Grant Thornton

RODO a dyrektywa o sygnalistach

Przykład planowania procesu przetwarzania

Purpurowy Informator

Listopad 2021

Purpurowy Informator - źródło cennych informacji

Z przyjemnością prezentujemy kolejną odsłonę „Purpurowego Informatora" – cyklu analiz, w którym omawiamy istotne i aktualne zagadnienia dla przedsiębiorców.

W bieżącym opracowaniu przedstawiamy **w jaki sposób przedsiębiorcy zobowiązani od 17 grudnia br. do ustanowienia wewnętrznych procedur zgłaszania naruszeń oraz ochrony sygnalistów powinni przygotować się do procesu przetwarzania danych**. Zwłaszcza, że – jak wskazuje dyrektywa o ochronie praw sygnalistów – katalog osób, od których pracodawca może otrzymać dane osobowe oraz które będzie musiał przetwarzać w związku ze zgłoszeniem naruszenia, jest bardzo szeroki.

Swoją wiedzą i doświadczeniem w tym wydaniu dzieli się **Kacper Rączkowiak, Starszy specjalista ds. ochrony danych osobowych**.

Zespół Outsourcingu Grant Thornton

Wstęp

Niniejszy informator jest poświęcony procesowi przetwarzania danych w kontekście wchodzącej za miesiąc w życie tzw. dyrektywy o sygnalistach.

Kacper Rączkowiak omawia w nim przykładowy plan projektowania procesu przetwarzania, wraz ze wszystkimi niezbędnymi krokami, tj.:

1. ustalenie podmiotu danych;
2. ustalenie podstawy przetwarzania danych;
3. ustalenie zakresu przetwarzania danych;
4. zabezpieczenie przetwarzania danych;
5. ustalenie okresu przechowywania danych;
6. ustalenie osób upoważnionych do przetwarzania;
7. ustalenie odbiorców danych spoza organizacji w ramach procesu przetwarzania.

Na początku jednak autor przypomina podstawowe i kluczowej informacje, takie jak:

- zakres nowych obowiązków pracodawców dotyczący ochrony sygnalistów,
- kogo i od kiedy będą dotyczyły najnowsze regulacje
- oraz kim jest sygnalista zgodnie z projektowanymi na polskim gruncie przepisami.

Bieżące opracowanie stanowi bardzo praktyczną „pigułkę informacyjną" w poruszanym zakresie.

Serdecznie zapraszamy do lektury!

Grant Thornton Polska

Nowe obowiązki pracodawców od 17 grudnia 2021/2023

Dyrektywa o ochronie praw sygnalistów (tj. Dyrektywa Parlamentu Europejskiego i Rady U 2019/1937 z 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii), wejdzie w życie 17 grudnia 2021 roku.

Wspomniana dyrektywa nakłada na wybrane grupy pracodawców (wyszczególnione na następnej stronie) obowiązek ustanowienia wewnętrznych procedur zgłaszania naruszeń (także w zakresie ich ewidencji i podejmowania działań następczych) w sposób anonimowy i bezpieczny oraz obowiązek ochrony sygnalistów.

Wymienione w projekcie grupy podmiotów mają zatem ok. miesiąca na uruchomienie nowego procesu, a to z kolei pociąga za sobą – zgodnie z art. 25 ustawy o RODO – obowiązek ochrony danych osobowych w fazie projektowania (tzw. Privacy by design). Zatem uruchamiając każdy kolejny/nowy proces przetwarzania unijny ustawodawca oczekuje od pracodawców uwzględnienia konieczności ochrony danych osobowych.

W niniejszym opracowaniu przybliżymy zatem w jaki sposób zobligowani do tego przedsiębiorcy mogą przygotować się do nowych obowiązków w zakresie planowania procesu przetwarzania dotyczącego zgłaszania naruszeń w firmach oraz ochrony sygnalistów.

Kto i od kiedy musi chronić sygnalistów?

Już od 17 grudnia 2021 roku następujące grupy podmiotów będą zobligowane do wprowadzenia u siebie rozwiązań służących zgłaszaniu nieprawidłowości i naruszeń prawa oraz ochronie sygnalistów (zależnie od ostatecznego kształtu krajowej ustawy, poniższe wyliczenie może ulec zmianie).

Należą do nich:

- podmioty zatrudniające co najmniej 50 osób w sektorze publicznym,
- podmioty zatrudniające co najmniej 250 osób w sektorze prywatnym,
- wykonujące działalność w zakresie usług, produktów i rynków finansowych oraz zapobiegania praniu pieniędzy i finansowania terroryzmu, bezpieczeństwa transportu i ochrony środowiska.

W przypadku podmiotów działających w sektorze prywatnym, zatrudniających od 50 do 249 pracowników realizacja wspomnianego powyżej obowiązku opóźni się o dwa lata i będzie wymagana prawem od 17 grudnia 2023 roku.

Podstawą nowych obowiązków ww. grup pracodawców będzie dyrektywa o sygnalistach oraz implementująca ją ustawa o ochronie osób zgłaszających naruszenia prawa, której projekt został już opublikowany w Rządowym Centrum Legislacji:

ZOBACZ PROJEKT

Nowe zadania dla pracodawców

Rządowy projekt dotyczący ochrony sygnalistów zakłada, że od 17 grudnia 2021/2023 roku pracodawcy będą zobowiązani do:

- ustalenia regulaminu zgłoszeń wewnętrznych, który wejdzie w życie po upływie 2 tygodni od dnia podania go do wiadomości pracowników w sposób przyjęty u danego pracodawcy;
- zapoznania nowych pracowników z treścią regulaminu zgłoszeń wewnętrznych przed dopuszczeniem ich do pracy;
- utworzenia i prowadzenia tzw. kanałów dokonywania zgłoszeń (kanały zgłoszeń powinny umożliwiać dokonywanie ich: na piśmie oraz przekazywanie zgłoszeń drogą pocztową, za pośrednictwem fizycznych skrzynek na skargi lub na platformie online, intra- lub internetowej, bądź dokonywanie zgłoszeń ustnie, za pośrednictwem gorącej linii lub innego systemu komunikacji głosowej);
- prowadzenia rejestru zgłoszeń wewnętrznych, w ramach którego pracodawca będzie gromadził dane, w tym dane osobowe, przez okres 5 lat od dnia przyjęcia zgłoszenia.

WAŻNE!

Każdy, kto wbrew przepisom polskiej ustawy nie ustanowi wewnętrznej procedury zgłaszania naruszeń prawa i nie podejmie działań następczych albo ustanowi procedurę, która narusza prawo, będzie ukarany grzywną, karą ograniczenia wolności albo karą pozbawienia wolności do lat 3.

Sygnalista, czyli kto?

Na gruncie projektu omawianej ustawy sygnalistą jest każda osoba zgłaszająca lub ujawniająca publicznie informacje na temat naruszeń, które uzyskała w związku z wykonywaną przez siebie pracą (bez względu na to, czy pracuje w sektorze publicznym czy prywatnym).

> **Zatem krąg osób, od których pracodawca może otrzymać dane osobowe, oraz które będzie musiał przetwarzać w związku ze zgłoszeniem naruszenia, jest szeroki.**

Projekt ustawy wymienia (choć nie jest to katalog zamknięty) podmioty, które będą uznane za sygnalistów, czyli uprawnionych do przekazywania zgłoszeń. Są nimi:

Pracownicy (także w przypadku, gdy stosunek pracy ustał) **oraz osoby ubiegające się o zatrudnienie**

Osoby świadczące pracę na innej podstawie niż stosunek pracy, w tym na podstawie umowy cywilnoprawnej

Przedsiębiorcy

Akcjonariusze lub wspólnicy oraz osoby będące członkami osoby prawnej

Osoby świadczące pracę pod nadzorem i kierownictwem wykonawcy, podwykonawcy lub dostawcy, w tym na podstawie umowy cywilnoprawnej

Wolontariusze i stażyści

Osoby pomagające w dokonaniu zgłoszenia.

Kluczowe zasady przy planowaniu procesu przetwarzania

Przygotowując się do projektowania nowego procesu przetwarzania warto zwrócić uwagę na kilka podstawowych zadań, które w tym zakresie czekają przedsiębiorców.

W fachowej literaturze można spotkać wytyczne lub zasady uznawane jako podstawowe w odniesieniu do prywatności w fazie projektowania. Są to kolejno:

1) podejście proaktywne, niereaktywne i zaradcze, nienaprawcze;

2) prywatność jako ustawienie domyślne;

3) prywatność włączona w projekt;

4) pełna funkcjonalność: suma dodatnia, nie suma zerowa;

5) ochrona od początku do końca cyklu życia informacji;

6) widoczność i przejrzystość;

7) poszanowanie dla prywatności użytkowników.

Przykład planowania procesu przetwarzania

Zaprojektowanie nowego procesu przetwarzania, umieszczenie go w rejestrze czynności przetwarzania, a także ocena ryzyka naruszenia praw i wolności podmiotów danych wymaga zaplanowania kolejnych kroków. Należą do nich:

Na kolejnych stronach rozłożymy powyższe etapy na czynniki pierwsze.

1. Ustalenie podmiotu danych

Podmiot danych to osoba fizyczna, której dane osobowe przetwarzamy.

Dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą").

Zatem w projektowanym procesie podmiotem danych będzie:

a) osoba dokonująca zgłoszenia, tj. sygnalista – osoba fizyczna, która zgłasza lub ujawnia publicznie informacje na temat naruszeń uzyskane w kontekście związanym z wykonywaną przez nią pracą (pracownik, B2B, quasi pracownik, pracownik tymczasowy, stażysta, praktykant, podwykonawca, freelancer – motyw 38 i 39);

b) osoba pomagająca w dokonaniu zgłoszenia – osoba fizyczna, która pomaga sygnaliście w czynności zgłoszenia i której pomoc nie powinna być ujawniona;

c) osoba, której dotyczy zgłoszenie – osoba fizyczna, która jest wskazana w zgłoszeniu lub ujawnieniu publicznym jako osoba, która dopuściła się naruszenia lub z którą osoba ta jest powiązana.

2. Ustalenie podstawy przetwarzania danych

Skoro już wiemy czyje dane będziemy przetwarzać, w dalszej kolejności powinniśmy się zastanowić nad podstawą, która upoważnia nas do przetwarzania danych osobowych.

Zawsze w takim przypadku warto rozważyć jaki rodzaj danych przetwarzamy, tj. czy będzie to zbiór informacji, który możemy określić jako dane zwykłe, czy też szczególne kategorie danych osobowych.

UWAGA!

W obecnym stanie faktycznym możemy przyjąć, że przetwarzanie danych osobowych wynikające z tzw. dyrektywy o sygnalistach, to działania na tzw. danych zwykłych.

Zgodnie z art. 6 ust. RODO przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Kluczowa zatem wydaje się trzecia przesłanka, tj. realizacja prawnego obowiązku ciążącego na administratorze danych osobowych, o której mowa w art. 6 ust. 1 lit. c RODO.

3. Ustalenie zakresu przetwarzania danych

W unijnej dyrektywie nie ma konkretnych przesłanek określających ściśle zakres danych, który przedsiębiorcy mogliby przetwarzać w związku z realizowanymi działaniami.

Warto zatem pamiętać o minimalizacji danych, tj. o tym, by dane były:

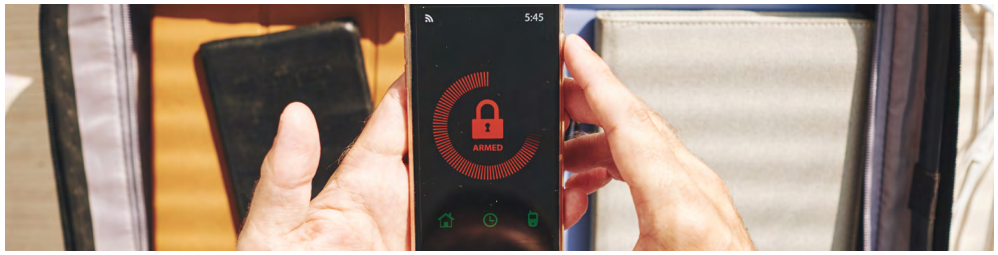
1. adekwatne,
2. stosowne
3. oraz ograniczone do tego, co niezbędne do realizacji celu.

Pamiętajmy także o tym, że dane osobowe, to nie tylko imię i nazwisko i np. dane kontaktowe, ale także szereg informacji, które my wytworzymy w trakcie przetwarzania, jak i informacji, które mają związek z daną osobą fizyczną.

Art. 16 ust. 1

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.

4. Zabezpieczenie przetwarzania danych
Wskazania dyrektywy



W dyrektywie o sygnalistach nie zostały wyszczególnione wskazówki na temat tego jak zabezpieczać dane osobowe, ale taki punkt musi się pojawić w planach dotyczących nowego procesu przetwarzania.

Ogólnym obowiązkiem administratora, wynikającym m.in. z art. 24 RODO, jest konieczność uwzględnienia: (1) charakteru, (2) zakresu, (3) kontekstu i (4) celu przetwarzania oraz (5) ryzyka naruszenia praw lub wolności osób fizycznych, by dobrać odpowiednie środki techniczne i organizacyjne.

Przyjrzyjmy się co w tym zakresie mówią wprost unijne regulacje:

Art. 7 ust. 2
Państwa członkowskie zachęcają do zgłaszania za pośrednictwem wewnętrznych kanałów dokonywania zgłoszeń przed dokonaniem zgłoszenia za pośrednictwem zewnętrznych kanałów dokonywania zgłoszeń w przypadku, gdy naruszeniu można skutecznie zaradzić wewnątrz organizacji, a osoba dokonująca zgłoszenia uważa, że nie zachodzi ryzyko działań odwetowych.

Art. 8 ust. 1
Państwa członkowskie zapewniają, by podmioty prawne w sektorze prywatnym i publicznym ustanowiły kanały i procedury na potrzeby dokonywania zgłoszeń wewnętrznych i podejmowania działań następczych, po konsultacji z partnerami społecznymi, jeżeli tak przewiduje prawo krajowe.

Art. 8 ust. 2
Kanały dokonywania zgłoszeń mogą być obsługiwane wewnętrznie przez wyznaczoną do tego celu osobę lub wyznaczony dział lub zapewniane zewnętrznie przez osobę trzecią. Zabezpieczenia i wymogi, o których mowa w art. 9 ust. 1, stosuje się również do osób trzecich, którym powierzono obsługę kanału dokonywania zgłoszeń na rzecz podmiotu prawnego w sektorze prywatnym.

Art. 9 ust. 1
Procedury na potrzeby zgłoszeń wewnętrznych i działań następczych, o których mowa w art. 8, obejmują następujące elementy:
a) kanały przyjmowania zgłoszeń 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 nieupoważnionym członkom personelu;
b) (...)
c) wyznaczenie bezstronnej osoby lub bezstronnego wydziału właściwych do podejmowania działań następczych w związku ze zgłoszeniami, przy czym może to być ta sama osoba lub ten sam wydział, które przyjmują zgłoszenia, które będą komunikować się z osobą dokonującą zgłoszenia i w stosownych przypadkach zwracać się do osoby dokonującej zgłoszenia o dalsze informacje oraz przekazywać jej informacje zwrotne.

Art. 9 ust. 2
Kanały przewidziane w ust. 1 lit. a) muszą umożliwiać dokonywanie zgłoszeń na piśmie lub ustnie. Zgłoszenie ustne może być dokonane telefonicznie lub za pośrednictwem innych systemów komunikacji głosowej oraz, na wniosek osoby dokonującej zgłoszenia, za pomocą bezpośredniego spotkania zorganizowanego w rozsądnym terminie.

4. Zabezpieczenie przetwarzania danych
Uwagi praktyczne

Z zastrzeżeniem zapewnienia poufności tożsamości osoby dokonującej zgłoszenia, każdy podmiot prawny w sektorze prywatnym i publicznym sam określa, jakiego rodzaju kanały dokonywania zgłoszeń ustanowi.

W szczególności kanały dokonywania zgłoszeń powinny umożliwiać osobom dokonywanie zgłoszeń na piśmie oraz przekazywanie zgłoszeń drogą pocztową, za pośrednictwem fizycznych skrzynek na skargi lub na platformie online, intra- lub internetowej, bądź dokonywanie zgłoszeń ustnie, za pośrednictwem gorącej linii lub innego systemu komunikacji głosowej. Na wniosek osoby dokonującej zgłoszenia kanały takie powinny również umożliwiać dokonywanie zgłoszeń za pośrednictwem bezpośrednich spotkań, w rozsądnym terminie.

Ciężko wskazać jednoznaczne środki zabezpieczeń w ww. przypadkach, ponieważ te zawsze powinny być dobrane do poziomu oceny ryzyka. Warto jednak pamiętać, że w przypadku obsługi każdego rodzaju skrzynek kontaktowych pożądane są wszelkie metody szyfrowania wiadomości – od standardowego szyfrowania treści i uruchomienia prostych reguł wysyłki poczty e-mail, po wdrożenie dodatkowych narzędzi, takich jak klucze PGP.

Wartą rozważenia metodą może być także outsourcing tego obszaru i skorzystanie z zewnętrznego dostawcy usług, który w analizowanym przypadku może stać się podmiotem przetwarzającym dane osobowe.

Wytyczne znajdziemy także w normach ISO, tj. m.in. ISO 37002:2021, która zawiera szereg wskazówek dla wdrożenia systemu zgłaszania nieprawidłowości i zarządzania zgłoszeniami (nie podlega certyfikacji/ można ją wdrożyć, ale nie certyfikować). Można także szukać wskazówek w innych dokumentach i opracowaniach, np. Opinii 1/2006 w sprawie zastosowania zasad ochrony danych do wewnętrznych systemów informowania o nieprawidłowościach (WP 117).

5. Ustalenie okresu przechowywania danych

W każdym procesie przetwarzania musimy określić czas przetwarzania danych osobowych, ponieważ jest to kolejna podstawowa zasada opisana w art. 5 RODO (ograniczenie przechowywania). Jakie wskazówki odnajdziemy w Dyrektywie o sygnalistach?

Art. 18 ust. 1

Państwa członkowskie zapewniają, aby podmioty prawne w sektorze prywatnym i publicznym oraz właściwe organy prowadziły rejestr wszystkich przyjętych zgłoszeń, zgodnie z wymogami w zakresie poufności przewidzianymi w art. 16. Zgłoszenia przechowuje się nie dłużej, niż jest to konieczne i proporcjonalne, aby zapewnić zgodność z wymogami ustanowionymi w niniejszej dyrektywie lub innymi wymogami ustanowionymi w prawie unijnym lub krajowym.

Co to znaczy w praktyce? Rozsądny termin poinformowania osoby dokonującej zgłoszenia nie powinien przekraczać trzech miesięcy. Jeżeli nadal trwają ustalenia dotyczące odpowiednich działań następczych, należy poinformować osobę dokonującą zgłoszenia o tym fakcie i o wszelkich dalszych informacjach zwrotnych, jakich ma prawo oczekiwać.

Generalnie można przyjąć, że czas przetwarzania powinien być uzależniony od charakteru ewentualnego postępowania. Popularna praktyka odnosząca się do określenia czasu przetwarzania na podstawie okresu ochrony roszczeń zapewne nie będzie wystarczająca.

6. Ustalenie osób upoważnionych do przetwarzania

Kolejna podstawowa zasada dotycząca planowania procesu przetwarzania, to dopuszczenie przez administratora do przetwarzania wyłącznie osób do tego upoważnionych.

Pamiętajmy, że liczy się faktycznie nadany poziom uprawnień do danych (np. w systemie informatycznym), który wynika z zakresu obowiązków służbowych. Istotą art. 29 RODO nie jest nadawanie odrębnych druków upoważnień do przetwarzania danych osobowych.

W polskim porządku prawnym istnieje kilka przypadków, w których prawodawca zobligował administratorów do nadawania odrębnych i pisemnych uprawnień, tj. np. w Kodeksie pracy. Być może takie zobowiązanie pojawi się także w ostatecznym tekście krajowej ustawy dotyczącej sygnalistów – obecne zapisy projektu ustawy wskazują na taką konieczność.

Artykuł 29.
Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego. Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

Art. 16 ust. 1
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.

Wybór najwłaściwszych osób lub wydziałów w ramach podmiotu prawnego w sektorze prywatnym, które mają zostać wyznaczone jako właściwe do przyjmowania zgłoszeń i podejmowania działań następczych w związku z nimi, zależy od struktury danego podmiotu, ale w każdym przypadku ich funkcja powinna zapewniać brak konfliktu interesów i niezależność.

W przypadku mniejszych podmiotów funkcja ta może być podwójną funkcją sprawowaną przez osobę odpowiedzialną za określone zadania w przedsiębiorstwie, której stanowisko umożliwia zgłaszanie naruszeń bezpośrednio dyrektorowi organizacji (może to być np. dyrektor ds. zgodności z przepisami lub dyrektor ds. zasobów ludzkich, urzędnik ds. etyki, urzędnik ds. prawnych lub ds. prywatności, dyrektor finansowy, dyrektor ds. audytu lub członek zarządu).

7. Ustalenie odbiorców danych spoza organizacji

Ostatnim elementem planowania procesu przetwarzania w kontekście dyrektywy o sygnalistach jest określenie grona odbiorców danych spoza organizacji.

Oczywistym jest, że takim odbiorcą danych będą uprawnione organy państwowe, które będą pełniły rolę odrębnego administratora danych osobowych. Natomiast należy pamiętać także o podmiotach przetwarzających, tj. podmiotach przetwarzających dane w imieniu administratora/w celu określonym przez administratora. Przykładem takiego podmiotu będzie ewentualny dostawca platformy na potrzeby obsługi zgłoszeń.

Generalnie do przyjmowania zgłoszeń naruszeń w imieniu podmiotów prawnych w sektorze prywatnym i publicznym mogą zostać upoważnione osoby trzecie, pod warunkiem, że zapewniają należyte gwarancje poszanowania niezależności, poufności, ochrony danych i zachowania tajemnicy. Takimi osobami trzecimi mogą być nie tylko dostawcy platform na potrzeby zgłoszeń zewnętrznych, ale również zewnętrzni doradcy, audytorzy, przedstawiciele związków zawodowych lub przedstawiciele pracowników.

Zapraszamy do kontaktu!

Skontaktuj się bezpośrednio z ekspertem

Kacper Rączkowiak

Starszy Specjalista ds. ochrony danych osobowych
Departament Outsourcingu

T +48 789 119 094

E kacper.raczkowiak@pl.gt.com

Redakcja:
Honorata Zakrzewska-Krzyś

Skład:
Aleksandra Mendak

Grant Thornton

Grant Thornton to jedna z wiodących organizacji audytorsko-doradczych na świecie.

Wiedza ponad 56 000 pracowników dostępna jest dla klientów w 140 krajach. W Polsce działamy od 28 lat. Zespół 700 pracowników oraz obecność w kluczowych aglomeracjach (Warszawa, Poznań, Katowice, Wrocław, Kraków i Toruń) zapewniają bliski kontakt z Klientami oraz umożliwiają realizację usług audytorskich, doradztwa podatkowego, doradztwa gospodarczego, prawnego oraz outsourcingu rachunkowości, kadr i płac bez względu na wielkość, rodzaj i lokalizację prowadzonego biznesu.

GrantThornton.pl