Jak chronić dane osobowe sygnalisty

AUTOR: KAROLINA MISIAK*

Za chwilę zaczną obowiązywać przepisy zawarte w ustawie o ochronie sygnalistów. Organizacje, firmy i instytucje miały wiele czasu na przygotowanie się do wejścia ich w życie, gdyż prace nad kolejnymi projektami ustaw ciągnęły się kilka lat. Szczególnie ważną kwestią jest zapewnienie ochrony danych zarówno sygnalisty, jak i osoby, której zgłoszenie dotyczy. W artykule skupiamy się na tym, jak zorganizować cały proces, aby chronić tożsamość zgłaszającego i jego dane.

Ustawa z 14 czerwca 2024 r. o ochronie sygnalistów została opublikowana w Dzienniku Ustaw 25 czerwca 2024 r. Ma wejść w życie po upływie 3 miesięcy od dnia ogłoszenia, tj. 25 września 2024 r., z wyjątkiem wybranych przepisów (dotyczących zgłoszeń zewnętrznych) – te wejdą w życie 25 grudnia. Jednak aby spełnić wymogi ustawowe już teraz trzeba mieć gotową procedurę zgłoszeń wewnętrznych. Ponadto jeżeli w organizacji nie działają związki zawodowe, to powinni już być wybrani przedstawiciele, z którymi podmioty prawne są zobowiązane procedurę skonsultować.

Osoby wyznaczone do przyjmowania i weryfikacji zgłoszeń oraz podejmowania działań następczych muszą posiadać pisemne upoważnienie podmiotu prawnego i być zobowiązane do zachowania w tajemnicy informacji i danych osobowych, które uzyskały.

Podmioty zobowiązane

Obowiązek przygotowania procedur zgłoszeń wewnętrznych mają podmioty, na rzecz których wykonuje pracę zarobkową co najmniej 50 osób (nie chodzi tylko o pracowników w rozumieniu kodeksu pracy, ale także osoby współpracujące na podstawie umowy zlecenia czy kontraktu b2b) oraz wszystkie podmioty (bez względu na liczbę osób) wykonujące działalność w określonym zakresie (m.in. usługi finansowe czy ochrona środowiska). Przed nimi stoi nie lada wyzwanie – wdrożenie skutecznego systemu ochrony sygnalistów. Skutecznego, a więc zapewniającego poufność, co nieodłącznie wiąże się z koniecznością ochrony danych osobowych.

Co stanowi ustawa?

W ustawie problemowi przetwarzania danych osobowych sygnalisty poświęcono jeden artykuł. Regulacja jest lakoniczna i daleka od doskonałej. W art. 8 ust. 4 wskazano, że „podmiot prawny albo organ publiczny po otrzymaniu zgłoszenia przetwarza dane osobowe w zakresie niezbędnym do przyjęcia zgłoszenia lub

podjęcia ewentualnego działania następczego. Dane osobowe, które nie mają znaczenia dla rozpatrywania zgłoszenia, nie są zbierane, a w razie przypadkowego zebrania są niezwłocznie usuwane. Usunięcie tych danych osobowych następuje w terminie 14 dni od chwili ustalenia, że nie mają one znaczenia dla sprawy". Administratorem danych osobowych jest zatem podmiot prawny, czyli organizacja, która otrzymała zgłoszenie. Podmiot

Podmiot prawny albo organ publiczny po otrzymaniu zgłoszenia przetwarza dane osobowe w zakresie niezbędnym do przyjęcia zgłoszenia lub podjęcia działania następczego. Dane osobowe, które nie mają znaczenia dla rozpatrywania zgłoszenia, nie są zbierane, a w razie przypadkowego zebrania są niezwłocznie usuwane. Usunięcie tych danych następuje w terminie 14 dni od chwili ustalenia, że nie mają znaczenia dla sprawy.

ten będzie miał status administratora danych osobowych sygnalisty, ale też innych danych osobowych pozyskanych w związku z przyjmowaniem i weryfikacją zgłoszeń. Należy bowiem pamiętać, że w związku z dokonaniem zgłoszenia będą przetwarzane nie tylko dane sygnalisty, ale także osoby, której dotyczy zgłoszenie, czy osób trzecich wskazanych w zgłoszeniu, np. świadków naruszenia.

Ustawa wprost nie wskazuje na ochronę innych osób, należy zatem na to zagadnienie patrzeć szerzej, tj. z uwzględnieniem Dyrektywy (UE) 2019/1937 w sprawie ochrony osób zgłaszających naruszenia prawa UE oraz przepisów RODO (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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). Jak czytamy w motywie 85 dyrektywy: „skuteczna ochrona poufności tożsamości osób dokonujących zgłoszenia jest równie konieczna w celu ochrony praw i wolności innych osób […]. Państwa członkowskie powinny zapewnić skuteczność niniejszej dyrektywy, w tym w stosownych przypadkach poprzez ograniczenie – w drodze aktów prawnych – wykonywania niektórych praw do ochrony danych osobowych osób, których dotyczy zgłoszenie […], w zakresie w jakim i o ile jest to konieczne, by zapobiec i zaradzić próbom utrudniania dokonywania zgłoszeń lub utrudniania, udaremniania lub spowalniania działań następczych, w szczególności postępowań wyjaśniających, lub próbom ustalenia tożsamości osób dokonujących zgłoszenia". Istotnym przepisem na gruncie polskiej ustawy jest art. 8 ust. 5 i 6, który daje podstawę do nieinformowania tych osób, kto przekazał ich dane w ramach zgłoszenia. Innymi słowy, przepisy mają na celu zachowanie w tym aspekcie poufności sygnalisty (zatem ustawa wyłącza obowiązek informowania, jak określa to RODO, o „źródle danych"), chyba że sygnalista wyrazi zgodę na ujawnienie jego danych.

Przy okazji warto wspomnieć, że wykonanie klauzuli informacyjnej czy prawa dostępu do danych w stosunku do tych osób w pozostałym wymaganym przez RODO zakresie

jest konieczne. Realizacja praw osób, których dane dotyczą, ale także praw osób, których dotyczy zgłoszenie, musi odbywać się z poszanowaniem obowiązków wynikających z RODO. W związku z tym administrator musi zapewnić, aby system sygnalny dawał możliwość zrealizowania tych praw.

Co możemy zrobić?

1. Kompleksowa procedura zgłoszeń wewnętrznych

Przyjmujący zgłoszenia, jako administrator danych osobowych, musi wdrożyć odpowiednie środki bezpieczeństwa danych sygnalisty. Zasadne jest przyjęcie takich rozwiązań także w procedurze zgłoszeń wewnętrznych. Wybór konkretnych środków, adekwatnych do poziomu ryzyka przetwarzania danych, należy do administratora. Powinien być poprzedzony i mieć swoje oparcie w uprzednio przeprowadzonej analizie ryzyka. Kanały przyjmowania zgłoszeń powinny być zaprojektowane, ustanowione i obsługiwane w bezpieczny sposób zapewniający ochronę poufności tożsamości osoby dokonującej zgłoszenia i osoby trzeciej wymienionej w zgłoszeniu oraz uniemożliwiający uzyskanie do nich dostępu osobom nieupoważnionym.

2. Starannie dobrane osoby bądź podmioty przyjmujące zgłoszenia

Osoby wyznaczone do przyjmowania i weryfikacji zgłoszeń oraz podejmowania działań następczych muszą posiadać pisemne upoważnienie podmiotu prawnego i być zobowiązane do zachowania w tajemnicy informacji i danych osobowych, które uzyskały w ramach przyjmowania i weryfikacji zgłoszeń wewnętrznych oraz podejmowanych działań następczych. Osoby wyznaczone do przyjmowania i rozpatrywania zgłoszeń powinny być bezstronne oraz odpowiednio przeszkolone, m.in. w kwestii ochrony danych.

Z kolei w przypadku powierzenia przyjmowania zgłoszeń podmiotom zewnętrznym, np. gdy administrator danych osobowych chce skorzystać z systemu informatycznego do obsługi zgłoszeń dostawcy zewnętrznego, powinien w pierwszej kolejności dokonać weryfikacji takiego podmiotu oraz zawrzeć z nim umowę o powierzenie przetwarzania danych. Upoważnienie podmiotu zewnętrznego 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.

Szkolenia sprawdzą się przy wdrażaniu całego systemu ochrony sygnalistów. Powinny odbyć się nie tylko przed uruchomieniem procedury zgłoszeń wewnętrznych, ale także w trakcie jej stosowania, co przyczyni się do uzyskania przez pracodawcę wiedzy o zdarzeniach, które mogą mieć znaczenie dla bezpiecznego i prawidłowego funkcjonowania organizacji.

Taka umowa powinna również określać szczegółowe prawa i obowiązki podmiotu zewnętrznego związane z przetwarzaniem danych osobowych, o których mowa w szczególności w art. 28 ust. 3 RODO. Ustanawia on wymogi prawidłowego powierzenia przetwarzania danych osobowych, w tym obowiązek dochо-

wania odpowiedniej formy powierzenia przetwarzania danych osobowych, czyli umowy.

3. Rejestr zgłoszeń wewnętrznych z danymi osobowymi

Warto wskazać, że przyjmujący zgłoszenie jako administrator będzie musiał prowadzić rejestr zgłoszeń wewnętrznych. Ewidencja musi zawierać:

- numer zgłoszenia;
- przedmiot naruszenia;
- dane osobowe sygnalisty oraz osoby, której dotyczy zgłoszenie, niezbędne do identyfikacji tych osób;
- adres do kontaktu sygnalisty;
- datę dokonania zgłoszenia;
- informację o podjętych działaniach następczych;
- datę zakończenia sprawy.

Jest to wymóg wynikający z ustawy. Podmiot musi rejestr prowadzić w dowolnej formie, co oznacza, że dopuszczalna jest zarówno forma pisemna, jak i elektroniczna. W zakresie danych osobowych należy mieć jednak na uwadze, że jednym z elementów obligatoryjnych, które rejestr musi zawierać, są dane sygnalisty oraz osoby, której zgłoszenie dotyczy, dlatego tak istotne jest zadbanie o ich bezpieczne przetwarzanie.

Należy pamiętać, aby dostęp do rejestru miały tylko powołane do tego osoby, legitymujące się stosownym upoważnieniem. W zależności od formy jego prowadzenia, należy rozważyć bezpieczne przechowywanie wersji papierowych czy to w zamkniętych szafach, czy w pomieszczeniach do tego przeznaczonych zamykanych na klucz. W przypadku wersji elektronicznych należy zadbać o stosowne szyfrowanie, kody zabezpieczeń z dostępem tylko dla osób upoważnionych. To wszystko jest bardzo istotne przede wszystkim z uwagi na konieczność zachowania poufności. Niezbędne będzie więc zadbanie o szkolenie pracowników.

Warto zauważyć, że szkolenia sprawdzą się przy wdrażaniu całego systemu ochrony sygnalistów. Powinny odbyć się nie tylko przed uruchomieniem procedury zgłoszeń wewnętrznych, ale także w trakcie jej stosowania, co powinno przyczynić się do jej faktycznego obowiązywania i do uzyskania przez pracodawcę wiedzy o zdarzeniach, które mogą mieć znaczenie dla bezpiecznego i prawidłowego funkcjonowania.

W przypadku powierzenia przyjmowania zgłoszeń podmiotom zewnętrznym, np. gdy administrator danych osobowych chce skorzystać z systemu informatycznego do obsługi zgłoszeń dostawcy zewnętrznego, powinien w pierwszej kolejności dokonać weryfikacji takiego podmiotu oraz zawrzeć z nim umowę o powierzenie przetwarzania danych.

Okres retencji danych

Dane w rejestrze powinny być przechowywane przez 3 lata, licząc od zakończenia roku kalendarzowego, w którym sfinalizowano działania następcze lub od zakończenia postępowań zainicjowanych tymi działaniami. Dane osobowe, które nie mają znaczenia dla rozpatrywania zgłoszenia, nie są zbierane, a w razie przypadkowego zebrania są niezwłocznie usuwane. Usunięcie tych danych osobowych następuje w terminie 14 dni od chwili ustalenia, że nie mają znaczenia dla sprawy. ■

**radca prawny w kancelarii Ostrowski i Wspólnicy sp.k. z Torunia, ostrowski.legal*

ZARZĄDZANIE KADRY PŁACE

PRACOWNIK SAMORZĄDOWY

9/2024
ROK XIV (165)
PRENUMERATA:
WWW.WSPOLNOTA.ORG.PL/KSIEGARNIA
ISSN 2082-6346

NA CO WPŁYWA PODWYŻKA WYNAGRODZENIA Z MOCĄ WSTECZNĄ

DODATEK MOTYWACYJNY DLA NAUCZYCIELI

KIEDY ŚWIADCZENIA Z ZFŚS SĄ ZWOLNIONE ZE SKŁADEK I PODATKU?