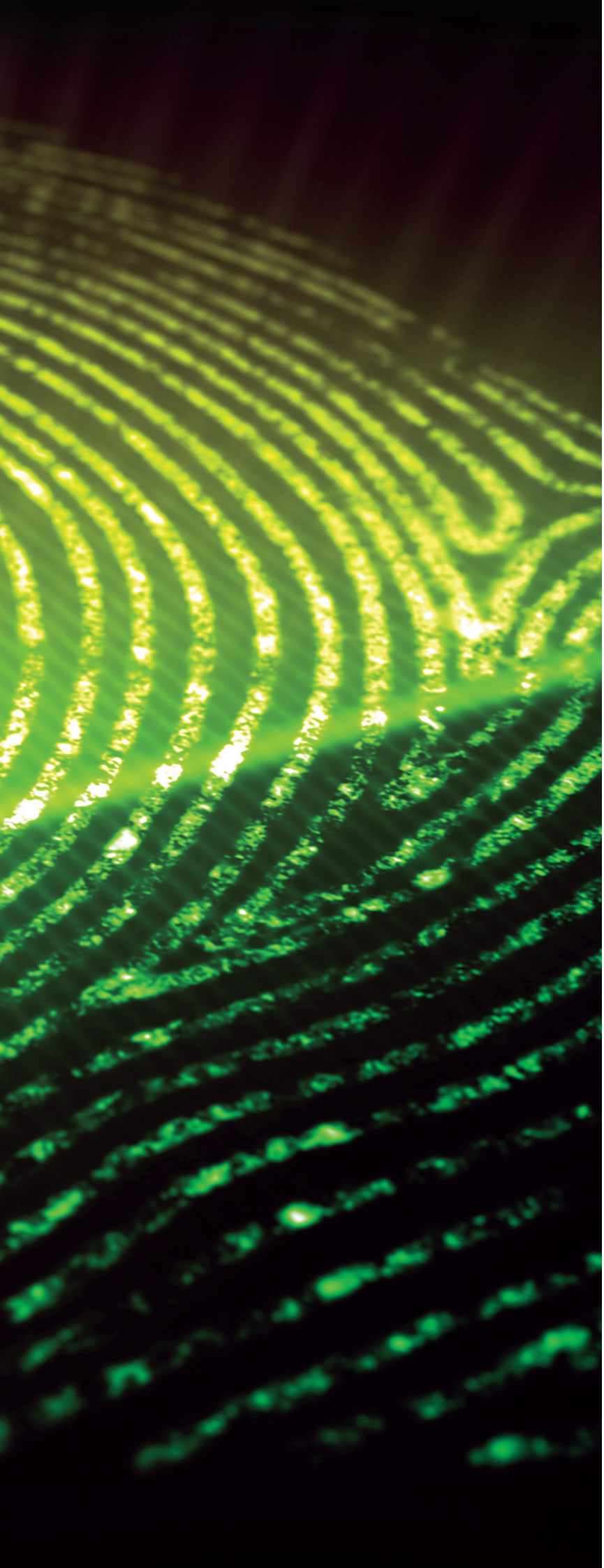


DZP

więcej niż prawo

NOWE WYZWANIA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

SYNTETYCZNE PORÓWNANIE NOWEGO EUROPEJSKIEGO ROZPORZĄDZENIA Z USTAWĄ O OCHRONIE DANYCH OSOBOWYCH

Wstęp

Bartosz Marcinkowski
Partner DZP
tel. 22 557 76 17
bartosz.marcinkowski@dzp.pl

Potrzeba głębokiej reformy unijnego systemu ochrony danych osobowych sygnalizowana była w UE już od wielu lat. Konieczność wprowadzenia kompleksowych zmian determinowana jest wieloma okolicznościami. Po pierwsze wynika to z faktu, iż obowiązujące w UE przepisy dotyczące ochrony danych osobowych liczą sobie już ponad 20 lat, co w realiach zatrważającego i bezprecedensowego tempa rozwoju środków gromadzenia i przetwarzania informacji stanowi wieczność.

Po drugie rozwiązania w zakresie ochrony danych osobowych przyjęte w krajach członkowskich UE znacząco się od siebie różnią. Regulująca dziedzinę unijna Dyrektywa 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych („Dyrektywa") wymagała stosownej implementacji tj. mniej lub bardziej twórczego wprowadzenia jej rozwiązań do systemów prawnych każdego z państw UE. W Polsce przepisy Dyrektywy zostały wprowadzone przez ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych („UODO"), która jest przykładem dość wiernej implementacji rozwiązań Dyrektywy w porządku prawnym. Z drugiej strony mamy przykład brytyjskiej ustawy o ochronie danych osobowych, która cechuje się znacznym stopniem liberalizmu i która wprowadza znaczące ustępstwa na tle wzorca z Dyrektywy.

Po trzecie, wobec nasilającej się fali naruszeń danych osobowych nagląca stała się konieczność wyposażenia krajowych organów ochrony danych osobowych (w Polsce jest to Generalny Inspektor Ochrony Danych Osobowych - „GIODO") w realne środki prawne umożliwiające im skuteczne wyegzekwowanie przetwarzania danych osobowych zgodnie z obowiązującymi przepisami. Znów, także i w tej dziedzinie w różnych państwach UE w różny sposób implementowano postanowienia Dyrektywy dotyczące sankcji za niezgodne przetwarzanie danych osobowych. Dla przykładu hiszpański odpowiednik GIODO już dziś dysponuje prawem nakładania sankcji finansowych na administratorów danych łamiących obowiązujące przepisy, podczas gdy organ polski nie został wyposażony w takie uprawnienie.

Wreszcie ostatnim z palących problemów jest zagadnienie transferu danych osobowych poza Europejski Obszar Gospodarczy, w tym m.in. transfer danych do USA czy Chin. Problem ten, choć znany i szeroko omawiany, nie został dotychczas rozwiązany w satysfakcjonujący sposób.

Wypadkową powyższych okoliczności jest przyjęcie, po przeszło 4 latach prac analitycznych i uzgodnień pomiędzy organami unijnymi, unijnego Ogólnego rozporządzenia o ochronie danych („Ogólne rozporządzenie UE"), które w dniu 25 maja 2018 r. zastąpi zarówno Dyrektywę jak i regulacje krajowe, w tym m.in. UODO.

Wciąż jednak Ogólne rozporządzenie UE przewiduje szereg kwestii, które krajowi ustawodawcy będą mogli doprecyzować – stąd na przykład w Polsce obecnie mówi się o nowej ustawie o ochronie danych osobowych, dopełniającej i uzupełniającej regulacje unijną.

Od 25 maja 2018 r. omawiana dziedzina będzie w jednolity osób regulowana na szczeblu unijnym, co zapewni jednolitość regulacji w skali UE. Nie jest jednak przesądzone, że paneuropejskie rozporządzenie zapewni jednolitość wykładni i praktyki w stosowaniu go przez krajowe organy nadzorcze. Niemniej przetwarzanie danych osobowych odbywać się będzie w całkowicie nowym otoczeniu prawnym. Podkreślić należy również, że mamy tu do czynienia z niezbyt często spotykaną sytuacją, w której, unijna regulacja, oddziałuje wprost i bezpośrednio na prawa i obowiązki obywateli. Osobną kwestią jest zagadnienie czytania i stosowania nowego prawa z uwzględnieniem dotychczasowych regulacji i doświadczeń.

Poza tym, owa powszechna europejska regulacja będzie oddziaływała wprost na prawa i obowiązki zarówno podmiotów (firm i innych jednostek) z UE, jak i z krajów spoza UE. Z uwagi na rewolucyjne zmiany dotyczące zasad przetwarzania danych osobowych pewne nowe wymogi, obowiązki i obostrzenia zasługują na szczególną uwagę.

Niniejsze opracowanie poświęcone jest wybranym obszarom - nowym wymogom, obowiązkom i obostrzeniom - a naszym zamiarem jest możliwie przystępnie i obrazowo przybliżyć wskazane zagadnienia. Wybrana forma i objętość materiału nie pozwalają ani na wyczerpanie tematu, ani udzielenie odpowiedzi na wszelkie nurtujące pytania. Stąd zapraszam nie tylko do zapoznania się z naszym omówieniem, ale też do kontaktu w celu kontynuacji zapoczątkowanej tu dyskusji!

Spis treści

Zakres terytorialny

Dylematy i pytania praktyczne rodziły i nadal rodzą zagadnienia tak elementarne jak zakres terytorialny stosowania przepisów o ochronie danych osobowych.

Do 24 maja 2016	Od 25 maja 2016
Przepisy stosuje się wobec podmiotów, które albo mają siedzibę w Polsce, albo w państwie poza Europejskim Obszarem Gospodarczym (ale tu jedynie, gdy przetwarzają dane przy wykorzystaniu środków technicznych na terytorium polskim).	Przepisy stosuje się niezależnie od miejsca przetwarzania danych, o ile realizuje je podmiot przetwarzający dane w UE. Poza tym, przepisy Ogólnego rozporządzenia UE stosuje się również gdy przetwarzane są dane osób przebywających w UE nawet jeśli dane przetwarzane są przez podmioty spoza UE. Powyższe dotyczy wyłącznie sytuacji kiedy dochodzi do: ■ oferowania usług lub towarów, lub ■ monitorowania ich zachowania do którego dochodzi na terenie UE. Zastosowanie przepisów Ogólnego rozporządzenia UE do podmiotu nie mającego siedziby w UE obliguje administratora danych do wyznaczenia swojego przedstawiciela na terenie UE.

Definicja pojęcia danych osobowych i zgody

Inną sferą budzącą wątpliwości pozostaje sfera definicji, w tym rozumienia pojęcia „dane osobowe" oraz „zgody" na przetwarzanie danych.

Do 24 maja 2016	Od 25 maja 2016
Zgodnie z definicją zawartą w UODO za „dane osobowe" uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.	W rozumieniu Ogólnego rozporządzenia UE „dane osobowe" obejmują informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (bezpośrednio lub pośrednio), na podstawie m.in. identyfikatora takiego jak imię i nazwisko, danych o lokalizacji, identyfikatora internetowego lub jednego lub kilku czynników określających fizyczną, socjologiczna, genetyczną, psychiczną tożsamość osoby fizycznej. Przez dane osobowe Ogólne rozporządzenie UE rozumie również wyraźnie wymienione i definiowane: ■ dane genetyczne, ■ dane biometryczne, ■ dane dotyczące zdrowia.
Zgodnie z definicją zawartą w UODO przez „zgodę osoby" rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści i może być odwołana w każdym czasie.	Przez „zgodę" Ogólne rozporządzenie UE rozumie dobrowolne, konkretne, świadome i jednoznaczne okazanie woli podmiotu danych, przejawiające się w formie oświadczenia lub wyraźnego działania potwierdzającego, które przyzwala na przetwarzanie jej danych osobowych.

Zasługuje na uwagę nieco liberalniejsze potraktowanie zgody w naszej regulacji, zwłaszcza w świetle obecnie dominujące w Polsce praktyki zbierania – dla celów dowodowych – zgód w formie pisemnej. Aczkolwiek Ogólne rozporządzenie UE wymaga od adresata zgody zdolności wykazania jej otrzymania.

Filary legalnego przetwarzania danych osobowych

Legalne przetwarzanie i zabezpieczenie danych osobowych obejmuje szereg składowych, które muszą wystąpić łącznie. Są to:

- **Podstawa**
- **Informowanie**
- **Zabezpieczenia**
- **Inspektor danych osobowych**

Nowe przepisy nie wprowadzają rewolucyjnych zmian w zakresie filarów legalnego przetwarzania danych, jednak pewne elementy i okoliczności wymagają odnotowania.

Podstawa przetwarzania danych osobowych

W nowej regulacji położono szczególny nacisk na ważenie praw i interesów jednostki, eliminując przykładowe zwolnienia ustawowe mające zastosowanie m.in. do marketingu bezpośredniego własnych produktów lub usług.

Do 24 maja 2016

Jedną z podstaw przetwarzania danych osobowych przewidzianą przez UODO stanowi sytuacja w której przetwarzanie danych osobowych jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Za prawnie usprawiedliwiony cel uważa się w szczególności:

- marketing bezpośredni własnych produktów lub usług administratora danych;
- dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Od 25 maja 2016

Zgodnie z regulacjami Ogólnego rozporządzenia UE przetwarzanie danych osobowych jest dopuszczalne m.in. jeżeli jest ono niezbędne dla celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora danych lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub prawa podstawowe i wolności podmiotu danych, wymagające ochrony danych osobowych, w szczególności gdy podmiot danych jest dzieckiem.

„Dzieckiem" w rozumieniu naszych przepisów jest co do zasady osoba, która nie ukończyła 16 lat. W tym zakresie regulacje Ogólnego rozporządzenia UE są tożsame z polskimi regulacjami krajowymi. Rozporządzenie pozostawia jednak pewną dozę uznaniowości państwom członkowskim, które mogą przewidzieć w prawie krajowym niższą granicę wiekową, którą musi jednak wynosić co najmniej 13 lat.

Przejrzyste informowanie podmiotu danych osobowych

Nadal obowiązywać będą wymogi szczegółowego i zrozumiałego informowania osób, których dane dotyczą, o fakcie i okolicznościach przetwarzania ich danych osobowych. Obowiązki informacyjne mają to do siebie, że usunięcie wcześniejszych uchybień może być szczególnie kosztowne, a jednocześnie realizacja tych obowiązków ma kluczowe znaczenie z perspektywy ochrony praw i wolności jednostki. Obywatel nie będzie w stanie bronić się przed naruszeniami, jeśli nie będzie świadomy kto i w jakich celach wykorzystuje informacje na jego temat.

W razie braku doinformowania obywatel miałby m.in. trudności ze skorzystaniem z nowych przysługujących mu prawa – tj. m. in. „prawa do bycia zapomnianym", a także prawa do ograniczenia przetwarzania danych do niezbędnego minimum oraz prawa do przeniesienia danych (tj. przekazania w pewnych przypadkach danych nowemu administratorowi, o ile jest to technicznie możliwe).

Do 24 maja 2016	Od 25 maja 2016
Przepisy UODO nakazują m.in. podać cel przetwarzania danych, kategorie odbiorców czy zidentyfikować administratora danych osobowych.	Przepisy Ogólnego rozporządzenia UE nakazują, podać nie tylko cel przetwarzania danych, ale i m.in. podstawę przetwarzania danych, informacje o prawie wniesienia skargi do organu nadzorczego, informacje o zamiarze przekazania danych poza EOG oraz informację o okresie przez który dane będą przechowywane.

Jak zatem widać obowiązkowe i kluczowe w dziedzinie ochrony danych osobowych klauzule informacyjne będą obejmować więcej informacji niż obecnie, a ich redagowaniu będzie musiała towarzyszyć pogłębiona refleksja. Co więcej, w pewnych przypadkach wymagane będzie wskazanie prawnie usprawiedliwionego interesu, dla realizacji którego dane są przetwarzane oraz informacja o profilowaniu jednostek przy wykorzystaniu ich danych osobowych.

Zabezpieczenie danych osobowych

Zabezpieczenie danych osobowych ma na celu zapewnienie, aby były one wykorzystywane zgodnie z prawem przez podmioty, które są do tego uprawnione. Zabezpieczenie danych osobowych ma służyć m.in. ochronie danych przed ujawnieniem ich niepowołanym osobom czy wykorzystaniem dla celów innych niż te, dla których zostały one zgromadzone.

Do 24 maja 2016

Zasadnicze znaczenie w zabezpieczeniu danych osobowych w rozumieniu UODO mają „Polityka Bezpieczeństwa" oraz „Instrukcja Zarządzania Systemem Informatycznym", o treści precyzyjnie wskazanej w aktach wykonawczych do UODO. Przygotowanie i wdrożenie takiej dokumentacji jest obligatoryjne dla każdego administratora danych osobowych.

Od 25 maja 2016

Regulacje Ogólnego rozporządzenia UE przypisują bardzo istotną rolę branżowym lub środowiskowym kodeksom dobrych praktyk (kodeksy postępowania) podlegającym procesowi monitorowania przez organ nadzorczy oraz certyfikacji stanowiącej potwierdzenie spełnienia wymogów prawa dotyczących ochrony danych osobowych.

Oba wskazane środki mają charakter dobrowolny i mają towarzyszyć obowiązkowej i odpowiedniej dokumentacji ochrony danych, stanowiącej o zastosowaniu odpowiednich środków technicznych i organizacyjnych zabezpieczających dane.

Jak wcześniej wspomniano, administrator musi umieć wykazać nadzór nad procesami przetwarzania danych odbywającymi się w jego jednostce organizacyjnej (tzw. zasada rozliczalności). W szczególności, w celu zapewnienia owej rozliczalności administrator danych osobowych rejestruje podejmowane czynności przetwarzania danych oraz prowadzi rejestr kategorii czynności dokonywanych na przetwarzanych danych osobowych.

Inspektor ochrony danych

Aktualnie Administrator Bezpieczeństwa Informacji („ABI"), a od 25 maja 2018 r. Inspektor Ochrony Danych („IOD") ma pełnić szczególną funkcję wewnątrz jednostki organizacyjnej w sferze ochrony danych osobowych. I tak, jak obecnie przepisy nie przewidują bezwzględnego obowiązku powołania i zarejestrowania ABI w GIODO, tak w przyszłości, zgodnie z Ogólnym rozporządzeniem UE, powołanie IOD będzie obowiązkowe zawsze w sytuacji gdy:

- dane przetwarzane są przez organ lub podmiot publiczny, z wyjątkiem sądów;
- główna działalność administratora danych lub przetwarzającego dane polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
- główna działalność administratora danych polega na przetwarzaniu na dużą skalę szczególnych kategorii danych – tj. dane dotyczące m.in. pochodzenia rasowego, poglądów politycznych, zdrowia lub danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, oraz przetwarzania danych dotyczących wyroków skazujących i naruszeń prawa.

Zatem w wielu przypadkach powołanie takiego inspektora będzie obowiązkowe. Należy jednak zaznaczyć, że kryteria jego obowiązkowego powołania są określone dość nieprecyzyjne, m.in. poprzez użycie nieostrych pojęć takich jak np. „monitorowanie (..) na duża skalę" lub „przetwarzanie na dużą skalę".

Inne istotne zmiany od 25 maja 2018

We wcześniejszej części opracowania porównaliśmy zasadnicze instytucje prawne i definicje - dotychczasowe i wprowadzone nowymi przepisami. Informacje te służą zbudowaniu stanu świadomości w jakim zakresie znajomość dziedziny wymaga rewizji.

Poniżej natomiast kilka nowych kwestii, które mogą mieć szczególne znaczenie praktyczne, w tym zwłaszcza omówienie całkowitej nowości, tj. sankcji finansowych, które będzie mógł już od 25 maja 2018 roku, nakładać GIODO.

Współadministratorzy danych osobowych

Ogólne rozporządzenie UE wyraźnie przewiduje sytuację, w której dwóch lub więcej administratorów wspólnie ustala cele i sposoby przetwarzania danych osobowych. Taka sytuacja będzie dotyczyć np. grup spółek, w których wykorzystywany jest jeden, wspólny zbiór danych.

Powierzenie przetwarzania danych

Pisemna lub utrwalona elektronicznie umowa będzie musiała zawierać szereg postanowień dotychczas przez przepisy niewymagane, m.in. czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj powierzonych danych osobowych oraz kategorie osób, których dane dotyczą.

W związku z powyższym konieczne będzie gruntowne przeanalizowanie umów tego rodzaju z udziałem prawników i dostosowanie tych dokumentów do nowych przepisów. Tego typu sytuacja skłania kontrahentów do próby negocjowania warunków istniejących umów!

Rejestr czynności przetwarzania

Ogólne rozporządzenie UE wprowadza nowy wymóg, tj. obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, o treści precyzyjnie określonej w przepisach. Za brak rejestru odpowiada administrator danych.

Obowiązek zgłaszania naruszeń ochrony danych organowi nadzorczemu

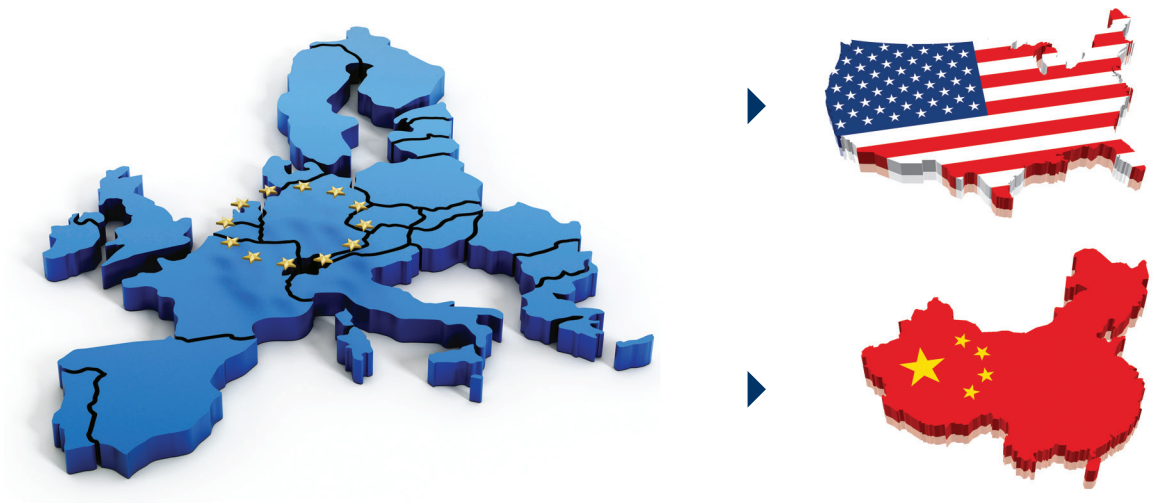
Wzorem m.in. amerykańskich regulacji stanowych, Ogólne rozporządzenie UE wymaga zgłoszenia faktu naruszenia ochrony danych osobowych w ciągu 72 godzin od stwierdzenia naruszenia.

Zgłoszenie musi zawierać informacje wskazane w przepisach. Za brak zgłoszenia w terminie odpowiada obowiązany podmiot.

Gdy naruszenie ochrony danych może spowodować wysokie ryzyko naruszenia praw lub wolności osoby fizycznej, administrator musi zawiadomić tę osobę o takim naruszeniu. Przepis nie tylko posługuje się nieostrym i ocennym pojęciem „wysokiego ryzyka", ale też przewiduje wyjątki od opisanej reguły. Każda taka sprawa będzie wymagała zatem stosownej oceny sytuacji dokonanej przez prawnika.

Przekazywanie danych osobowych do państwa trzeciego

Tego rodzaju przekazywanie danych podlega szczególnym rygorom i ograniczeniom, m.in. wymagane jest precyzyjne określenie podstawy prawnej przekazania.



Od 25 maja 2018 roku katalog tych podstaw ulega zmianom. Konieczne w związku z tym będzie przeprowadzenie, wraz z udziałem prawnika, przeglądu stosowanych obecnie podstaw przekazywania danych do państw trzecich, pod kątem ich prawidłowości i aktualności.

Wiodący organ nadzorczy

W konkretnych przypadkach spośród grup administratorów danych (np. działających w ramach jednej grupy kapitałowej) możliwe będzie wybranie jednego organu wiodącego spośród spośród organów ochrony danych osobowych działających w państwach członkowskich UE . Należy jednak zaznaczyć, że wyłonienie takiego organu nie umniejszy uprawnieniom i zakresowi zadań organów nadzorczych w poszczególnych państwach członkowskich.

Chodzi tu o rozwiązanie typu one–stop-shop, gdzie większość spraw dotyczy transgranicznego przetwarzania danych osobowych realizowanego w kilku państwach członkowskich EOG. Ogólne rozporządzenie UE przewiduje i reguluje szczegółowo zasady współpracy, w tym wzajemnej pomocy i wspólnych operacji organów nadzorczych z kilku państw członkowskich EOG.

Sankcje finansowe

Wprowadzenie ogólnoeuropejskiego uprawnienia do wymierzania wysokich kar finansowych przez organy nadzorcze ochrony danych osobowych jest jedną z najważniejszych i najbardziej przełomowych zmian przewidywanych przez Ogólne rozporządzenie UE. Tak jak już wspominaliśmy na wstępie, obecnie na terenie UE obowiązuje pewna niespójność w zakresie uprawnień do wymierzania kar finansowych za niezgodne z prawem przetwarzanie danych osobowych. Ustawodawstwa wielu krajów, np. Francji, przewidują uprawnienie do nakładania kar finansowych, a z drugiej strony organy nadzorcze krajów takich jak np. Polska są takiego uprawnienia pozbawione.

Do 24 maja 2016

Zgodnie z regulacjami UODO, GIODO nie może nakładać kar finansowych, aczkolwiek może nakładać grzywnę administracyjną w wysokości 50.000 zł w celu przymuszenia do wykonania wydanej przez niego decyzji administracyjnej.

Za wielokrotne niewykonywanie decyzji GIODO wysokość grzywny przymuszającej może wynieść maksymalnie 200.000 zł.

Od 25 maja 2016

W zależności od kategorii naruszenia przepisów Ogólne rozporządzenie UE przewiduje kary finansowe w wysokości:

- 10.000.000 EUR lub 2% całkowitego rocznego światowego obrotu przedsiębiorstwa, lub
- 20.000.000 EUR lub 4 % całkowitego rocznego obrotu przedsiębiorstwa,

przy czym w obu przypadkach zastosowanie znajdzie kwota wyższa.

Podsumowanie

Jak Państwo widzą, Ogólne rozporządzenie UE wprowadza szereg fundamentalnych zmian w zasadach przetwarzania danych osobowych. Jednak przede wszystkim Ogólne rozporządzenie UE wprowadza kolosalną zmianę w zakresie ryzyka związanego z przetwarzaniem danych osobowych co powoduje, iż znaczenie i waga tej dziedziny diametralnie wzrośnie.

Implementacja zmian w Państwa organizacji może okazać się procesem czasochłonnym i skomplikowanym, co rodzi potrzebę rychłego przystąpienia do działania tak, aby zdążyć przed datą wejścia w życie rozporządzenia - 25 maja 2018 r.

Zachęcamy Państwa do kontaktu celem omówienia potrzeb oraz przygotowania i przeprowadzenia tego złożonego i wielopłaszczyznowego procesu.

Domański Zakrzewski Palinka sp. k.
Rondo ONZ 1, 00-124 Warszawa
tel. +48 22 557 76 00
fax +48 22 557 76 01

ul. Paderewskiego 8, 61-770 Poznań
tel. +48 61 642 49 00
fax +48 61 642 49 50

ul. Gwiaździsta 66, 53-413 Wrocław
tel. +48 71 712 47 00
fax +48 71 712 47 50
www.dzp.pl