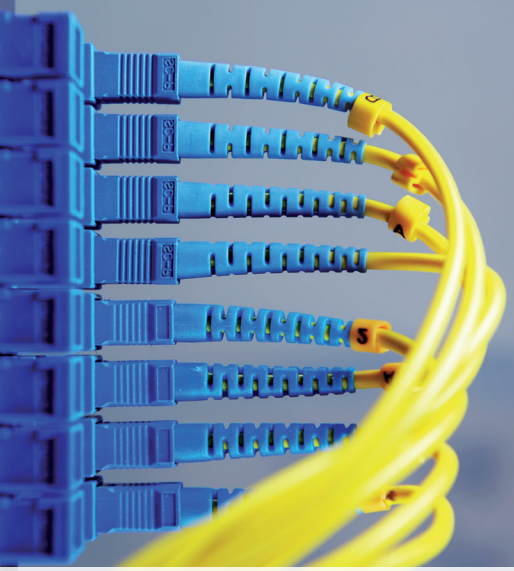


KPMG

Wsparcie w dostosowaniu do Unijnego Rozporządzenia o Ochronie Danych

USŁUGI POŚWIADCZAJĄCE

GDPR – nowe prawo w zakresie danych osobowych

Uchwalone i ogłoszone w 2016 r. rozporządzenie Parlamentu Europejskiej i Rady (UE) 2016/679 z dnia 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 (ang. General Data Protection Regulation, dalej GDPR), jest największą jak dotychczas zmianą w zakresie ochrony prywatności i danych osobowych.

GDPR jest ukierunkowane na ochronę danych osobowych „obywateli" UE (osób przebywających na terenie UE) we współczesnym świecie cyfrowym, jednocześnie ujednolicając przepisy dotyczące przetwarzania danych osobowych w całej Unii Europejskiej.

Odliczanie rozpoczęte – czas na zmiany tylko do 25.05.2018 r.

GDPR będzie mieć zastosowanie od 25 maja 2018 r.

Od dnia wejścia w życie (24.05.2016 r.) rozpoczęło się odliczanie okresu dwóch lat do stanu pełnej gotowości przypadającego na dzień 25.05.2018 r. Z tym dniem, zgodnie z zasadą rozliczalności, organizacje, do których GDPR ma zastosowanie, będą musiały stosować się do wymogów GDPR i jednocześnie być w stanie to wykazać.

Dlatego też już dziś należy podjąć działania przygotowujące organizację do GDPR.

Jakie najważniejsze zmiany wprowadza GDPR?

GDPR wprowadza wiele nowych wymogów, bądź znacząco zmienia istniejące w porównaniu do Dyrektywy 95/46/WE.

Zwracamy uwagę na najważniejsze aspekty wybranych nowych lub zmienionych wymogów.

Nowe wymogi dot. zgody

- Wymogi zostały znacząco zaostrzone.
- Należy zmienić ustawienia dotyczące uzyskiwania zgody zarówno na platformach jak i w formie papierowej czy cyfrowej.
- Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie oznaczają zgody.

Ochrona danych w fazie projektowania & domyślne ustawienia prywatności (ang. Privacy by Design & Default)

- Administrator już w fazie koncepcyjnej nowej usługi lub produktu zobowiązany jest uwzględniać ochronę danych (privacy by design), czego elementem jest także prywatność jako domyślne ustawienie (privacy by default), dobierając i wdrażając odpowiednie środki techniczne i organizacyjne. Takie podejście administrator ma zapewnić także w fazie realizacji i trwania nowego projektu biznesowego (przez cały okres procesu przetwarzania danych).

Ocena skutków dla ochrony danych (ang. Privacy Impact Assessments - PIA)

- Organizacje będą zobowiązane do dokonania PIA m.in. w przypadku istnienia dużego prawdopodobieństwa wysokiego ryzyka naruszenia praw lub wolności osób w związku z przetwarzaniem danych.
- Dodatkowo, jeśli PIA potwierdzi wysokie ryzyko, administrator przed przystąpieniem do przetwarzania danych powinien skonsultować jego warunki z organem nadzorczym.

Obowiązkowy Inspektor Ochrony Danych (IOD, ang. Data Protection Officer – DPO)

- Powołanie DPO jest konieczne m.in. przy przetwarzaniu szczególnych kategorii danych osobowych „na dużą skalę".
- DPO musi posiadać kwalifikacje zawodowe, na które składa się zarówno fachowa wiedza, jaki i umiejętności do wypełniania zadań DPO.
- GDPR nakazuje organizacjom zapewnić DPO status niezależności, dostarczyć niezbędne zasoby do realizacji danych, dostęp do danych i operacji przetwarzania, włączać we wszystkie sprawy dot. ochrony danych osobowych.

Obowiązek zawiadomienia o naruszeniu danych

- GDPR wprowadza obowiązek zawiadamiania o naruszenia danych do organu nadzoru w ciągu 72 godzin od stwierdzenia naruszenia.
- Ponadto, jeśli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia podmiot danych o takim naruszeniu.
- Naruszenia danych, niezależnie od ich rozmiaru lub wpływu, będą musiały być rejestrowane i udokumentowane w celu wykazania zgodności z rozporządzeniem GDPR.

Kary do 20 MLN lub do 4% rocznych obrotów grupy

- Nieprzestrzeganie zdefiniowanych obowiązków dla administratorów oraz przetwarzających dane może skutkować nałożeniem kary pieniężnej do 10 MLN EUR lub 2% obrotu rocznego (zależnie od tego która kwota będzie wyższa).
- Niezgodność z podstawowymi zasadami przetwarzania danych (na przykład warunków zgody), praw podmiotów danych, bądź mechanizmów transferu danych może skutkować nałożeniem kary pieniężnej do 20 MLN EUR lub 4% obrotu rocznego (zależnie od tego która kwota będzie wyższa).

Inne nowe wymogi to usystematyzowane zasady przetwarzania danych, w tym zasada rozliczalności, nowe prawa podmiotów danych – prawo do bycia zapomnianym, prawo do przenoszenia danych i ograniczenia przetwarzania danych, prawo sprzeciwu wobec profilowania.

!

Naruszenie wymogów GDPR może prowadzić do nałożenia bardzo wysokich kar, które do tej pory były w Polsce iluzoryczne. Dlatego odpowiednie wdrożenie wymogów w zakresie ochrony danych osobowych stało się kluczowe. Teraz jest czas na zmiany.

Jak się przygotować?

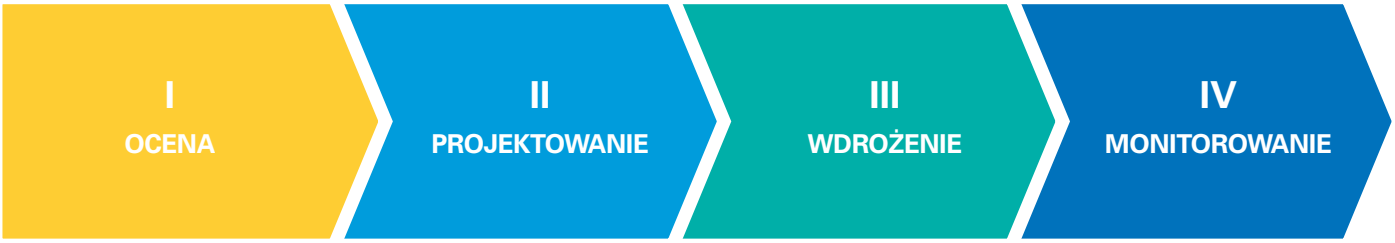
Ustalenie jak GDPR wpływa na Państwa organizację wymaga ocen gotowości do wymogów ochrony danych wynikających z GDPR. W tym celu KPMG posługuje się Systemem Zarządzania Ochroną Danych.

Schemat Zarządzania Ochroną Danych opiera się na następującym podejściu: (I) ocena, (II) projektowanie, (III) wdrożenie i (IV) monitorowanie.

Schemat zapewnia pragmatyczne i ustrukturyzowane podejście do ochrony danych osobowych w Państwa Organizacji.

Możemy pomóc Państwa organizacji w każdym aspekcie ochrony danych osobowych i przygotowań do wymogów GDPR.

W zależności od tego jak wygląda obecny poziom ochrony danych osobowych w Państwa organizacji, możliwe są różne usługi dostosowane do Państwa potrzeb i stanu gotowości obejmujące ocenę ryzyka, rozwiązania IT, doradztwo prawne:



© 2017 KPMG Advisory spółka z ograniczoną odpowiedzialnością sp. k. jest polską spółką komandytową i członkiem sieci KPMG składającej się z niezależnych spółek członkowskich stowarzyszonych z KPMG International Cooperative ("KPMG International"), podmiotem prawa szwajcarskiego. Wszelkie prawa zastrzeżone. Wydrukowano w Polsce.

© 2017 D.Dobkowski sp. k. jest kancelarią prawniczą stowarzyszoną z KPMG w Polsce.

	Usługi GDPR	Opis
ocena	**Szybka analiza luki GDPR**	Ocena oparta na kluczowych wymogach GDPR w porównaniu do Dyrektywy 95/46/WE oraz ustawy z 1997 r. Wynikiem tej oceny jest oszacowanie stanu gotowości do nowych wymogów GDPR, łącznie z odpowiednimi zaleceniami.
projektowanie	**Pełny Audyt Ochrony Danych**	Generalny audyt ochrony danych osobowych, którego celem jest ustalenie i ocena obecnych procesów przetwarzania danych i poziomu ochrony danych osobowych, a także analiza luki pod kątem nowych lub zmienionych wymogów GDPR, ustrukturyzowany wg. Systemu Zarządzania Ochroną Danych
	Opracowanie strategii przygotowań do GDPR	Opracowanie strategii przygotowań i stosowania GDPR zawiera projekt i harmonogram działań, wskazujących na środki, które należy wdrożyć celem przygotowań do wymogów GDPR. Strategia ma na celu usystematyzować podejście do działań przygotowujących i wdrażających GDPR.
wdrożenie	**Ocena wdrożonych rozwiązań GDPR**	Zalecana jako element usystematyzowanego podejścia do wdrożenia rozwiązań i środków spełniających wymogi GDPR w organizacji po ich wdrożeniu.
monitorowanie	**Okresowe monitorowanie zgodności**	Bieżące audyty w zakresie zgodności z GDPR, w celu potwierdzenia ciągłej zgodności z wymogami prawa.

W odniesieniu do każdego nowego wymogu wynikającego z GDPR, nasze wsparcie polegać może na:

analizach + **przygotowaniu narzędzi informatycznych** + **przygotowaniu porcedur, dokumentacji, rekomendacji** + **reprezentacji przed organem nadzorczym i sądem**

Przykładowe usługi dot. PIA

analiza potrzeby PIA + przeprowadzenie PIA + raport PIA + reprezentacja przed organem w ramach konsultacji

© 2017 KPMG Advisory spółka z ograniczoną odpowiedzialnością sp. k. jest polską spółką komandytową i członkiem sieci KPMG składającej się z niezależnych spółek członkowskich stowarzyszonych z KPMG International Cooperative ("KPMG International"), podmiotem prawa szwajcarskiego. Wszelkie prawa zastrzeżone. Wydrukowano w Polsce.

© 2017 D.Dobkowski sp. k. jest kancelarią prawniczą stowarzyszoną z KPMG w Polsce.

Jakie są korzyści?

Korzystając z usług KPMG Państwa organizacja może:

Ustalić i ocenić stan gotowości pod kątem nowych lub zmienionych standardów ochrony danych osobowych wynikających z GDPR. Audyt wskaże luki, przedstawi jasne i konieczne zalecenia dotyczące zmiany lub poprawy stanu ochrony danych.

Skorzystać ze sprawdzonego podejścia do ochrony danych. Nasz system zarządzania ochroną danych osobowych to pragmatyczne i elastyczne podejście, które pozwala skupić się na obecnych i nadchodzących wyzwaniach ochrony danych.

Zapewnić sobie dostęp do branżowych standardów ochrony danych i najlepszych praktyk branżowych stosowanych w całej UE.

Skorzystać z narzędzi do zarządzania ryzykiem i zgodnością dla celów oceny i monitorowania przestrzegania GDPR.

Korzystać z interdyscyplinarnego zespołu doradczego (prawnicy, specjaliści oceny ryzyka oraz od rozwiązań IT) specjalizującego się w ochronie danych.

Globalna obecność KPMG pozwala również na wdrażanie jednolitych standardów w Państwa organizacjach, równocześnie z uwzględnieniem uregulowań lokalnych.

Doradztwo KPMG wykracza poza zgodność z prawem, kładzie nacisk na ocenę, wdrażanie i monitorowanie odpowiednich środków kontroli ochrony danych osobowych.

Kontakt

KPMG Advisory spółka z ograniczoną odpowiedzialnością sp. k.
ul. Inflancka 4A
00-189 Warszawa
T: +48 22 528 11 00
F: +48 22 528 10 09
E: kpmg@kpmg.pl

D.Dobkowski sp. k.
ul. Inflancka 4A
00-189 Warszawa
T: +48 22 528 13 00
F: +48 22 528 13 09
E: legal@kpmg.pl

Krzysztof Radziwon
Partner
Usługi doradcze
Risk Consulting
T: +48 22 528 11 37
T: +48 508 047 500
E: kradziwon@kpmg.pl

Paweł Skowroński
Starszy menedżer
Usługi doradcze
Risk Consulting
T: +48 22 528 13 50
T: +48 664 718 627
E: pskowronski@kpmg.pl

Katarzyna Wojciechowska
Associate
Kancelaria prawna
T: +48 61 845 46 82
T: +48 691 197 582
E: kwojciechowska@kpmg.pl

Michał Wołoszczuk
Of counsel
Kancelaria prawna
T: +48 61 845 46 88
T: +48 603 988 951
E: mwoloszczuk@kpmg.pl

© 2017 KPMG Advisory spółka z ograniczoną odpowiedzialnością sp. k. jest polską spółką komandytową i członkiem sieci KPMG składającej się z niezależnych spółek członkowskich stowarzyszonych z KPMG International Cooperative ("KPMG International"), podmiotem prawa szwajcarskiego. Wszelkie prawa zastrzeżone. Wydrukowano w Polsce.

© 2017 D.Dobkowski sp. k. jest kancelarią prawniczą stowarzyszoną z KPMG w Polsce.

Dostępne w App Store

KPMG Poland

Zeskanuj kod, aby przejść do strony kpmg.pl