 ustawy nie może być rozumiany w ten sposób, że jedyną przesłanką legalnego dostępu i przetwarzania danych tam wskazanych jest tylko formalne nadanie upoważnienia (o którym mowa w treści art. 27 ust. 2 ustawy).

Nadanie upoważnienia, o którym mowa w art. 27 ust. 2 ustawy jest tylko formalnym potwierdzeniem tego, że wskazane osoby (zgodnie z postanowieniami procedury zgłoszeń wewnętrznych) są uprawnione do dostępu do danych osobowych (i w konsekwencji ich przetwarzania). Przepis art. 27 ust. 2 ustawy, który dotyczy zgłoszeń wewnętrznych należy czytać w kontekście art. 25 ust. 1 ustawy, który wymienia obligatoryjne elementy procedury zgłoszeń wewnętrznych m.in. wymaga wskazania, kto będzie uprawniony do przyjmowania zgłoszeń i prowadzenia działań następczych. Należy go interpretować także zgodnie z art. 16 ust. 1 dyrektywy o ochronie sygnalistów, który wskazuje, że tożsamość osoby dokonującej zgłoszenia nie może zostać 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.

Upoważnienie powinno być szczegółowe, tj. na tyle, aby wyłączyć możliwe wątpliwości co do jego zakresu. Musi wskazywać do wykonywania jakich czynności na danych osobowych upoważnia daną osobę.

Wskazano również na brak kompleksowej regulacji ustawy. Podkreślono, by nie ograniczać się do samej ustawy o sygnalistach. Niezbędne jest korzystanie również z RODO, przy równoczesnym zachowaniu ostrożności w tym aspekcie.

Każdy przypadek trzeba będzie oceniać indywidualnie – które informacje przekazać, a które

nie. Jest to kwestia oceny i należy tu również wziąć pod uwagę zasadę rozliczalności.

Procedura przyjmowania zgłoszeń wewnętrznych i prowadzenia postępowań wyjaśniających

W drugim panelu uczestnicy seminarium omawiali procedury przyjmowania zgłoszeń wewnętrznych i prowadzenia postępowań wyjaśniających z perspektywy zasad przetwarzania danych osobowych.

Wiele pytań, które wpłynęły do Społecznego Zespołu Ekspertów oraz UODO dotyczyło możliwości zgłoszeń anonimowych oraz sposobów przekazywania zgłoszeń (kontrowersje wzbudziło ustne zgłaszanie naruszeń).

Poruszono również zagadnienie tzw. „fałszywego sygnalisty" – dopiero na zaawansowanym etapie postępowania można stwierdzić, czy sygnalista mieści się w ustawowych ramach definicji. Należy ostrożnie podchodzić do stwierdzenia, że ktoś nie jest sygnalistą.

Dużą część dyskusji poświęcono grupom kapitałowym w kontekście sygnalistów, kanałów zgłoszeń i tego, jak powinno wyglądać zgłoszenie. W kontekście kanałów zgłoszeń rozważano różne możliwości ich wdrażania przez grupy kapitałowe z perspektywy praktycznej oraz zgodności z prawem. Przede wszystkim zwrócono uwagę na ryzyko, jakie niesie za sobą pozostawienie jedynie kanałów korporacyjnych. Eksperci podkreślili, że ustawa – w art. 28 – posługuje się różnymi pojęciami „wspólnych zasad" czy „wspólnych procedur". Jak zauważyli prelegenci, są to pojęcia odmienne od tych użytych w dyrektywie, gdzie jest mowa np. o możliwości łączenia zasobów w przypadku niektórych kategorii podmiotów. Ustawa krajowa nie mówi o łączeniu zasobów co do przyjmowania zgłoszeń i ich rozpatrywania. Jednocześnie zaznaczono, że nie wyklucza to oczywiście powierzenia czynności np. jednej ze spółek w grupie na ogólnych zasadach wynikających z art. 28 ust. 1 ustawy.

UODO interesowały również grupy kapitałowe o zasięgu międzynarodowym, rozmówcy zastanawiali się, co robić w sytuacji, gdy grupa kapitałowa jest tak skonstruowana, że

występuje w niej relacja „spółka-matka”. Próba zmierzenia się z wyzwaniem, jakie działania podjąć w danej sytuacji nie była łatwa, padły różne propozycje reakcji ze strony prelegentów.

Przede wszystkim zwrócono uwagę, że „spółka matka” może występować w roli podmiotu, któremu powierzono czynność na podstawie art. 28 ust. 1 ustawy (i w zakresie tam wskazanym), ale jeżeli spółka matka (poza RP) przyjmuje zgłoszenia do własnych celów, to nie jest to przypadek regulowany ustawą o ochronie sygnalistów (nie wyklucza to oczywiście, że wejdą wtedy w grę przepisy krajowe innego państwa członkowskiego UE).

Zastanawiano się jak podmiot ma realizować ustawę, gdy zadania są przekazywane na zewnątrz – czy podmiot któremu organizacja zdecydowała się powierzyć outsourcing daje gwarancję ochrony danych osobowych i ochrony sygnalisty. W przypadku outsourcingu wewnątrz grupy podmiotów (np. do spółki „matki”) należy uwzględnić ryzyka związane np. z nieuprawnionym dostępem do danych.

Dokonano próby rozróżnienia pojęcia zasady od procedury. Przypomniano, że procedury należy przyjmować w sposób przyjęty w danej strukturze, a wraz z rozpoczęciem rekrutacji muszą być one dostępne dla kandydatów w ustalonej przez daną organizację formie.

Poinstruowano słuchaczy jak powinno wyglądać modelowe upoważnienie do procesów przetwarzania danych. Dyskutowano, jaki jest minimalny zakres upoważnienia, by spełniało wymogi prawne. Ustalono, że powinno zawierać informacje, kto upoważnia, kogo, do czego – jakich konkretnie czynności.

Podkreślono, że podczas konsultacji społecznych, często pojawiały się pytania o zgłoszenia anonimowe. Jak ustalono, przyjęcie zgłoszeń anonimowych zależeć będzie w dużej mierze od kultury organizacji. Podmioty, które się na to zdecydują, będą musiały wziąć pod uwagę konsekwencje tej decyzji, równocześnie pamiętając, że anonimowość może być pozorna.

Prelegenci zastanawiali się nad słusznością zgłoszeń telefonicznych – wyrażenie zgody na

transkrypcję, utrwalenie zgłoszenia zdaje się być w przepisach. Powinno się jednak zgłaszającego powiadomić, że rozmowa jest nagrywana. Zdaniem prowadzących panel, zgoda może być wyrażona także poprzez wolę kontynuacji rozmowy. Eksperci zastanawiali się, czy jest to zgoda w rozumieniu art. 7 RODO (pojęcie „zgody" pojawiło się w art. 26 ust. 3 ustawy o ochronie sygnalistów). Większość uczestników spotkania przyjęło, że nie jest to zgoda w rozumieniu RODO.

Jak ustalili specjaliści, więcej argumentów przemawia za tym, że – wskazana w ustawie zgoda dotycząca sposobu dokumentowania rozmowy z sygnalistą (art. 26 ust. 3 ustawy o ochronie sygnalistów) nie jest zgodą w rozumieniu RODO.

Zgłoszenia zewnętrzne

Panel trzeci dał możliwość uzyskania informacji, w jaki sposób Biuro Rzecznika Praw Obywatelskich przygotowuje się do wejścia w życie ustawy o sygnalistach. Bowiem polski ustawodawca właśnie RPO powierzył rolę centralnego organu wspierającego sygnalistów w korzystaniu z przysługujących im praw.

Jak zauważył przedstawiciel Biura RPO dyr. Marcin Malecko, nowo powstający w Biurze Rzecznika Praw Obywatelskich Zespół ds. Sygnalistów wciąż ma więcej pytań niż gotowych odpowiedzi Wyzwaniem dla BRPO jest zorganizowanie systemu zgłoszeń zewnętrznych i odseparowanie
go od systemu zgłoszeń wewnętrznych.

Słuchacze mogli się dowiedzieć, że prawdopodobnie powstanie elektroniczny formularz zgłoszeniowy na odrębnej stronie niż BRPO. W założeniu ma być prosty w obsłudze oraz wymagać jedynie niezbędnych danych do procedowania zgłoszenia.

Zakres pozyskiwanych danych – np. tych, które będzie musiał wpisać sygnalista, wypełniając formularz online do dokonywania zgłoszeń – musi być zgodny z zasadą minimalizacji (art. 5 ust. 1 lit. c) RODO) oraz skorelowany z treścią procedury zgłoszeń wewnętrznych i decyzją

podmiotu prawnego co do przyjmowania zgłoszeń anonimowych (m.in. art. 25 ust. 1 pkt 4 ustawy wymaga, aby procedura zgłoszeń wewnętrznych określała m.in. tryb postępowania z informacjami
o naruszeniach prawa zgłoszonymi anonimowo).

Podobnie treść klauzuli informacyjnej w rozumieniu art. 13-14 RODO musi uwzględniać tę kwestię, tj. m.in. trzeba wyraźnie wskazać czy podanie danych jest dobrowolne czy nie (uwzględniając decyzję co do zgłoszeń anonimowych).

Ustawa nakłada na BRPO obowiązek upowszechniania informacji na temat uprawnień sygnalistów i ich roli w społeczeństwie. Niestety nie definiuje jak tę funkcję poradniczą, edukacyjną Rzecznik ma pełnić. Na razie RPO zastanawia się nad utworzeniem dwóch infolinii – jednej czysto poradniczej, drugiej do zgłaszania sygnałów przez sygnalistów.

Wciąż nie wiadomo jak wyglądać będzie weryfikacja zgłoszeń zewnętrznych – do jakiego stopnia dopuścić weryfikację i w jaki sposób ją przeprowadzić.

Poruszono problem zgłaszania naruszeń przez „nie sygnalistów” – wydaje się, że właściwą praktyką jest przyjmowanie zgłoszeń również przez osoby, które nie wpisują się w definicję sygnalisty, a więc nie mają związku z zatrudnieniem.

Dyskutanci zastanawiali się, czy można takiego zgłoszenia nie przyjąć. Szczególnie, że gdy zgłoszenie jest anonimowe mogą wystąpić trudności w ustaleniu, czy osoba zgłaszająca ma jakieś konotacje z zatrudnieniem, a więc jest sygnalistą w rozumieniu ustawy. Pojawiła się wątpliwość, czy takiej osobie przysługuje ochrona i – jeśli tak – w jaki sposób ją zapewnić.

Zastanawiano się, czy sygnalistą może być aktywista, obserwator, któremu na sercu leży dobro publiczne, ale nie ma powiązania z zatrudnieniem.

Zabezpieczenia techniczne i organizacyjne

W ostatnim panelu dyskutowano o bezpieczeństwie wybranych kanałów zgłaszania naruszeń

poprzez zapewnienie odpowiednich zabezpieczeń technicznych i organizacyjnych.

Podkreślono konieczność uwzględnienia, w projektowanych procesach przetwarzania danych, ochrony danych osobowych zgodnie z zasadami privacy by design i privacy by default – przy równoczesnym zadbaniu o integralność i dostępność danych oraz przy zachowaniu ich poufności.

W ramach oceny ryzyka należy uwzględnić m.in. scenariusze związane z nieuprawnionym dostępem do danych sygnalisty i innych osób (wewnątrz organizacji przyjmującej zgłoszenia), co jest szczególnie istotne z perspektywy treści art. 27 ustawy oraz ryzyk dotyczących działań odwetowych.

Zauważono, że komunikacja musi być zaszyfrowana zarówno w transporcie, jak i w procesie składowania informacji. Zaproponowano metody zapobiegania email spoofingu. Rozmawiano o bezpieczeństwie przekazywania zgłoszeń do podmiotu prawnego.

Zastanawiano się nad potrzebą wysyłania zaszyfrowanych maili – choć szyfrowanie zwiększa bezpieczeństwo, może być uznane dla zgłaszających za rozwiązanie zbyt trudne, przez co będą oni rezygnować z wysyłania zgłoszeń.

Dyskutowano o tym, jakie trudności rodzą platformy zgłoszeniowe. Eksperci wskazali, że zanim się na platformę zdecydujemy, należy ją odpowiednio zabezpieczyć, zaszyfrować, zweryfikować zgodnie z RODO, zmierzyć i ocenić.

Prelegenci szukali odpowiedzi na pytanie, jak zadbać o poufność danych, również w kontekście monitoringu stacji roboczej pracowników przyjmujących zgłoszenia.

Zwrócono uwagę na zasadę integralności danych – komunikat wysłany przez system informatyczny, gdy jest źle zabezpieczony, istnieje ryzyko, że zostanie zmieniony przez osobę trzecią.

Ryzyka naruszenia praw lub wolności osób, których dane będą przetwarzane w procesie

obsługi zgłoszeń sygnalistów należy rozważać m.in. w kontekście przyjętej przez podmiot prawny procedury zgłoszeń wewnętrznych (odpowiednio dotyczy to zgłoszeń zewnętrznych), a w szczególności w powiązaniu z kanałami komunikacyjnymi przyjęcia zgłoszenia oraz aktywami wspierającymi ten proces – środkami przetwarzania, takimi jak: systemy, sprzęt, aplikacje, personel i inne zasoby.

W trakcie oceny ryzyka należy szczególną uwagę zwrócić na to, kto z personelu organizacji będzie miał (nawet potencjalny) dostęp do danego środka przetwarzania (komputery, serwery, sieci, aplikacje, praformy, pomieszczenie do przyjmowania zgłoszeń ustnych itd.).

Przepisy ustawy zwracają szczególną uwagę na zapobieganie działaniom odwetowym, dlatego w ocenie ryzyka i doborze środków należy przeanalizować, komu z wewnątrz organizacji może zależeć na uzyskaniu dostępu do treści zgłoszeń naruszeń prawa czy poznaniu tożsamości sygnalistów (czy też innych osób).

Podsumowanie – na co organizacja musi zwrócić uwagę, wdrażając przepisy ustawy o sygnalistach

- Przed przystąpieniem do wdrożenia ustawy, organizacja musi ustalić jakimi kanałami będzie przyjmować zgłoszenia (elektronicznie, telefonicznie, czy dopuszczalne są anonimowe zgłoszenia i czym to będzie skutkowało w ocenie ryzyka formularza).

- Powinna podjąć decyzję, kto będzie przyjmował zgłoszenia i prowadził działania następcze. Mogą to robić wyłącznie osoby bezstronne. W tym kontekście pojawił się również temat outsourcingu –
że zakres dopuszczalnego outsourcingu wynika z art.28 ust.1 ustawy o ochronie sygnalistów w powiązaniu w zakresie przetwarzania danych osobowych z RODO.

- Musi przeprowadzić ocenę ryzyka naruszenia praw lub wolności osób fizycznych (z art. 25 RODO
i 32 RODO) już w fazie projektowania procesu przyjmowania zgłoszeń sygnalistów

uwzględniając także wymagania dotyczące oceny skutków (art. 35 RODO).

• Organizacja powinna również zastanowić się, jak będzie spełniać obowiązki informacyjne – należy je wypełniać warstwowo.

• Jeśli chodzi o informowanie o procedurze kandydatów do pracy, kontrahentów – tu istnieje możliwość spełnienia wprost obowiązku informacyjnego, jak i przekierowania do właściwych dokumentów.

• Klauzule informacyjne muszą być dostosowane w szczególności w zakresie informowania o obowiązku lub też dobrowolności podania danych przez sygnalistę.

• Ustawa o ochronie sygnalistów nie wymaga podania danych do kontaktu przez sygnalistę. Należy to zsynchronizować z kwestią zakresu tych danych, w zależności od tego, czy organizacja dopuści anonimowe zgłoszenia czy też nie.

• Bardzo ważne jest uwzględnienie kwestii powierzenia przekazania danych oraz weryfikacji nadawanych upoważnień.

• Organizacja musi też ustalić jak zarządzać usuwaniem danych i dokonać aktualizacji rejestru czynności, w zależności od typu i zakresu pozyskiwanych danych.

• Niezbędne jest, by wskazała podstawę do przetwarzania danych.

• Musi również uwzględnić konieczność aktualizacji rejestru czynności o nowy proces przetwarzania danych (w tym kontekście warto wspomnieć o tym, że w procesie szeroko pojętej obsługi zgłoszeń sygnalistów pojawiają się różne kategorie osób, których dane są przetwarzane

m.in. sygnalista, osoba, której dotyczy zgłoszenie, świadek, osoba powiązana z sygnalistą).

Co dalej?

Prezes UODO podkreślił, że przepisy tej ustawy budzą liczne wątpliwości. Rolą Urzędu jest nadzór nad przestrzeganiem tej ustawy. Na ile przepisy wymagają dalszych sugestii zmian, pokaże praktyka.

W następstwie dyskusji seminaryjnej na stronie UODO systematycznie będą pojawiać się pisemne wyjaśnienia UODO podpowiadające właściwe kierunki interpretacji przepisów ustawy o sygnalistach w zakresie dotyczącym danych osobowych.

W związku z tym, że bardzo dużo pytań dotyczyło roli kancelarii prawnych w kontekście outsourcingu czynności zgłoszeń sygnalistów Mirosław Wróblewski, prezes UODO, zapowiedział, że zwróci się do samorządów radców prawnych i adwokatów o spotkanie w celu omówienia roli kancelarii prawnych we wspieraniu klientów, biorąc pod uwagę możliwość zawarcia z nimi umowy powierzenia przyjmowania zgłoszeń wewnętrznych w rozumieniu art. 28 ust. 1 ustawy o ochronie sygnalistów.