Grant Thornton

Ochrona danych osobowych w kontekście ustawy o ochronie sygnalistów

Webinar, 5 września 2024 r.

Łukasz Jarecki, Emilia Martynowicz-Mamajek

Agenda

1 Obowiązki podmiotu prawnego
2 Kategorie podmiotów danych oraz zakres danych osobowych
3 Okres przetwarzania danych osobowych
4 Podstawa prawna przetwarzania danych osobowych
5 Wyłączenie obowiązku przekazania informacji dotyczących źródła pozyskania danych
6 Obowiązek zapewnienia ochrony poufności tożsamości sygnalisty
7 Podmioty obsługujące zgłoszenia sygnalistów
8 Analiza ryzyka i DPIA
9 Wątpliwości na tle ustawy o ochronie sygnalistów

Obowiązki podmiotu prawnego

- Po upływie 3 miesięcy od dnia ogłoszenia ustawy podmiot prawny – bez względu na to, czy działa w sektorze publicznym czy prywatnym – zatrudniający co najmniej 50 osób (z pewnymi wyjątkami) będzie zobowiązany do:

ustalenia **wewnętrznych procedur** dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych

określenia i wdrożenia **kanałów przekazywania zgłoszeń wewnętrznych** przez sygnalistę (powinny obejmować co najmniej możliwość dokonywania zgłoszeń ustnie lub pisemnie)

prowadzenia **rejestru zgłoszeń wewnętrznych**

- Każdy, kto wbrew przepisom polskiej ustawy nie ustanowi procedury zgłoszeń wewnętrznych lub ustanowi ją z istotnym naruszeń wynikających z ustawy wymogów, będzie podlegał grzywnie.
- Kto wbrew przepisom ustawy ujawnia tożsamość sygnalisty, osoby pomagającej w dokonaniu zgłoszenia lub osoby powiązanej z sygnalistą, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Kategorie podmiotów danych oraz zakres danych osobowych

- W ramach sposobów, za pośrednictwem których sygnaliści będą dokonywać zgłoszeń, przetwarzaniu mogą zostać poddane dane osobowe:

sygnalisty | **osoby, której dotyczy zgłoszenie** | **świadka** | **osoby pokrzywdzonej**

- **Dane osobowe, które mogą być przetwarzane:**
  - imię, nazwisko czy dane kontaktowe, ale także
  - szereg innych informacji, które zostaną wskazane w zgłoszeniu czy w ramach postępowania wyjaśniającego, może to obejmować również:
  - **dane dotyczące wyroków skazujących i czynów zabronionych** oraz
  - **szczególne kategorie danych osobowych**, w tym dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dotyczące zdrowia, seksualności lub orientacji seksualnej.

Podstawowe zasady przetwarzania danych

Z uwagi na konieczność zapewnienia sygnaliście odpowiedniej ochrony, **jego dane osobowe pozwalające na ustalenie jego tożsamości, nie będą podlegać ujawnieniu nieupoważnionym osobom**, chyba że sygnalista wyrazi na to wyraźną zgodę.

Podmiot prawny po otrzymaniu zgłoszenia będzie musiał przetwarzać dane osobowe **w zakresie niezbędnym do przyjęcia zgłoszenia lub podjęcia ewentualnego działania następczego**.

Okres przetwarzania danych osobowych

- Dane osobowe, które nie będą miały znaczenia dla rozpatrzenia zgłoszenia, nie będą mogły być zbierane, a w razie ich przypadkowego zebrania – powinny zostać niezwłocznie usunięte. **Usunięcie tych danych osobowych powinno nastąpić w terminie 14 dni od chwili ustalenia, że nie mają one znaczenia dla sprawy.**
- Dane osobowe przetwarzane w związku z przyjęciem zgłoszenia lub podjęciem działań następczych oraz dokumenty związane z tym zgłoszeniem będą musiały być **przechowywane przez podmiot prawny przez okres 3 lat po zakończeniu roku kalendarzowego, w którym zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami.**
- Prowadzenie rejestru zgłoszeń wewnętrznych, w ramach którego podmiot prawny będzie gromadził dane osobowe oraz pozostałe informacje **przez okres 3 lat po zakończeniu roku kalendarzowego, w którym zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami.**

Podstawa prawna przetwarzania danych osobowych

- Podmiot prawny który otrzyma zgłoszenie, na gruncie RODO wystąpi w roli **administratora** i będzie uprawniony do przetwarzania danych osobowych sygnalisty, jak i danych innych osób ujawnionych w zgłoszeniu czy w trakcie postępowania wyjaśniającego.
- **Podstawę takiego przetwarzania** będą stanowić odpowiednio:

art. 6 ust. 1 lit. c/e/f RODO

- w odniesieniu do **zwykłych danych osobowych**

art. 9 ust. 1 lit. g RODO

- w odniesieniu do **szczególnych kategorii danych osobowych**

art. 10 RODO

- w odniesieniu do **danych dotyczących wyroków skazujących i czynów zabronionych**

Wyłączenie obowiązku przekazania informacji dotyczących źródła pozyskania danych

- Z uwagi na specyfikę i zakres przedmiotowy ustawy, realizacja niektórych z praw podmiotów danych może powodować nieefektywność mechanizmów w nim przewidzianych. W szczególności dotyczy to **prawa do informacji o przetwarzaniu danych osobowych oraz prawa dostępu przysługujących osobie, której dane dotyczą**.
- Związana z tym jest realizacja przez podmiot prawny obowiązku przekazania osobie, której dotyczy zgłoszenie, informacji o źródle danych może wiązać się z ujawnieniem tożsamości samego sygnalisty.
- **W przypadku obu wskazanych praw przysługujących osobie, której dotyczy zgłoszenie – jak wynika z ustawy – wykluczony został obowiązek podania źródła danych**.

Obowiązek zapewnienia ochrony poufności tożsamości sygnalisty

- Podmiot prawny gwarantuje, że procedura zgłoszeń wewnętrznych oraz związane z przyjmowaniem zgłoszeń przetwarzanie danych osobowych **uniemożliwiają nieupoważnionym osobom uzyskanie dostępu do informacji objętych zgłoszeniem oraz zapewniają ochronę poufności tożsamości sygnalisty, osoby, której dotyczy zgłoszenie, oraz osoby trzeciej wskazanej w zgłoszeniu**. Ochrona poufności dotyczy informacji, na podstawie których można bezpośrednio lub pośrednio zidentyfikować tożsamość takich osób.

  - Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – **wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą**.
  - **Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania**. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

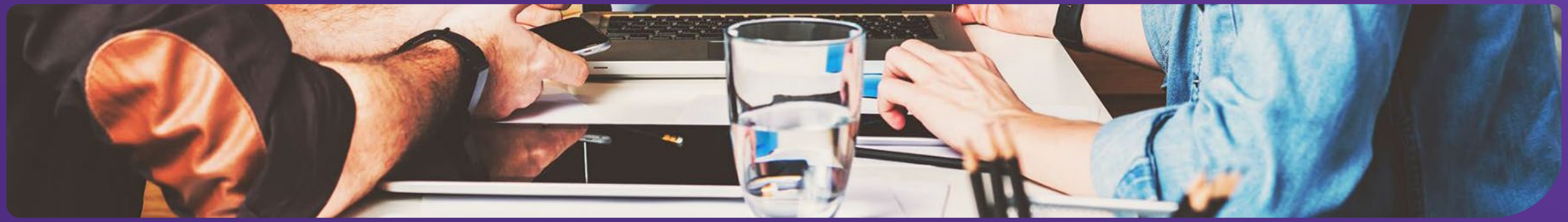
Podmioty obsługujące zgłoszenia sygnalistów

- Ustawa o ochronie sygnalisty wskazuje, iż przyjmowanie zgłoszeń wewnętrznych może być obsługiwane:

wewnętrznie przez wyznaczoną do tego celu osobę lub jednostkę organizacyjną

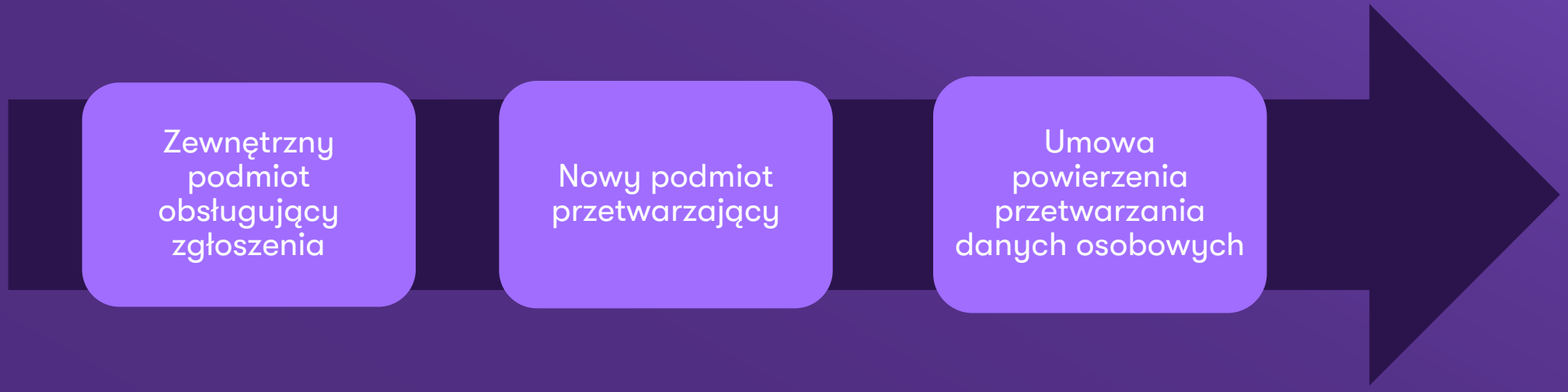
zewnętrznie przez osobę trzecią

- W każdym przypadku – na co wskazuje dyrektywa o sygnalistach, która nakłada na państwa członkowie obowiązek uchwalenia stosownych przepisów – podmiot obsługujący zgłoszenie, zapewniając **brak konfliktu interesów i niezależność**, jednocześnie powinien zagwarantować niezbędny poziom ochrony danych osobowych, o którym mowa w RODO.



Podmioty obsługujące zgłoszenia sygnalistów

- Do przyjmowania i weryfikacji zgłoszeń wewnętrznych, podejmowania działań następczych oraz przetwarzania danych osobowych mogą być dopuszczone **wyłącznie osoby posiadające pisemne upoważnienie podmiotu prawnego, zobowiązane do zachowania tajemnicy**. To dobry moment na dokonanie weryfikacji wewnętrznego procesu nadawania upoważnień do przetwarzania danych, czy też uprawnień do pracy w systemach informatycznych.
- W przypadku natomiast, gdy podmiot prawny zdecyduje się na skorzystanie z usług podmiotu zewnętrznego przy obsłudze zgłoszeń, to z punktu prawa ochrony danych osobowych pojawi się **nowy podmiot przetwarzający**, a zatem zasadne będzie **zawarcie umowy powierzenia danych osobowych do przetwarzania** na gruncie RODO.



Podmioty obsługujące zgłoszenia sygnalistów

- 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.
- Umowa określa szczegółowe prawa i obowiązki podmiotu zewnętrznego związane z przetwarzaniem danych osobowych zgodnie z art. 28 ust. 3 RODO.
- Zawarcie umowy **nie uchyla odpowiedzialności podmiotu prawnego za dochowanie obowiązków określonych w niniejszym rozdziale, w szczególności dotyczących zachowania poufności, udzielenia informacji zwrotnej oraz podjęcia działań następczych.**

Podmioty obsługujące zgłoszenia sygnalistów

- Podmioty prywatne, na rzecz których pracę zarobkową wykonuje co najmniej 50 (lecz nie więcej niż 249) osób, mogą na podstawie umowy ustalić **wspólne zasady dotyczące przyjmowania i weryfikacji zgłoszeń wewnętrznych oraz prowadzenia postępowań wyjaśniających**, pod warunkiem zapewnienia zgodności wykonywanych czynności z ustawą.

  - Podmioty te są **odrębnymi administratorami danych osobowych pozyskanych w związku z przyjmowaniem i weryfikacją zgłoszeń**. Administrator nie ma dostępu do danych osobowych pozyskanych przez innego administratora.
  - Nie ma to jednak zastosowania w przypadku, gdy w toku postępowania wyjaśniającego ustalono, że właściwy do przyjęcia zgłoszenia wewnętrznego lub obowiązany do podjęcia działań następczych jest inny administrator niż ten, do którego wpłynęło zgłoszenie, lub właściwych jest co najmniej dwóch administratorów. Administratorowi udostępnia się tylko te dane osobowe, które są niezbędne do podjęcia działań następczych.

- Podmioty prywatne należące do grupy kapitałowej w rozumieniu ustawy o ochronie konkurencji i konsumentów mogą ustalić **wspólną procedurę zgłoszeń wewnętrznych**, pod warunkiem zapewnienia zgodności wykonywanych czynności z ustawą

Analiza ryzyka i DPIA

- Podmiot prawny powinien również przeprowadzić **analizę ryzyka dla nowego procesu**, aby zidentyfikować potencjalne obszary narażone na naruszenia ochrony danych osobowych.

Kontekst przetwarzania danych osobowych

Identyfikacja zagrożeń i występujących podatności

Analiza i ocena następstw zmaterializowania się zagrożeń

Szacowanie poziomu ryzyka

- Zgodnie z komunikatem Prezesa Urzędu Ochrony Danych Osobowych systemy służące do zgłaszania nieprawidłowości (whistleblowing) zostały wskazane w **wykazie rodzajów operacji przetwarzania danych osobowych wymagających przeprowadzenia oceny skutków przetwarzania dla ich ochrony (DPIA)**. Oznacza to, że przed rozpoczęciem przetwarzania administrator powinien przeprowadzić DPIA.

Wątpliwości na tle ustawy o ochronie sygnalistów

- Możliwość przyjmowania przez podmioty prawne zgłoszeń dokonywanych anonimowo a dane osobowe ujawniane w rejestrze zgłoszeń wewnętrznych prowadzony przez podmiot prawny
- Dane osobowe umożliwiające identyfikację tożsamości sygnalisty
- Możliwość przetwarzania danych dot. wyroków skazujących
- Obowiązek informacyjny – dopuszczalność wstrzymania się z obowiązkiem informacyjnym wobec osoby, której dotyczy zgłoszenie sygnalisty
- Skorzystanie przez ustawodawcę z prawa do wprowadzania ograniczeń w celu zapewnienia poufności tożsamości sygnalisty
- Ujawnienie danych osobowych tylko, gdy zgłaszający wyrazi na to wyraźna zgodę
- Upoważnienie podmiotu zewnętrznego do przyjmowania zgłoszeń i umowa zawarta z pomiotem zewnętrznym
- Przetwarzanie danych w grupie kapitałowej – wspólna procedura dla grupy kapitałowej, dopuszczanie współadministrowania danymi

Skontaktuj się z nami!

Łukasz Jarecki
Associate, Prawnik
Zespół Ochrony Danych Osobowych
M +48 885 661 839
E lukasz.jarecki@pl.gt.com

Emilia Martynowicz-Mamajek
Junior Associate
Zespół Ochrony Danych Osobowych
M +48 667 778 891
E Emilia.Martynowicz-Mamajek@pl.gt.com

Ostatnio pisaliśmy o temacie przetwarzania danych osobowych w kontekście ustawy o ochronie sygnalistów w artykułach:

RODO a sygnaliści – ochrona danych zgłaszających naruszenia→

Jaka ochrona przysługuje sygnalistom w kontekście RODO? [INFORMATOR] →