MARIAŃSKI
GROUP

E-BOOK

Łódź, marzec 2018r.

RODO
od 25 maja 2018 r.

Kancelaria Mariański Group
Łódź

MARIAŃSKI
GROUP

E-BOOK

INFORMACJE PODSTAWOWE

RODO czyli Rozporządzenie Parlamentu Europejskiego 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 weszło w życie 25 maja 2018 roku.

RODO ciężar ochrony danych dużo wyraźniej przerzuca na przedsiębiorcę z uwagi na podejście **oparte na ryzyku oraz neutralność technologiczną przepisów** - przy stosowaniu nowych przepisów niezbędne jest uwzględnianie:

- specyfiki działalności administratora,
- przedmiotu działalności,
- związku działalności z przetwarzaniem danych osobowych,
- wykorzystywanych w tym celu środków,
- skali i zakresu przetwarzania danych.

RODO oparto na założeniu aktywnej roli administratorów w doborze form i zakresu zabezpieczeń, przetwarzania oraz zgodności, dostosowaniu zabezpieczeń do specyfiki danego biznesu, w tym do branży i do rozmiaru prowadzonej działalności – wymuszając staranną analizę i dobór adekwatnych środków ochrony.

RODO będzie miało zatem wpływ na działalność przedsiębiorstw, szczególną uwagę na nowe przepisy zwrócić będą musiały podmioty prowadzące sprzedaż online. Prawidłowe przetwarzanie danych osobowych ma o tyle szczególne znaczenie, że naruszenie przepisów RODO skutkować może nie tylko bardzo wysokimi karami finansowymi, może też wiązać się z odpowiedzialnością karną.

MARIAŃSKI
GROUP

E-BOOK

DANE OSOBOWE

Dane osobowe, to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Identyfikacja ta może mieć miejsce w szczególności na podstawie identyfikatora takiego jak:

- imię i nazwisko,
- numer identyfikacyjny (np. NIP, REGON, PESEL, numer klienta),
- dane o lokalizacji,
- identyfikator internetowy (w tym adresy IP oraz identyfikatory plików cookie, identyfikatory generowane np. przez etykiety RFID)
- szczególne czynniki określające fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość tej osoby.

Nie jest istotne czy dane te dotyczą życia prywatnego i rodzinnego podmiotu, czy podejmowanej działalności zawodowej, ekonomicznej lub społecznej, o ile umożliwiają jej identyfikację.

PRZETWARZANIE DANYCH OSOBOWYCH

Każda operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych. W pojęciu przetwarzania danych mieści się m.in.:

zbieranie	utrwalanie	organizowanie
porządkowanie	przechowywanie	opracowywanie
zmienianie	przekazywanie	udostępnianie
rozpowszechnianie	usuwanie	

MARIAŃSKI
GROUP

E-BOOK

W zależności od charakteru i rodzaju prowadzonej przez dany podmiot działalności gospodarczej, przetwarzanie będzie polegało na wszelkich działaniach na danych osobowych. Na przykład na realizacji zamówień, kontroli i prowadzeniu sprzedaży, prowadzeniu dokumentacji pracowniczej i księgowej.

W sprzedaży e-commerce - sprzedaż online – poza powyższym możemy mieć do czynienia z przetwarzaniem danych będą m.in. takie działania jak:

- przechowywanie danych osobowych w ramach usługi hostingu,
- zapisywanie danych osobowych w chmurze obliczeniowej (cloud computing),
- prowadzenie newsletterów,
- zbieranie danych niezbędnych do wysyłki towaru,
- prowadzenie fanpage'a na profilach społecznościowych

LEGALNE PRZETWARZANIE DANYCH

Podejmowanie działań na danych osobowych (ich przetwarzanie) jest zgodne z prawem, wyłącznie w przypadkach, gdy spełniona jest jedna z przesłanek legalizacyjnych, taka jak**:**

1. **zgoda** osoby, której dane dotyczą, na przetwarzanie jej danych osobowych w jednym lub większej liczbie określonych celów – np. zgoda na przesłanie newslettera,
2. przetwarzanie w zakresie **niezbędnym do wykonania umowy** lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy – np. na wysyłkę towaru pod określony adres,
3. przetwarzanie w zakresie **niezbędnym do wypełnienia obowiązku prawnego** ciążącego na administratorze – np. wystawianiu faktur

W szczególnych wypadkach mogą wystąpić inne przesłanki legalizacyjne.

MARIAŃSKI
GROUP

E-BOOK

PRZYKŁAD

Podstawą do udzielenia odpowiedzi na zadane przez potencjalnego klienta przez formularz kontaktowy pytanie o dostępność produktu, będzie przesłanka podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. Z kolei, przetwarzanie danych osobowych, w tym danych adresowych, w celu przesłania zamówionych produktów, spełni przesłankę działań niezbędnych do wykonania umowy.

W takiej sytuacji nie jest konieczne uzyskanie zgody na przetwarzanie danych, o czym podmioty prowadzące sprzedaż online często zapominają.

Zgoda taka będzie z kolei niezbędna do wysyłania informacji handlowych – newsletteru, reklam, ofert promocyjnych i rabatowych.

Z punktu widzenia legalności działania, jak i uproszczenia stosowanych procedur, tak duże znaczenie ma znajomość podstaw przetwarzania danych i ich prawidłowe stosowanie.

CZYM JEST ZGODA?

Zgoda to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

SZCZEGÓLNE KATEGORIE DANYCH

Przy omawianiu zasad przetwarzaniu danych osobowych należy brać pod uwagę specyficzne branże np. w branży farmaceutycznej i medycznej, z uwagi na ich przynależność do sektora ochrony zdrowia i przetwarzanie w jej obrębie danych szczególnie intymnych, należy zwrócić uwagę na wydzielenie w RODO szczególnych kategorii danych.

MARIAŃSKI
GROUP

E-BOOK

PRZETWARZANIE DANYCH WRAŻLIWYCH

Przetwarzanie tych najbardziej wrażliwych danych zmienia przesłanki legalności przetwarzania danych i obowiązki związane z tym przetwarzaniem. Szczególne kategorie danych osobowych to takie, które ujawniają:

1) pochodzenie rasowe lub etniczne,
2) poglądy polityczne,
3) przekonania religijne lub światopoglądowe,
4) przynależność do związków zawodowych
5) dane genetyczne,
6) dane biometryczne (w celu jednoznacznego zidentyfikowania osoby fizycznej)
7) dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby.

Przetwarzanie takich danych jest **co do zasady zabronione,** jednak jedną z okoliczności znoszących stosowanie tego zakazu jest niezbędność przetwarzania danych m.in. do celów zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego.
Uprawnienie do przetwarzania danych sensytywnych w oparciu o tę przesłankę dotyczy lekarzy, lekarzy dentystów, pielęgniarek, położnych, fizjoterapeutów oraz diagnostów laboratoryjnych, a także farmaceutów, gdyż przez pojęcie „usługi medyczne" rozumie się także zaopatrywanie pacjentów w leki.

OBOWIĄZKI ADMINISTRATORA DANYCH

Administrator danych osobowych samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
Dla administratorów wejście w życie RODO wiąże się z szeregiem obowiązków. Niektóre z nich są powieleniem tych istniejących dotychczas, część z nich jest novum. Niektóre nałożone są przez Rozporządzenie wprost, niektóre zaś wynikają pośrednio z praw przyznanych podmiotom, których dane są przetwarzane.

MARIAŃSKI GROUP

E-BOOK

Administrator powinien zapewnić podmiotowi danych informacje w zakresie m.in.:

- tożsamości administratora,
- danych kontaktowych,
- celów przetwarzania i podstawy prawnej,
- odbiorców lub kategorii odbiorców,
- okresu przetwarzania danych,
- kategorii danych,
- profilowania,
- transferu danych do państw trzecich (poza Europejski Obszar Gospodarczy)
- praw podmiotu danych (w tym o prawie do cofnięcia zgody, przenoszenia danych czy wniesienia skargi do organu nadzorczego).

OSTRZEŻENIE!

Informacje udzielane powinny być osobie, której dane dotyczą, jasnym i prostym językiem oraz powinny mieć zwięzłą, przejrzystą, zrozumiałą i łatwo dostępną formę – nie powinny być pisane językiem specjalistycznym, w szczególności żargonem prawniczym.

OBOWIĄZKI ORGANIZACYJNE ADMINISTRATORA DANYCH

Obowiązkiem administratora danych jest wdrażanie odpowiednich środków technicznych i organizacyjnych w celu ochrony przetwarzania danych.

Na to jakie dokładnie działania musi podjąć wpływa m.in.:
charakter danych → zakres przetwarzania → kontekst przetwarzania → cel przetwarzania → ryzyko naruszenia praw i wolności → waga zagrożenia

MARIAŃSKI
GROUP

E-BOOK

Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Na administratorze ciąży obowiązek utrzymania bezpieczeństwa przetwarzania i zapobieganie naruszaniu przepisów RODO w zakresie adekwatnym do ryzyka związanego z przetwarzaniem w jego firmie.

Środki, jakie powinien uwzględnić administrator danych to m.in.

1) pseudonimizacja
2) szyfrowanie danych osobowych,
3) zdolność do ciągłego zapewnienia poufności,
4) integralności, dostępności i odporności systemów i usług przetwarzania,
5) zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich w razie incydentu fizycznego lub technicznego
6) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Podstawowym obowiązkiem, wyrażonym wprost w RODO, jest:

1) uwzględnianie ochrony danych już w fazie projektowania (*privacy by design*) - kwestia ochrony prywatności musi stanowić jeden z elementów branych pod uwagę w trakcie decydowania o podejmowanej działalności gospodarczej
2) realizacja zasady domyślnej ochrony danych (*privacy by default*) - obowiązek skonfigurowania działań przedsiębiorstwa w ten sposób, że zapewniona była domyślna ochrona danych osobowych w maksymalnym zakresie

Przykład Privacy by design

Przy wyborze dostawcy usług hostingowych do prowadzenia sklepu internetowego, przedsiębiorca powinien uwzględnić na równi: cenę, funkcjonalność, ale też możliwość zapewnienia realizacji obowiązków wynikających z RODO.

MARIAŃSKI
GROUP

E-BOOK

Przykład privacy by default
Przedsiębiorca powinien ograniczyć okres przechowywania danych do minimum wyznaczonego przez przepisy prawa – szczególnie przez przepisy dotyczące przedawnienia.

OBOWIĄZKI DOKUMENTACYJNE

Kluczowe znaczenie ma prowadzenie **rejestru czynności przetwarzania**, który powinien obejmować oprócz danych administratora m.in.

- cele przetwarzania danych,
- opis kategorii osób, których dane dotyczą oraz kategorii danych ich dotyczących,
- informację o planowanych terminach usunięcia poszczególnych kategorii danych
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Przed przygotowaniem takiego rejestru administrator powinien przeanalizować, jakich czynności przetwarzania dokonuje oraz z jakimi celami są one związane, np. pozyskiwaniem klientów, sprzedażą w ramach prowadzonego sklepu internetowego, marketingiem e-mailowym czy z zatrudnianiem pracowników.

OBOWIĄZEK DOKONANIA OCENY SKUTKÓW PLANOWANYCH OPERACJI

Administrator powinien ponadto, w przypadku, gdy operacje przetwarzania stwarzają z dużym prawdopodobieństwem wysokie ryzyko naruszenia praw i wolności osób fizycznych, **dokonać oceny skutków planowanych operacji przetwarzania** dla ochrony danych osobowych

OBOWIĄZKI ZWIĄZANE Z POWIERZENIEM DANYCH

Administrator może powierzyć przetwarzanie danych w całości lub w części wyspecjalizowanym podmiotom zewnętrznym w zakresie:

1) usług hostingowych
2) usług i aplikacji ERP, CRM, CMS
3) obsługi kadrowo-płacowej
4) usług biura rachunkowego.

Podmioty zewnętrzne mają styczność z danymi osobowymi administrowanymi przez zleceniodawcę - administrator jest zobowiązany korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

UMOWA POWIERZENIA PRZETWARZANIA

Umowa z podmiotem przetwarzającym powinna być zawarta w formie pisemnej lub elektronicznej i określać:

1) przedmiot,
2) charakter i cel przetwarzania,
3) czas przetwarzania,
4) kategorie osób, których dane dotyczą,
5) rodzaj danych osobowych,
6) obowiązki stron umowy,
7) zobowiązanie procesora do przetwarzania danych osobowych wyłącznie na polecenie administratora,
8) zapewnienia, że osoby upoważnione do przetwarzania danych osobowych zostaną zobowiązane do zachowania tajemnicy,
9) wdrożenie odpowiednich środków technicznych i organizacyjnych,
10) umożliwienie przeprowadzenia audytów u procesora,
11) współdziałanie z administratorem,
12) kwestie związane z dalszym powierzeniem.

MARIAŃSKI
GROUP

E-BOOK

OSTRZEŻENIE!

W związku z wprowadzeniem przez RODO wielu nowych obligatoryjnych elementów umowy powierzenia, większość dotychczasowych umów zawartych z procesorami będzie wymagała dostosowania do wymogów RODO.

OBOWIĄZEK POWOŁANIA INSPEKTORA DANYCH OSOBOWYCH

Administrator danych zobowiązanych jest do wyznaczenia Inspektora Ochrony Danych (IOD) m.in. gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych albo danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Większość podmiotów prowadzących działalność gospodarczą dokonuje przetwarzania danych osobowych. Również sklepy internetowe nie mogą skutecznie prowadzić sprzedaży wysyłkowej, bez przetwarzania danych osobowych klientów. Zatem każdy prowadzący działalność powinien szczegółowo przeanalizować te przesłanki i zastanowić się, czy przetwarzanie przez niego danych osobowych nie będzie skutkować obowiązkiem wyznaczenia inspektora danych osobowych.

OBOWIĄZKI ZWIĄZANE Z NARUSZENIEM ZASAD PRZETWARZANIA

Naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

1) zniszczenia,
2) utracenia,
3) zmodyfikowania,
4) nieuprawnionego ujawnienia,
5) nieuprawnionego dostępu,
6) do danych osobowych.

pociąga za sobą odpowiednie obowiązki:

1) prowadzenia dokumentacji wszelkich naruszeń ochrony danych osobowych,
2) zgłoszenia w ciągu 72 godzin do organu nadzorczego (prezesa Urzędu Ochrony Danych Osobowych, który zastąpi Generalnego Inspektora Ochrony Danych Osobowych) – chyba, że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,
3) poinformowania podmiotu, którego dane przetwarzamy – gdy naruszenie może powodować powstanie wysokiego ryzyka dla praw i wolności tego podmiotu.

PRZYKŁAD

Nie trzeba informować PUODO w sytuacji, gdy utracony zostanie nośnik z danymi osobowymi (np. dysk twardy zawierający backup systemu komputerowego apteki), jednak dane te były poddane pseudonimizacji, a klucz do przypisania danych konkretnym osobom, znajduje się osobno i jest odpowiednio zabezpieczony.

ZASADA ROZLICZALNOŚCI

Na wykonywanie opisanych powyżej obowiązków wpływ będzie miała również zasada rozliczalności, zgodnie z którą administrator jest zobowiązany do udowodnienia wykonania nałożonych na niego obowiązków i realizacji zasad przetwarzania wskazanych w RODO.

Prawodawca unijny kierował się chęcią odformalizowania procesów z zakresu ochrony danych osobowych, dlatego nakładając na administratorów kolejne obowiązki, nie wskazywał co do zasady formy ich wykonania.

W związku z tym, to na administratorze ciąży dobór odpowiednich środków umożliwiających udowodnienie zarówno w toku kontroli, jak i na wezwanie osoby, której dane dotyczą, realizację założeń RODO.

MARIAŃSKI
GROUP

E-BOOK

KARY

Naruszenie przepisów RODO może pociągnąć za sobą kosztowne konsekwencje w postaci wysokich kar administracyjnych.

RODO wprowadza wysokie limity kar i wskazuje 2 progi (do 10 milionów EUR, a w przypadku przedsiębiorstwa – do 2 % wartości rocznego światowego obrotu przedsiębiorstwa oraz do 20 milionów EUR, a w przypadku przedsiębiorstwa – do 4 % obrotu), uzależniając ich stosowanie od rodzaju zaistniałych naruszeń.

Surowszej karze podlegać będą:

- naruszenia podstawowych zasad przetwarzania danych,
- brak podstawy prawnej do przetwarzania,
- wadliwie odebrana zgoda,
- niewykonanie obowiązku informacyjnego,
- niezapewnienie prawa dostępu do danych osobowych,
- nieusunięcie lub niesprostowanie danych
- niezapewnienie realizacji prawa do przenoszenia danych i ograniczenia przetwarzania.

CO TRZEBA ZROBIĆ?

Przy tak dotkliwych skutkach wadliwego obchodzenia się z danymi osobowymi niezwykle istotnym jest odpowiednie przygotowanie przedsiębiorstwa na działalność zgodną z nowymi przepisami.

Wprowadzone zmiany powinny dotyczyć:

1) sposobu realizacji nowych praw osób, których dane są przetwarzane
2) współpracy z organem nadzoru – prezesem Urzędu Ochrony Danych Osobowych
3) zarządzania ryzykiem.

MARIAŃSKI
GROUP

E-BOOK

Przy wdrażaniu nowych mechanizmów ochrony danych osobowych szczególnie istotne jest:

1) dostosowanie z wyprzedzeniem systemów nadzoru oraz zarządzania danymi,
2) analiza prowadzonych procesów marketingowych oraz reklamy,
3) zapewnienie i wykazanie zgodności z zasadą *privacy by design* oraz zasadą *privacy by defauly*,
4) Zapewnienie stałego przeglądu i inwentaryzacji danych,
5) Opracowanie i wdrożenie polityki bezpieczeństwa wraz z odpowiednią dokumentacją.
6) Przeszkolenie pracowników, w celu prawidłowego stosowania wprowadzonych procedur.

CZY JESTEŚ GOTOWY NA RODO?

Poniżej znajduje się kilka pytań, które pozwolą ustalić, czy firma gotowa jest na RODO – jeśli na którekolwiek z nich odpowiesz „NIE", oznacza to, że czeka Twoją firmę jeszcze wiele pracy.

1. Czy odpowiadają Państwo na żądania udzielenia informacji o przetwarzaniu, żądania sprostowania danych, żądania usunięcia danych, sprzeciwy wobec przetwarzania danych, lub inne zapytania związane z przetwarzaniem danych w terminie miesiąca?

MARIAŃSKI
GROUP

E-BOOK

2. Czy istniejące procedury przewidują, że administrator na żądanie osoby, której dane dotyczą:

A. czasowo przenosi wybrane dane do innego systemu przetwarzania,

B. odbiera użytkownikom uprawnienia dostępowe do wybranych danych na określony czas,

C. czasowo usuwa opublikowane dane ze strony internetowej,

D. w zautomatyzowanych procesach ogranicza środkami technicznymi przetwarzanie w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane,

E. ogranicza przetwarzanie w inny sposób?

3. Czy została opracowana polityka ochrony danych zgodna z RODO?

4. Czy opracowano standardy postępowania w przypadku wdrażania nowych procesów przetwarzania danych lub nowych systemów informatycznych do przetwarzania danych osobowych?

5. Czy posiadają Państwo ustalone kryteria wyboru procesora pod kątem tego, czy zapewnia on – dla danego procesu przetwarzania – wdrożenie środków technicznych i organizacyjnych, aby przetwarzanie było zgodne z RODO?

6. Czy stosując środki techniczne i organizacyjne w celu zapewnienia odpowiedniego stopnia bezpieczeństwa danych osobowych uwzględniany jest charakter, zakres, kontekst i cel przetwarzania oraz ryzyko naruszenia praw lub wolności osób, których dane dotyczą?

7. Czy opracowano procedury dokonywania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (DPIA), w przypadku gdy dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych?

8. Czy dla każdego procesu przetwarzania danych istnieje podstawa prawna przetwarzania danych?

MARIAŃSKI
GROUP

E-BOOK

9. Czy przetwarzają Państwo lub mają Państwo zamiar przetwarzać dane zebrane w ramach tego procesu w celu innym niż w tym, dla którego dane zostały pierwotnie zebrane, np. dla celów marketingu?

10. Czy wdrożono procedury zapewniające, iż dane osobowe są przetwarzane jedynie tak długo, jak długo istnieje jednocześnie podstawa prawna oraz cel dla ich przetwarzania? Czy przewidziano okresy przechowywania danych dla poszczególnych kategorii danych?

11. Czy są Państwo w stanie zidentyfikować każdą osobę, która wyraziła zgodę na przetwarzanie jej danych osobowych (np. przez jej imię i nazwisko, adres email, inny identyfikator)?

12. Czy w ramach prowadzonej strony internetowej dochodzi do profilowania na podstawie danych osobowych i wyświetlania spersonalizowanych treści (np. dobieranie sugestii produktów na podstawie oglądanych wcześniej produktów)?

13. Czy dane osobowe są przekazywane poza Europejski Obszar Gospodarczy – np. do Szwajcarii, Chin?

Uprzejmie prosimy abyście Państwo potraktowali niniejszy materiał jako informacyjny i nie mający charakteru opinii lub porady prawnej.

W razie jakichkolwiek pytań lub wątpliwości zapraszamy Państwa do kontaktu z Kancelarią:
kancelaria@marianskigroup.pl

Osoba kontaktowa ws. związanych z przetwarzaniem danych osobowych oraz wdrożeniem RODO: Mecenas Bartosz Rodak
brodak@marianskigroup.pl

Informacje o bieżącej działalności Kancelarii, zakresie praktyki oraz wszystkie alerty możecie znaleźć Państwo na naszej stronie internetowej:
www.marianskigroup.pl