RODO w spółkach

- jak przygotować się do nowych unijnych przepisów o ochronie danych

experto24.pl

Spis treści

Rozporządzenie Parlamentu Europejskiego i Rady (UE) z 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 osobowych, RODO) zacznie być stosowane od 25 maja 2018 r. Kilka miesięcy, jakie pozostały do tego czasu, spółki powinny w szczególności wykorzystać na przygotowanie się do wypełniania nowych obowiązków wynikających z tego rozporządzenia. Trzeba bowiem pamiętać, że podmioty prywatne będą musiały się liczyć z karą finansową w wysokości nawet do 20 mln euro lub 4% swojego światowego obrotu za naruszenie przepisów ogólnego rozporządzenia o ochronie danych.

Jakie obowiązki będzie miał administrator zgodnie z RODO

W RODO pojęcie „administrator danych" zostało zastąpione pojęciem „administrator". Jest nim osoba fizyczna lub prawna, urząd publiczny, agenda lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych. W przypadku spółki administratorem

będzie spółka reprezentowana przez prezesa. Do podstawowych obowiązków i odpowiedzialności administratora zgodnie z RODO będzie w szczególności należało:

1) przetwarzanie danych osobowych zgodnie z podstawowymi zasadami określonymi w rozporządzeniu,
2) wykonywanie obowiązków, które wynikają z praw osób, których dotyczą dane osobowe,
3) zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych,
4) przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych zgodnie z zasadami określonymi w rozporządzeniu – jeżeli takie operacje administrator realizuje,
5) wyznaczenie inspektora ochrony danych – gdy jest do tego zobowiązany na podstawie art. 37 ust. 1 rozporządzenia.

Przed wdrożeniem zmian należy opracować harmonogram

Aby przygotować się do właściwego wypełniania nowych obowiązków, osoby wyznaczone do wdrożenia RODO w spółce muszą opracować dostosowany odpowiednio do celów, zakresu i złożoności prowadzonych operacji przetwarzania danych osobowych szczegółowy harmonogram realizacji zadań, które należy w ramach takiego przygotowania zrealizować. Powinien on określać:

- osobę lub strukturę organizacyjną, która jest odpowiedzialna za realizację zadania,
- osoby lub struktury organizacyjne współpracujące podczas realizacji zadania,
- sposób realizacji zadania oraz opracowania wyników jego realizacji,
- termin realizacji zadania.

Po opracowaniu i zatwierdzeniu harmonogramu należy zorganizować szkolenie poświęcone nowym obowiązkom wynikającym z RODO, w tym w szczególności zadaniom określonym w harmonogramie. Szkoleniem powinny zostać objęte przede wszystkim osoby, które będą realizowały zadania wskazane w harmonogramie.

Należy wskazać kategorie osób, których dane są przetwarzane

Spółka reprezentowana przez prezesa jako administrator musi przetwarzać dane osobowe zgodnie z podstawowymi zasadami określonymi w RODO. W związku z tym jednym z zadań, jakie należy określić w harmonogramie, aby przygotować się do ogólnego rozporządzenia o ochronie danych, będzie opracowanie wykazu kategorii osób, których dane dotyczą, i określenie celów przetwarzania danych w odniesieniu do poszczególnych kategorii osób oraz kategorii przetwarzanych danych w związku z realizacją poszczególnych celów.

Do opracowania wykazu należy wykorzystać dokumentację opisującą sposób przetwarzania danych oraz stosowane środki techniczne i organizacyjne zapewniające ich ochronę oraz zgłoszenia zbiorów danych przekazane do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO) lub rejestr zbiorów danych prowadzony przez administratora bezpieczeństwa informacji (ABI) – jeśli został w spółce powołany. Wykaz należy uzgodnić ze wszystkimi, którzy uczestniczą w wyznaczeniu celów przetwarzania danych osobowych oraz organizowaniu sposobu ich przetwarzania, w tym ustalaniu zakresu przetwarzanych danych oraz czasu ich przechowywania.

WAŻNE

Podstawowe zasady przetwarzania danych osobowych zgodnie z ogólnym rozporządzeniem o ochronie danych (art. 5 RODO):

1) zgodność z prawem, rzetelność i przejrzystość,
2) ograniczenie celu,
3) minimalizacja danych,
4) prawidłowość,
5) ograniczenie przechowywania,
6) integralność i poufność oraz
7) rozliczalność – zasada mówiąca, że administrator musi być w stanie wykazać w przejrzysty i zrozumiały sposób, że przestrzega zasad wymienionych w pkt 1–6.

Należy zweryfikować, czy dane są przetwarzane zgodnie z RODO

Kolejnym zadaniem, jakie stoi przed spółką jest i które należy określić w harmonogramie, będzie przeprowadzenie sprawdzenia (analizy i oceny), czy dane osobowe są przetwarzane zgodnie z zasadami przetwarzania danych określonymi w ogólnym rozporządzeniu o ochronie danych. Będzie trzeba również przygotować uzasadnienie, w którym zostanie wykazane, że te zasady są przestrzegane. Taką analizę i ocenę powinny przeprowadzić osoby, które mają istotny wpływ na określenie celów przetwarzania danych osobowych oraz zorganizowanie procesu ich przetwarzania w spółce. Wytyczne do przeprowadzenia takiej analizy i oceny powinien przygotować administrator bezpieczeństwa informacji.

Po przeprowadzeniu tej analizy i oceny, dla każdej kategorii osób i celu przetwarzania danych dotyczących danej kategorii osób, należy:

1) określić, jaki warunek jest podstawą prawną do przetwarzania danych,
2) określić, jaki warunek jest podstawą prawną do przetwarzania szczególnych kategorii danych osobowych,
3) uzasadnić jasnym i prostym językiem, przejrzystym dla osób, których dane dotyczą, że dane są przetwarzane rzetelnie,
4) potwierdzić i ewentualnie uzasadnić, że dane zbierane do konkretnych celów są adekwatne oraz niezbędne do osiągania tych celów oraz nie są dalej przetwarzane niezgodnie z tymi celami,
5) określić działania, które są prowadzone, aby zapewnić, że dane, które są nieprawidłowe w świetle celów ich przetwarzania, są niezwłocznie usuwane lub korygowane,
6) potwierdzić i ewentualnie uzasadnić, że przetwarzane dane osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których są przetwarzane.

Trzeba sprawdzić, czy zapewnione jest bezpieczeństwo danych osobowych

Kolejnym zadaniem, które należy określić w harmonogramie, jest przeprowadzenie sprawdzenia (analizy i oceny), czy dane osobowe są przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych, czyli czy jest przestrzegana zasada „integralność i poufność".

Taką analizę powinny przeprowadzić osoby odpowiedzialne w spółce za projektowanie, wdrażanie, funkcjonowanie oraz ocenę skuteczności środków technicznych i organizacyjnych, których zadaniem jest zapewnienie odpowiedniego bezpieczeństwa danych osobowych. Po przeprowadzeniu analizy, administrator bezpieczeństwa informacji powinien ocenić, czy bezpieczeństwo danych osobowych jest zapewnione na odpowiednim poziomie.

Należy przygotować się do realizacji praw osób, których dane dotyczą

Biorąc pod uwagę prawa osób, których dotyczą przetwarzane przez spółkę dane, przygotowując się do stosowania przepisów ogólnego rozporządzenia o ochronie danych, osoby odpowiedzialne w spółce za wdrożenie RODO powinny podjąć działania, dzięki którym ustalą:

- które z praw i w jakim zakresie będą przysługiwały osobom, których dotyczą dane,
- które z praw oraz wynikające z tych praw obowiązki należy ograniczyć polskim aktem prawnym,
- kto, w jakim zakresie i w jaki sposób będzie realizował obowiązki wynikające z praw osób, których dotyczą dane.

Informacje te powinien ustalić zespół, w którego w skład powinni wejść:

- administrator bezpieczeństwa informacji – jeżeli został powołany,
- prawnicy świadczący usługi w zakresie obsługi prawnej,
- osoby, które mają istotny wpływ na określenie celów przetwarzania danych osobowych oraz zorganizowanie procesu ich przetwarzania w spółce.

Trzeba oszacować ryzyko naruszenia bezpieczeństwa danych osobowych

Obowiązki spółki reprezentowanej przez prezesa jako administratora, których realizacja ma na celu zapewnienie odpowiedniego stopnia bezpieczeństwa przetwarzanych danych osobowych, oraz wskazówki, w jaki sposób taki cel należy osiągać, są określone w art. 32 oraz motywie (83) preambuły RODO. Zgodnie z nimi poziom bezpieczeństwa przetwarzanych danych osobowych powinien być odpowiedni do zidentyfikowanego ryzyka naruszenia praw i wolności osób fizycznych wiążącego się z przetwarzaniem danych.

UWAGA

Aby zapewnić odpowiedni poziom bezpieczeństwa danych, spółka musi wdrożyć odpowiednie środki techniczne i organizacyjne, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

Ogólne rozporządzenie o ochronie danych wprost nie nakłada na spółkę obowiązku zarządzania ryzykiem naruszenia praw i wolności osób fizycznych, które wiąże się z przetwarzaniem danych, jednak z treści i logiki przepisów RODO wynika, że właściwą drogą do zapewnienia odpowiedniego do tego ryzyka poziomu bezpieczeństwa jest zarządzanie tym ryzykiem.

Jednocześnie w art. 32 ust. 1 lit. a, b, c oraz d RODO znajduje się zalecenie, zgodnie z którym w stosownym przypadku należy wdrażać następujące środki techniczne i organizacyjne, które zapewniają stopień bezpieczeństwa odpowiadający zarządzanemu ryzyku:

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

UWAGA

Spółka reprezentowana przez prezesa jako administrator powinna wypracować odpowiednie dla siebie podejście do zarządzania ryzykiem naruszenia praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych uwzględniające swoje środowisko, specyfikę prowadzonej działalności oraz posiadane doświadczenie, a w szczególności charakter, zakres oraz cele i sposób przetwarzania danych osobowych.

Trzeba prowadzić rejestr czynności przetwarzania danych osobowych

Jednym z obligatoryjnych środków ochrony danych osobowych zawartym w ogólnym rozporządzeniu o ochronie danych jest prowadzenie rejestru czynności przetwarzania danych osobowych, który obejmuje informacje wymienione w art. 30 ust. 1 RODO. Rejestr ten można opracować, wykorzystując w szczególności:

1) posiadaną przez spółkę dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
2) prowadzony przez administratora bezpieczeństwa informacji rejestr zbiorów danych,
3) zgłoszenia zbiorów danych przekazane do rejestracji GIODO,
4) ustalenia wypracowane w wyniku realizacji zadań wyszczególnionych w harmonogramie.

UWAGA

Jeżeli w spółce został powołany administrator bezpieczeństwa informacji, to on powinien opracować rejestr czynności przetwarzania danych osobowych. Od 25 maja 2018 r. rejestr może prowadzić inspektor ochrony danych, jeżeli zostanie wyznaczony – taką rekomendację przedstawiła Grupa Robocza Art. 29 w wytycznych dotyczących inspektora ochrony danych.

Konieczna będzie współpraca z organem nadzorczym

Kolejnym środkiem bezpieczeństwa, jaki wskazuje ogólne rozporządzenie o ochronie danych, jest współpraca z organem nadzorczym – na jego żądanie oraz w ramach wykonywanych przez niego zadań. Zgodnie z art. 39 ust. 1 pkt d RODO współpraca z organem nadzorczym należy do jednych z podstawowych zadań inspektora ochrony danych. Jeśli inspektor ochrony danych nie zostanie w spółce wyznaczony, trzeba będzie oddelegować zespół własnych pracowników do współpracy z organem nadzorczym. Każdy z takich pracowników powinien mieć jasno określony zakres współpracy, w której będzie odgrywał wiodącą rolę i ponosił za nią odpowiedzialność.

O naruszeniach ochrony danych trzeba będzie poinformować organ nadzorczy

Do środków bezpieczeństwa danych, wskazanych przez ogólne rozporządzenie o ochronie danych, trzeba zaliczyć też obowiązek zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego. Pojęcie „naruszenie ochrony danych osobowych" zasługuje na szczególną uwagę w związku z tym, że zostało zdefiniowane jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

WAŻNE

Do organu nadzorczego nie trzeba będzie zgłaszać naruszeń, jeśli administrator oceni, że jest mało prawdopodobne, by skutkowały one ryzykiem naruszenia praw lub wolności osób fizycznych.

Przy pomocy administratora bezpieczeństwa informacji (jeżeli został w spółce powołany) należy wypracować zasady i sposób:

1) oceny i kwalifikowania stwierdzonych naruszeń ochrony danych osobowych jako naruszeń, które z dużym prawdopodobieństwem mogą skutkować ryzykiem naruszenia praw i wolności osób fizycznych,
2) zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu.

O naruszeniu trzeba będzie poinformować też osoby, których dane dotyczą

Zgodnie z ogólnym rozporządzeniem o ochronie danych o naruszeniu ochrony danych będzie trzeba niezwłoczne zawiadomić osoby, których dane dotyczą. Administrator będzie miał ten obowiązek, tylko jeśli uzna, że naruszenie będzie mogło spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Z pomocą administratora bezpieczeństwa informacji (jeżeli został w spółce powołany) należy opracować zasady i sposób wykrywania i dokonywania oceny naruszeń ochrony danych osobowych oraz:

1) kwalifikowania ich jako naruszeń, które z wysokim prawdopodobieństwem mogą skutkować ryzykiem naruszenia praw i wolności osób fizycznych,
2) ustalania, czy są spełnione warunki, o których mowa w art. 34 ust. 3 RODO, i w rezultacie jest wymagane lub nie zawiadomienie osoby, której dane dotyczą, o stwierdzonym naruszeniu,
3) zawiadamiania osób, których dane dotyczą, o stwierdzonym naruszeniu ochrony danych osobowych.

Trzeba będzie ocenić skutki planowanego przetwarzania danych

Kolejnym z obowiązków spółki reprezentowanej przez prezesa jako administratora zgodnie z RODO, którego realizacja ma zapewnić bezpieczeństwo danych, jest przeprowadzanie oceny skutków planowanych operacji przetwarzania danych osobowych przed rozpoczęciem przetwarzania, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Z pomocą administratora bezpieczeństwa informacji (jeżeli został w spółce powołany) należy opracować zasady i sposób:

1) przeprowadzania analizy planowanych operacji przetwarzania danych osobowych i oceniania, czy mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych,

2) oceniania skutków dla ochrony danych planowanych operacji przetwarzania danych osobowych, w szczególności z użyciem nowych technologii,

3) prowadzenia konsultacji z organem nadzorczym przed rozpoczęciem planowanych operacji przetwarzania danych.

Niektóre spółki będą musiały wyznaczyć inspektora ochrony danych

Niektóre spółki jako administratorzy będą miały obowiązek wyznaczenia inspektora ochrony danych o odpowiednich kwalifikacjach zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych, a także wspierania go w wypełnianiu przez niego zadań.

WAŻNE

W opinii GIODO funkcję inspektorów ochrony danych będą mogli pełnić jako kontynuację dotychczas pełnionej funkcji administratorzy bezpieczeństwa informacji zarejestrowani przed 25 maja 2018 r. w ogólnokrajowym, jawnym rejestrze. Takie rozwiązanie GIODO uzasadnia tym, że obecny status i kompetencje administratorów bezpieczeństwa informacji, który obowiązuje od 1 stycznia 2015 r., miał na celu przygotowanie tej grupy do wymogów określonych ogólnym rozporządzeniem o ochronie danych, jak również związaną z tym postępującą profesjonalizacją osób pełniących tę funkcję. Z tym stanowiskiem nie zgadza się jednak środowisko administratorów bezpieczeństwa informacji.

Podstawa prawna:

- ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2016 r. poz. 922),
- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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).

Autor:
Tomasz Błoński,
zastępca administratora bezpieczeństwa informacji w Zakładzie Ubezpieczeń Społecznych, w latach 2000–2015 naczelnik wydziału w Departamencie Zarządzania Bezpieczeństwem Informacji, wieloletni członek Stowarzyszenia Administratorów Bezpieczeństwa Informacji

Stopka redakcyjna

Redaktor:	Wioleta Szczygielska
ISBN:	978-83-269-7057-3
E-book nr:	2HH0668
Wydawnictwo:	Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł