Monika Wycykał

Jak wdrożyć RODO?

WYTYCZNE NA POTRZEBY WDROŻENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

Opracowanie przygotowała Monika Wycykał

www.ePorady24.pl

Kraków 2018

Fragment w wersji: 1.07 (10 lutego 2018 r.)

Szanowni Państwo,

25 maja 2018 r. wchodzi w życie rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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 (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L z dnia 4 maja 2016 r.), popularnie określane jako „RODO". Jest to akt prawny, który wprowadza jednolite przepisy dotyczące ochrony danych osobowych w całej Unii Europejskiej i bez wątpienia są to rewolucyjne zmiany w tym zakresie.

Aby przystąpić do wdrażania systemu ochrony danych osobowych u Państwa zgodnie z wymogami RODO, pierwszym warunkiem — i to warunkiem koniecznym — jest zmiana sposobu myślenia o ochronie danych osobowych. Dotychczas wiele podmiotów nie przywiązywało wagi do tych kwestii, ponieważ nie było realnych sankcji. Od maja 2018 r. zagadnienie to nie powinno być marginalizowane i należy traktować je poważnie, by uniknąć kar pieniężnych mogących sięgać wielu milionów złotych. Ochrona danych osobowych musi stanowić ważny element prowadzonej działalności, zwłaszcza u tych podmiotów, które przetwarzają wiele informacji o osobach fizycznych.

Budowa systemu danych osobowych zgodnego z RODO nie może ograniczyć się do zlecenia prawnikowi sporządzenia dokumentacji — tworzenie dokumentacji jest etapem OSTATNIM, a nie pierwszym. Wynika to stąd, że prawodawca unijny nie narzucił administratorom danych osobowych żadnego sztywnego modelu ochrony danych osobowych, do którego należy dostosować się w każdej organizacji. Wręcz przeciwnie, rewolucja w myśleniu o ochronie danych osobowych wyraża się między innymi w tym, że podmioty zobowiązane uzyskają dużą swobodę w kształtowaniu swojego własnego systemu ochrony danych osobowych — byle odpowiadał on zasadom zawartym w RODO i co najważniejsze, był skuteczny[1].

W związku z powyższym aby należycie zbudować taki system, konieczne staje się po pierwsze, bardzo dokładne przeanalizowanie przez Państwa rodzajów przetwarzanych danych osobowych, sposobów i celów ich przetwarzania, stosowanych rozwiązań, po drugie, realne wdrożenie systemu ochrony danych osobowych, jaki będzie u Państwa funkcjonował od 25 maja 2018 r. Stąd też nie obędzie się chociażby bez konsultacji z informatykami, którzy na przykład wskażą Państwu sposoby zabezpieczeń czy też zmodyfikują dotąd wykorzystywane systemy informatyczne.

Niniejsze Wytyczne mają za zadanie ułatwić Państwu powyższe działania i pomóc je usystematyzować. Stworzenie jakiejkolwiek dokumentacji jest możliwe dopiero po wdrożeniu zaprojektowanych rozwiązań i ich szczegółowym opisaniu — dokumentacja absolutnie nie może opierać się na fikcji.

[1] „Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane" — art. 24 ust. 1 RODO.

Należy pamiętać, że nie muszą się Państwo dostosowywać do wszystkich przedstawionych wytycznych (np. jeżeli nie chcą Państwo pseudonimizować zbiorów, to nie ma takiego wymogu), z wyjątkiem obowiązków bezwzględnie narzuconych przez RODO, ponieważ jest oczywistym, że system ochrony danych osobowych wprowadzony np. w warsztacie samochodowym będzie inny niż system ochrony danych osobowych w banku czy towarzystwie ubezpieczeniowym. Dlatego to Państwo we własnym zakresie decydują o wdrażanych rozwiązaniach, przy czym należy pamiętać, że ponoszą Państwo odpowiedzialność prawną za to, aby te rozwiązania były wystarczające i adekwatne do wykonywanej działalności. Będzie to podlegało kontroli ze strony Prezesa Urzędu Ochrony Danych Osobowych, który zastąpi dotychczasowego Generalnego Inspektora Ochrony Danych Osobowych.

Założenia, które Państwo opracują w oparciu o poniższe Wytyczne, powinny mieć charakter oficjalnego dokumentu, ponieważ mogą zostać one włączone do Państwa dokumentacji stworzonej na potrzeby RODO (dla udowodnienia, że administrator przeprowadził rzetelny audyt i przemyślał własne rozwiązania). Stąd też nie należy się ograniczać do jednowyrazowych odpowiedzi na pytania wskazane w Wytycznych, lecz tam, gdzie to wskazane, warto zamieścić jak najszerszy opis (dotyczy to zwłaszcza rozwiązań o charakterze technicznym).

Na końcu znajdą Państwo listę kontrolną, pozwalającą nadzorować realizację czynności opisanych szczegółowo w treści Wytycznych.

Mam nadzieję, że Wytyczne okażą się dla Państwa pomocne i pozwolą przygotować się w należyty sposób do zmian, jakie wprowadzi RODO.

Powodzenia!
doradca prawny Monika Wycykał
Zespół ePorady24.pl
www.eporady24.pl

Opis podmiotu

Imię i nazwisko/Nazwa: ……

Forma prawna: ……..

NIP: ……..

REGON: ……...

KRS: ……..

Adres: ……

Liczba zatrudnionych pracowników[2]: ……...

Charakterystyka działalności: ……

……..

……..

…….

[2] Ta informacja jest konieczna, ponieważ niektóre obowiązki z RODO nie dotyczą podmiotów zatrudniających określoną liczbę pracowników

DZIAŁ I: KWESTIE PODSTAWOWE

1. Osoby zaangażowane w proces przetwarzania danych osobowych

RODO nakłada obowiązki związane z ochroną danych osobowych nie tylko na administratora danych, ale również inne podmioty, które współpracują z administratorem.

W ramach pierwszego kroku trzeba zidentyfikować wszystkie osoby, jakie mogą być zaangażowane w proces przetwarzania danych osobowych u Państwa, aby przed wejściem w życie RODO ustalić z nimi zasady współpracy w przedmiocie ochrony danych osobowych.

1.1. Administrator i współadministrator danych osobowych

„Administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.

Jeżeli w Państwa przypadku będzie występował współadministrator lub współadministratorzy danych osobowych, proszę podać jego lub ich dane:

Imię i nazwisko/Nazwa: ……
Forma prawna: ……..
NIP: ……..
REGON: ……...
KRS: ……..
Adres: ……

1.2. Osoba upoważniona do przetwarzania danych osobowych

„Osoba upoważniona do przetwarzania danych osobowych" oznacza osobę podporządkowaną administratorowi danych osobowych i mającą dostęp do danych osobowych za jego wiedzą i zgodą. Innymi słowy, chodzi przede wszystkim o osobę, która pozostaje w strukturze organizacyjnej administratora, ponieważ jest np. pracownikiem, wykonawcą umowy o dzieło, zleceniobiorcą, i nad którą administrator może sprawować bezpośrednią kontrolę. Każda z tych osób powinna co do zasady dysponować formalnym upoważnieniem administratora, najlepiej wyrażonym na piśmie i określającym zakres upoważnienia.

Wykaz osób upoważnionych u Państwa wraz z zakresem upoważnień:

Lp.	Imię i nazwisko	Podstawa upoważnienia	Cel upoważnienia	Zbiory danych, które obejmuje upoważnienie

1.3. Inspektor ochrony danych

Przepisy RODO przewidują w pewnych sytuacjach obligatoryjne wyznaczenie przez administratora danych osobowych kogoś, kto będzie pełnił funkcję inspektora ochrony danych (IOD). Oprócz tego każdy administrator może dobrowolnie wyznaczyć IOD, np. po to, aby usprawnić zarządzanie systemem danych osobowych w firmie lub zyskać dodatkowy środek obrony w trakcie kontroli prowadzonej przez Prezesa Urzędu Ochrony Danych Osobowych.

Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:
a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
b) główna działalność administratora lub podmiotu przetwarzającego 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; lub

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych (danych wrażliwych), oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.

Szerzej na temat IOD:
https://www.eporady24.pl/inspektor_ochrony_danych,artykuly,17,233,1591.html

Powinni Państwo zatem przeanalizować, czy w Państwa przypadku zachodzi konieczność obowiązkowego wyznaczenia IOD, a jeżeli nie, to czy planują Państwo dobrowolne wyznaczenie IOD.

IOD będzie/nie będzie wyznaczony, ponieważ……
……..
…….

Opis wyznaczania IOD-a:
…….
…….
…….
…….
…….

1.4. Podmiot przetwarzający

„Podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Chodzi tutaj o sytuację, gdy administrator przekazuje innemu podmiotowi posiadane przez siebie dane osobowe, a podmiot przetwarzający wykonuje pewne operacje na tych danych — na polecenie administratora oraz w zakresie przez niego wskazanym. Przykład: zlecenie obsługi kadrowo-płacowej biuru rachunkowemu (biuro rachunkowe przetwarza dane osobowe kontrahentów i pracowników administratora), zlecenie obsługi informatycznej firmie IT (firma IT przetwarza np. dane w systemach informatycznych należące do administratora), zlecenie przeprowadzenia kampanii mailingowej agencji reklamowej (agencja reklamowa przetwarza np. bazę e-maili klientów administratora).

Wykaz podmiotów przetwarzających, z którymi Państwo współpracują lub będą współpracować:

1) Imię i nazwisko/Nazwa: …….
   Forma prawna: ……..
   NIP: ……..
   REGON: …….....
   KRS: …….
   Adres: ……

2) Imię i nazwisko/Nazwa: …….
   Forma prawna: ……..
   NIP: ……..
   REGON: …….....
   KRS: …….
   Adres: ……

3) Imię i nazwisko/Nazwa: …….
   Forma prawna: ……..
   NIP: ……..
   REGON: …….....
   KRS: …….
   Adres: ……

1.5. Odbiorca danych osobowych

„Odbiorca danych osobowych" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe. Każdy podmiot przetwarzający jest odbiorcą danych osobowych, ale nie każdy odbiorca danych osobowych jest podmiotem przetwarzającym. Najważniejszą cechą odróżniającą jest to, czy podmiot, któremu ujawnia się dane, przetwarza je w imieniu i na polecenie administratora danych osobowych. Przykład: jeżeli przedsiębiorca powierza firmie windykacyjnej ściągnięcie długu w jego imieniu, to firma windykacyjna będzie podmiotem przetwarzającym — a zarazem odbiorcą. Jeżeli natomiast

przedsiębiorca sprzedaje dług firmie windykacyjnej, to będzie ona tylko odbiorcą danych osobowych, ale już nie podmiotem przetwarzającym.

Wykaz indywidualnych odbiorców danych osobowych lub ich kategorii u Państwa (o ile są znani):

1) Imię i nazwisko/Nazwa: …….
   Forma prawna: ……..
   NIP: ……..
   REGON: …….....
   KRS: …….
   Adres: ……

2) Imię i nazwisko/Nazwa: …….
   Forma prawna: ……..
   NIP: ……..
   REGON: …….....
   KRS: …….
   Adres: ……

3) Imię i nazwisko/Nazwa: …….
   Forma prawna: ……..
   NIP: ……..
   REGON: …….....
   KRS: …….
   Adres: ……

Kategorie odbiorców danych osobowych:

a) ……;
b) ……;
c) ……;
d) ……;
e) …….

KONIEC DARMOWEGO FRAGMENTU

W pełnej wersji znajdziesz szczegółowe wytyczne, które należy przeanalizować (zwykle z wszystkimi działami w firmie oraz informatykiem) oraz uzupełnić, aby określić zakres niezbędny do prawidłowego przygotowania dokumentacji RODO.

Pełna wersja opracowania ma 80 stron i podzielona jest na kilka działów:

Dział I: Kwestie podstawowe
Dział II: Pracownicy
Dział III: Realizacja obowiązków Administratora Danych Osobowych
Dział IV: Procedury wewnętrzne Administratora Danych Osobowych
Dział V: Rejestry i ewidencje
Dział VI: Środki bezpieczeństwa

Na końcu znajduje się Lista kontrolna, która pomoże w samodzielnym uświadomieniu sobie zakresu koniecznych prac oraz określeniu terminu wdrożenia konkretnych czynności dotyczących wdrożenia RODO we własnej firmie.

Jak zamówić pełną wersję?

Aby złożyć zamówienie na nasze opracowanie pt. *Jak wdrożyć RODO? Wytyczne na potrzeby wdrożenia systemu ochrony danych osobowych* prosimy przejść do formularza na stronie:

http://www.ePorady24.pl/p.html

i w treści wpisać **RODO OPRACOWANIE** (i podać swoje dane).
Pełna wersja opracowania kosztuje 327 zł.

Jeśli zakupią Państwo opracowanie Jak wdrożyć RODO?, a następnie zlecą nam sporządzenie dokumentacji RODO – otrzymają Państwo zniżkę. Cena usługi zostanie pomniejszona o kwotę zapłaconą za Wytyczne.