Grant Thornton

An instinct for growth™

Purpurowy Informator GT

Zmiany w przepisach o ochronie danych osobowych

Lipiec 2017

Purpurowy Informator – źródło informacji

Z przyjemnością prezentujemy kolejną edycję „Purpurowego Informatora", czyli cyklu analiz, w którym omawiamy ważne dla przedsiębiorców kwestie prawne, księgowe i kadrowe.
Tym razem tematem naszego cyklu są zmiany w przepisach o ochronie danych osobowych, które mają wejść w życie maju 2018 r.
Jak należy dostosować organizację do nowych przepisów o ochronie danych osobowych?
Jakie wyzwania są stawiane przed administratorem danych oraz inspektorem ochrony danych?
O najważniejszych zmianach, jakie niesie za sobą unijne rozporządzenie przeczytają Państwo w naszym opracowaniu.

Zapraszamy do lektury.

Grant Thornton | Lipiec 2017

W maju 2018 roku zacznie obowiązywać unijne rozporządzenie o ochronie danych osobowych.
Nowe przepisy będą dotyczyć wszystkich podmiotów, które na terenie UE przetwarzają dane w sposób zautomatyzowany.
Warto zapoznać się z najważniejszymi zmianami zachodzącymi w rozporządzeniu i rozpocząć przygotowania już teraz.

Monika Smulewicz
Dyrektor Zarządzający/Partner
Outsourcing Rachunkowości,
Płac i Kadr Grant Thornton

25 maja 2018

Data obowiązywania nowych przepisów o ochronie danych osobowych

Od 25 maja 2018 r. państwa członkowskie UE zobowiązane będą do stosowania nowych przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 przyjętego 27 kwietnia 2016 r., które weszło w życie 25 maja 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).

Z tym dniem wszystkie państwa Unii zobowiązane będą stosować bezpośrednio przepisy tego Rozporządzenia bez konieczności uchwalania aktów implementujących.

nowe przepisy
o ochronie danych
osobowych

Skutek wejścia w życie przepisów Rozporządzenia dla przepisów krajowych

Wskutek zapowiadanych zmian, w całej Unii Europejskiej zaczną obowiązywać jednolite zasady ochrony danych osobowych. Oznacza to, że dotychczasowe przepisy ustaw krajowych zostaną w znacznej części zastąpione regulacjami prawnymi obowiązującymi w całej Unii.

W pozostałym zakresie przepisy ustaw krajowych będą mogły regulować materie ochrony danych osobowych odmiennie, częściowo będą precyzować przepisy unijne, częściowo ograniczać lub wyłączać prawa gwarantowane przez Rozporządzenie, a częściowo regulować te obszary, które Rozporządzenie przekazało ustawodawcom krajowym. Obecnie w sejmie trwają prace nad nowym brzmieniem ustawy o ochronie danych osobowych.

jednolite zasady ochrony danych osobowych w Unii Europejskiej

Cel nowej regulacji

Celem regulacji jest ujednolicenie zasad i wzmocnienie ochrony danych osobowych w związku z postępem technicznym i coraz szerszym zakresem cyfryzacji.

Wprowadzenie nowych przepisów pozwoli wyjść naprzeciw wyzwaniom stawianym przez osiągnięcia techniki, a w tym zakresie coraz większe możliwości gromadzenia i coraz szersze zakresy przetwarzania danych.

Celem Rozporządzenia jest również objęcie swoją regulacją nowych obszarów życia społecznego i nowych zjawisk społeczno-gospodarczych takich jak np. globalizacja czy transgraniczny przepływ danych, niepoddanych dotąd lub poddanych takiej regulacji cząstkowo (np. nowe sposoby przetwarzania danych osobowych, nowe kategorie danych), po to aby zapewnić skuteczniejszą ochronę danych osobowych.

Korzyści dla osób fizycznych

Niewątpliwie najbardziej doniosłą korzyścią jest uzyskanie przez osoby fizyczne prawa do bycia zapomnianym. Prawo to gwarantować będzie osobom, których dane przetwarzane były bez podstawy prawnej, i które nie chcą by ich dane były przetwarzane nadal, prawo do żądania usunięcia tych danych. Narzędzie to ma chronić prywatność osób, których dane są przetwarzane.

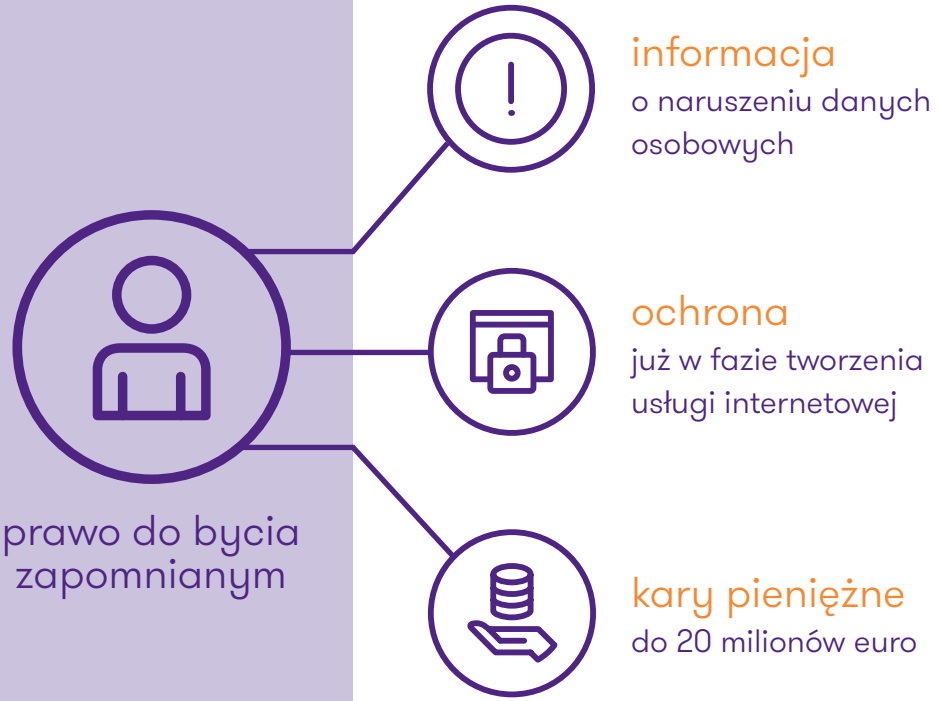
Jako kolejne korzyści należy wskazać uzyskanie łatwiejszego dostępu do danych poprzez poszerzenie zakresu dostępu do informacji o przetwarzaniu ich danych oraz prawo do uzyskania tych danych w jasnej i zrozumiałej formie.

Ochronie osób, których dane będą przetwarzane, służyć ma również obowiązek, nałożony na administratorów danych osobowych, o informowaniu organu nadzoru (będzie nim Urząd Ochrony Danych Osobowych, który zastąpi GIODO) oraz osób, których dane są przetwarzane o wszelkich przypadkach naruszenia danych.

Osoby fizyczne uzyskają również większe gwarancje skutecznej ochrony danych osobowych, wynikające z systemowej zmiany podejścia do ochrony poprzez wyeksponowanie postulatu ochrony już w fazie tworzenia usługi internetowej.

Kolejną zaletą nowej regulacji są większe gwarancje egzekwowania przestrzegania przepisów o ochronie danych osobowych poprzez wyposażenie UODO w możliwość nakładania administracyjnych kar pieniężnych w wysokości do 20 milionów euro lub do 4% całkowitego rocznego światowego obrotu.

Nowa regulacja pozwoli również łatwiej przenieść swoje dane osobowe od jednego administratora danych do drugiego. W przypadku takiego wniosku osoby zainteresowanej dotychczasowy administrator zobowiązany będzie wydać wnioskodawcy te dane w ustrukturyzowanej formie nadającej się do odczytu maszynowego.



Najważniejsze zmiany w obszarze definiowania danych osobowych

Zmiany rozszerzają niektóre definicje prawne, np. pojęcie danych osobowych, poprzez np. objęcie tym znaczeniem danych o lokalizacji oraz identyfikatorów internetowych, w tym np. nr IP urządzenia, z którego osoba korzysta art. 4 Rozporządzenia.

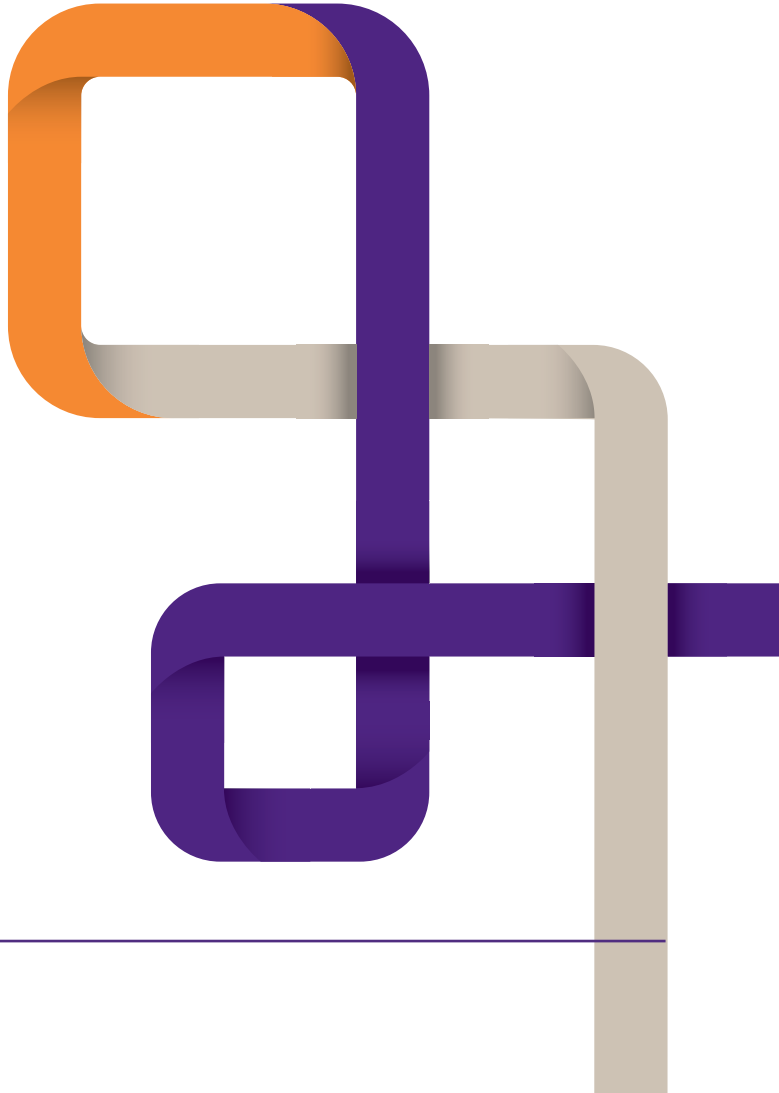
Doprecyzowana i poszerzona zostaje również definicja przetwarzania poprzez dodanie takich czynności jak przeglądanie, ujawnianie przez przesłanie, dopasowywanie lub łączenie – art. 4 Rozporządzenia.

Wprowadzone zostaje także pojęcie profilowania, które oznacza sposób przetwarzania polegający na wykorzystaniu danych do oceny niektórych czynników osobowych osoby fizycznej oraz pseudonimizacji, czyli takiego ich przetwarzania, które nie pozwala na przypisanie określonych danych konkretnej osobie bez użycia dodatkowych informacji – art. 4 Rozporządzenia.

Pojawiają się również nowe pojęcia prawne, takie jak dane biometryczne, dane genetyczne czy dane dotyczące zdrowia – art. 4 Rozporządzenia.

dane o lokalizacji
oraz o identyfikatorach internetowych

przeglądanie, ujawnianie
przez przesłanie, dopasowywanie lub łączenie



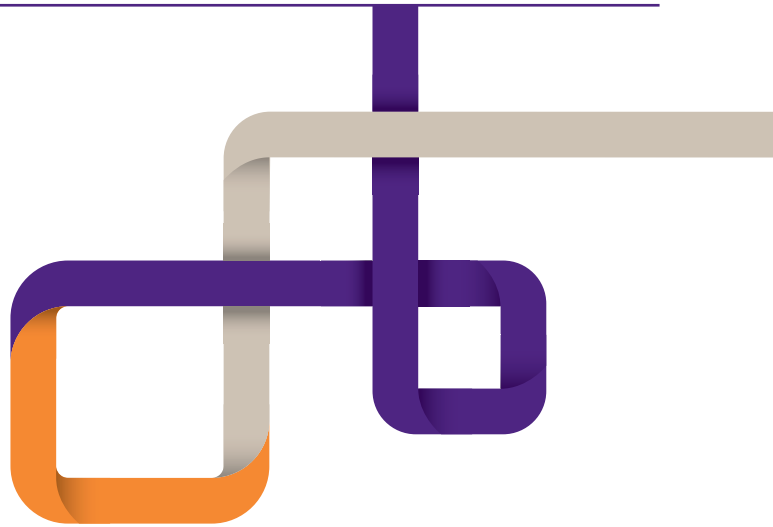
Najważniejsze zmiany instytucjonalne

Kompetencje organu nadzorczego

1 **Ustalenie nowych kompetencji organu nadzorczego, którym w Polsce docelowo ma być Urząd Ochrony Danych Osobowych**

Rozszerzone zostają kompetencje organu nadzorczego oraz zwiększona jego samodzielność i niezależność. Temu celowi służy obowiązek nałożony na państwa członkowskie zapewnienia rodzimym organom nadzoru (w Polsce UODO) niezbędnych środków organizacyjnych, technicznych i finansowych. Poszerzone zostają również możliwości działania organów nadzoru poprzez delegowanie na nie nowych lub rozszerzenie dotychczasowych kompetencji, takich jak działalność edukacyjna oraz doradcza, która będzie podejmowana zarówno na poziomie instytucji jak i względem zwykłych obywateli.

Najważniejsze zmiany instytucjonalne



Powołanie funkcji inspektora danych osobowych – IDO

2 Likwidacja Administratora Bezpieczeństwa Informacji i utworzenie w jego miejsce Inspektora Ochrony Danych Osobowych (IDO)

Planowana zmiana ma stanowić fundament skutecznego systemu ochrony danych osobowych. Należy jednak mieć na uwadze, że obowiązek wyznaczenia IDO dotyczył będzie tylko pewnej grupy administratorów danych osobowych, w tym także podmiotów przetwarzających dane osobowe w imieniu administratora danych osobowych.

W zamierzeniu twórców regulacji osoby wyznaczone do pełnienia funkcji IDO mają przede wszystkim przejawiać proaktywne podejście do ochrony danych osobowych i w tym zakresie powinny identyfikować zagrożenia i definiować ryzyka związane z przetwarzaniem określonych danych osobowych. IDO stanowić będzie również wsparcie dla administratora danych osobowych, a do jego zadań należeć będzie doradzanie administratorowi, które operacje na danych powinny być poddane kontroli i jaką przyjąć metodologię działań oraz czy zrealizować te czynności we własnym zakresie czy też zlecić je na zewnątrz. Ponadto, IDO obowiązany będzie stale weryfikować monitorować działania administratora. Ze względu zatem na znaczący wpływ IDO na proces przetwarzania danych osobowych niezwykle istotne staną się kwestie szczególnych kwalifikacji i umiejętności, które powinien on posiadać. Ponadto, gwarancją realizacji jego zadań w zamierzeniach prawodawców będzie duży zakres niezależności IDO osiągnięty poprzez poddanie kontroli jego działania wyłącznie osobom z najwyższego kierownictwa administratora danych lub podmiotu przetwarzającego dane osobowe.

W zamierzeniu prawodawcy IDO pełnił będzie również funkcję punktu kontaktowego dla UODO oraz osób, których dane są przetwarzane. W pierwszym przypadku będzie on ogniwem pośredniczącym pomiędzy administratorem, a UODO w fazie konsultacji przed rozpoczęciem przetwarzania danych osobowych, a w drugim przypadku będzie on osobą kontaktową w sprawach przetwarzania danych osobowych osób, których przetwarzanie dotyczy. Tu jego rola będzie polegać na udzielaniu pomocy i wyjaśnień.

Jednocześnie wskazuje się, że rola i zadania IDO nie będzie sprowadzać się wyłącznie do realizacji katalogu zadań wprost w Rozporządzeniu określonych. Wskazuje się bowiem w interpretacjach działającego jeszcze GIODO, że osoby wyznaczone do pełnienia tych funkcji wspierać będą administratorów danych we wszystkich ich zadaniach z wyłączeniem tych, których realizacja i ryzyko z tym związane zostało wyraźnie nałożone na administratorów (np. wdrożenie odpowiednich środków technicznych i organizacyjnych).

Najważniejsze zmiany instytucjonalne

Zniesienie wymogu rejestracji zbiorów danych osobowych

3 **Zniesienie wymogu rejestracji zbiorów danych osobowych**

Powstałą w ten sposób lukę ma zapełnić obowiązek współdziałania administratora danych osobowych z organem nadzoru w zakresie definiowania zagrożeń i podejmowania działań w celu ich wyeliminowania.

W tym celu UODO zobowiązany będzie ustalić i podać do publicznej wiadomości alternatywnie; wykaz operacji na danych nie podlegających ocenie pod kątem skutków dla ochrony danych osobowych albo wykaz operacji podlegających takiej ocenie. Dla przykładu do operacji, które należy oceniać pod kątem skutków dla ochrony danych osobowych należy zaliczyć, np. wspomniane wcześniej profilowanie. Do takich operacji będzie należeć również przetwarzanie na dużą skalę szczególnych kategorii danych.

Zmiana pozycji administratora danych osobowych

4 **Zmiana pozycji i obowiązków administratora danych osobowych**

Jego rola wzrośnie przed rozpoczęciem przetwarzania danych osobowych, gdyż na tym etapie powinien on zdefiniować zagrożenia w przetwarzaniu danych osobowych, ocenić ryzyka i podjąć działania w celu ich wyeliminowania. Jeżeli w trakcie tej oceny okaże się, że istnieje znaczne ryzyko dla ochrony danych osobowych i konieczne będzie zastosowanie odpowiednich środków zmniejszających to ryzyko, wówczas administrator zobowiązany będzie skonsultować się z organem nadzoru.

Obowiązkiem administratora będzie wdrożenie odpowiednich środków technicznych i organizacyjnych służących skutecznej realizacji zasad ochrony danych osobowych. Odpowiedzialność za przyjęcie i wdrożenie odpowiednich środków spoczywać będzie wyłącznie na administratorze danych osobowych. Co więcej, to na administratorze ciążył będzie obowiązek wykazania, że postępuje zgodnie z Rozporządzeniem – art. 24 Rozporządzenia.

W odniesieniu do niektórych administratorów danych osobowych, stanowiących np. jednostki sektora publicznego albo administratorów przetwarzających określone kategorie danych osobowych, taki administrator będzie miał obowiązek wyznaczenia inspektora danych osobowych – art. 37 Rozporządzenia.

W przypadku natomiast, gdy z przepisów nie wynika obowiązek wyznaczenia IDO, zaleca się administratorom danych osobowych oraz podmiotom przetwarzającym stworzenie dokumentu, z którego wynikać będzie, że przeprowadzili wewnętrzną procedurę mającą na celu ustalenie istnienia bądź braku obowiązku wyznaczenia IDO – wytyczne GIODO dla inspektorów ochrony danych osobowych.

Pozostałe zmiany

Do najważniejszych zmian, które zostaną wprowadzone Rozporządzeniem niewątpliwie należy zaliczyć:

ustanowienie uprawnienia do usunięcia danych, czyli do „bycia zapomnianym”

możliwość wprowadzania kodeksów postępowania

możliwość wspólnego prowadzenia postępowań przez organy nadzoru z różnych państw

powołanie Europejskiej Rady Ochrony Danych

prawo do wnoszenia skarg do organów nadzorczych

Sytuacja przedsiębiorcy po wejściu w życie Rozporządzenia

W zasadzie należałoby stwierdzić, że sam dzień wejścia w życie nowych przepisów nie będzie miał przełomowego znaczenia, gdyż i tak większość zmian oraz działań implementacyjnych będzie musiała być przeprowadzona przed dniem rozpoczęcia obowiązywania Rozporządzenia tj. 25 maja 2018 r.

Część przedsiębiorców (zatrudniająca ponad 250 pracowników oraz przetwarzająca dane w sposób zagrażający naruszeniem praw lub wolności osób których dane są przetwarzane) będzie zmuszona dokonać przeglądu obowiązujących procedur i systemów ochrony danych osobowych. Wynikać to będzie z konieczności oceny istniejących zabezpieczeń z punktu widzenia ryzyka, jakie wiąże się z przetwarzaniem określonych danych osobowych. W przypadku stwierdzenia przez administratora danych, że w obszarze przetwarzania danych osobowych istnieją ryzyka związane z ich ochroną, zobowiązany będzie wdrożyć odpowiednie środki. Nie można również wykluczyć, w niektórych przypadkach konieczności poprzedzenia konsultacji z inspektorem danych osobowych oraz UODO.

Ponadto, administratorzy danych już dziś powinni rozpocząć prace nad opracowaniem mechanizmów pozwalających na realizacje uprawnień osób, których dane są przetwarzane, a które np. złożą wniosek o przeniesienie danych do innego administratora lub też wniosek o udostępnienie na użytek osobisty przetwarzanych danych w formie pozwalającej na ich odczytanie. Dużym wyzwaniem będzie również sprostanie wymogowi usunięcia danych na żądanie osób uprawnionych zwłaszcza danych zawartych w systemach informatycznych.

Przedsiębiorcy (obowiązani do wyznaczenia IDO) będą również musieli rozważyć czy osobą pełniącą funkcję IDO będzie zatrudniony przez nich pracownik czy też osoba spoza tego grona. Należy przypuszczać, że czynnikiem decydującym o takiej decyzji będzie weryfikacja pod kątem kompetencji i umiejętności niezbędnych do pełnienia tej funkcji. Administratorzy danych osobowych będą zmuszeni zmienić sposób pełnienia swojej funkcji na bardziej aktywny, definiujący zagrożenia.

Niezwykle istotnaą kwestią w procesie weryfikacji procedur i systemów ochrony danych powinno być weryfikowanie zakresu i podstaw prawnych przetwarzania danych osobowych. W tym celu należy w pierwszej kolejności dokonać analizy zgodności przetwarzania danych pod kątem zgodności z zasadami przetwarzania danych osobowych (głównie zgodności z prawem, rzetelności, proporcjonalności, aktualności, bezpieczeństwa). Następnie należy zweryfikować podstawy przetwarzania danych pod kątem posiadania odpowiednich zgód osób, których dane są przetwarzane lub spełnienia przesłanek przetwarzania danych osobowych określonych w Rozporządzeniu. Za niedochowanie tych czynności odpowiedzialność ponosił będzie administrator.

Korzyści dla przedsiębiorców

Rozporządzenie wprowadza jednolity porządek prawny w zakresie ochrony danych osobowych na terytorium całej Unii, co pozwoli na tańsze i prostsze prowadzenie biznesu w Unii Europejskiej.

Spółki spoza Unii będą musiały dostosować się do przepisów Rozporządzenia.

Przedsiębiorstwa typu start-up i małe przedsiębiorstwa poprzez prawo do przenoszenia danych, ułatwiające zmianę dostawcy usług, będą mogły uzyskać dostęp do rynków danych zdominowanych przez duże przedsiębiorstwa oparte na technologiach cyfrowych, zachęcając konsumentów rozwiązaniami chroniącymi ich prywatność.

Warto również zwrócić uwagę na korzyści płynące z braku sztywnych reguł ochrony danych osobowych, co w założeniu prawodawców ułatwi dostosowanie tych reguł do specyficznych rodzajów prowadzonej działalności.

Kolejnym elementem jest mechanizm One-stop-shop, który umożliwiał będzie przedsiębiorcom ograniczenie kontaktu z organami nadzoru (w Polsce będzie to UODO) do jednego wyznaczonego organu. Mechanizm ten ułatwi także polskim podmiotom dochodzenie swoich praw wobec przedsiębiorców z innych krajów UE.

Wprowadzenie nowych przepisów zapewni także bezpieczne korzystanie z tzw. usług Big Data, dając przedsiębiorstwom z UE elastyczność korzystania z danych osobowych przy jednoczesnej ochronie praw podstawowych obywateli.

Monika Smulewicz
Dyrektor Zarządzający/Partner
Outsourcing Rachunkowości, Płac i Kadr
Grant Thornton
T +48 22 205 49 00
E Monika.Smulewicz@pl.gt.com

Magdalena Marcinowska
Payroll Partner
Outsourcing Rachunkowości, Płac i Kadr
Grant Thornton
T +48 61 625 14 02
E Magdalena.Marcinowska@pl.gt.com

Mamy nadzieję, iż przygotowany przez nas materiał będzie dla Państwa pomocny.
W razie pytań lub wątpliwości, zapraszamy do kontaktu!

Grant Thornton
An instinct for growth™

www.GrantThornton.pl